2026

CLAUSIER DATA et IA

datapublica
Data et IA pour l'intérêt général

Les interconnectés
RÉSEAU DES TERRITOIRES INNOVANTS

FRANCE URBAINE
MÉTROPOLES, AGGLOS ET GRANDES VILLES

INTERCOMMUNALITÉS DE FRANCE

SOMMAIRE

REMERCIEMENTS

Les Interconnectés, remercient les équipes des cabinets Civiteo et Alerion Avocats pour la proposition de clausier ainsi que la Communauté d'agglomération du Sicoval, la Rochelle Agglomération, Nantes Métropole, la Communauté de communes Terre de Confluences, la Communauté de communes de Lacq Orthez, la Métropole Aix Marseille, la Communauté d'agglomération Paris Saclay, Bordeaux Métropole ainsi que France urbaine pour leur relecture attentive et leurs contributions.

ÉDITO

Porte-voix des élus, fédératrice des attentes des collectivités locales, l'association les Interconnectés défend depuis sa création la vision du numérique comme politique publique.

Au fil des années, nous avons collectivement construit l'ambition d'un numérique responsable et indépendant qui engage la prise en compte des enjeux sociaux, environnementaux et fixe un cadre éthique de confiance.

Si les enjeux d'inclusion numérique et de data se sont invités dès 2010 à nos travaux, il aura fallu attendre 2020 pour que nous prenions collectivement la mesure de l'enjeux environnemental, des risques induits par une utilisation non maitrisée des technologies et de la nécessité de définir des règles du jeux claires dans la mise en œuvre du numérique responsable. C'est ainsi que progressivement **la question de l'achat public et de la contractualisation entre acteurs publics et opérateurs est devenu un enjeu stratégique.**

Fidèle à notre volonté de porter la stratégie commune mais aussi d'accompagner et d'outiller l'action, **le présent clausier data et IA s'inscrit dans la continuité de nos précédents travaux pour clarifier le cadre éthique et juridique de nos politiques locales.**

Mais aussi et surtout, il vise à activer la commande publique comme un levier efficace pour la réussite de nos projets et un moyen opérationnel actionnable pour faire valoir cette vision responsable du numérique.

Pensé pour pouvoir être mobilisé par des territoires de toute taille, le présent clausier ajoute aux approches classiques de sécurisation des contrats, les éléments socle de nos stratégies communes : respect des personnes, transparence, indépendance numérique, sobriété.

Rencontre de l'expertise des cabinets Civiteo et Alerion Avocats et des demandes des collectivités membres qui ont accepté de partager leurs pratiques et ont complété utilement les différents domaines, nous espérons que ce document saura vous être utile !

Céline COLUCCI,

Déléguée générale
Les Interconnectés

__Les Interconnectés__ est la première association nationale de collectivités centrée sur les politiques publiques numériques. Sa mission est d'accompagner les élus et les agents des collectivités pour mettre l'innovation et le numérique au service des territoires. Interlocuteur de référence de l'État, elle mobilise les acteurs et les experts afin de faciliter la mise en œuvre sur le terrain d'un numérique social, sobre et éthique.

PRÉAMBULE

Les collectivités territoriales n'ont jamais autant produit, collecté et exploité de données. Les données des usagers, de gestion et d'intérêt territorial sont au cœur de la capacité des collectivités à piloter leurs politiques publiques.

Leur maîtrise n'est pas qu'une question technique, c'est aussi une question de responsabilité. L'accélération de l'intelligence artificielle la rend encore plus pressante. L'IA ouvre des opportunités réelles, mais pose aussi des défis nouveaux : les sources de ces modèles, l'explicabilité des résultats, la transparence des traitements et le risque de dépendance à des systèmes toujours plus complexes.

De nombreux témoignages de collectivités soulignent un risque réel de dépendance à certaines technologies propriétaires, à des données produites dans des formats inexploitables, etc.

Au sein des Interconnectés, les travaux de la commission numérique qu'ils soient sur l'IA ou sur la gestion des données fixent un cap pour un numérique responsable qui encourage la transparence, le déploiement de services réellement utiles et maîtrisés sur tous les plans (éthique, démocratique, environnemental).

Lors des *Journées Experts* et *Territoir'Prod,* nous avons démontré à plusieurs moments en quoi la commande publique est un levier puissant et structurant pour prévenir ces situations. Un contrat qui prend en compte des critères de numérique responsable vise à produire un cadre de confiance. En faire l'impasse, c'est prendre le risque que le prestataire fixe seul ses propres règles et besoins.

Nous voyons aussi s'intensifier les obligations à travers une accumulation de cadres réglementaires *(Data et IA : les nouvelles règles du jeu en Europe (2024)).* Cependant entre le texte réglementaire et la pratique contractuelle, il existe un écart que ce document entend contribuer à combler.

La commande publique, levier structurant des stratégies numériques responsables, contribue à garantir la mise en œuvre de nos engagements. Pour outiller et défendre les intérêts des collectivités, la Commission Numérique, conjointe à Intercommunalités de France, France urbaine et Les Interconnectés, propose ce socle de clauses juridiques sur l'IA et la data.

Ces propositions de clauses, basées sur des expériences concrètes de terrain ont vocation à outiller les acheteurs et les directions métiers afin de structurer leurs exigences et engager des échanges éclairés avec leurs prestataires.

Ce document a vocation à être une ressource vivante, didactique, accessible à tous les territoires quelle que soit leur taille ou leur maturité sur ces sujets. Il pose un socle partagé qui devra être adapté au contexte et à la situation particulière de chacun et sera amené à évoluer suivant le cadre juridique et les pratiques issues du terrain.

Il s'adresse aussi aux offreurs de services. Éditeurs, intégrateurs, prestataires : ce clausier a vocation à rendre les attentes des collectivités plus lisibles et prévisibles. Les défis sont trop importants pour simplement opposer donneurs d'ordre et prestataires. Ces clauses visent une trajectoire. C'est en dialoguant sur des bases partagées, que nous pourrons répondre collectivement à ces besoins.

LE MOT DES AUTEURS

Écrire un clausier juridique sur la gestion des données publiques et sur l'intelligence artificielle dans les collectivités locales nécessite de faire preuve de convictions.

Acteur pionnier de la data territoriale depuis près de 10 ans, le collectif Data Publica (représenté ici par les cabinets Alérion Avocats et CIVITEO) connaît bien les enjeux auxquels font face les territoires. Les injonctions sont nombreuses, et parfois contradictoires. Il faut utiliser plus de données pour améliorer et accélérer la prise de décision, pour renforcer la performance des politiques publiques, et parfois faire des économies. Mais il faut aussi protéger la vie privée des habitants (sans oublier celle des agents), garantir la sécurité des systèmes d'information, limiter l'empreinte énergétique du numérique et dorénavant contribuer à la souveraineté nationale. À bien y regarder, l'irruption massive de l'intelligence artificielle ne fait qu'amplifier ces enjeux, ces exigences et parfois ces contradictions.

Beaucoup de collectivités, et ce faisant leurs agents, s'efforcent d'appliquer pour elles-mêmes des règles rigoureuses : mise en œuvre du RGPD, organisation du cycle de vie des données, gouvernance data et plus récemment, chartes et doctrines d'usage de l'intelligence artificielle. Mais l'enjeu dépasse les frontières des services. L'action publique repose sur de multiples interactions et de multiples partenariats. L'administration publique construit l'efficacité de son intervention en s'appuyant sur des partenaires subventionnés, publics ou privés, des prestataires via des contrats de la commande publique (délégation de service public, marchés publics…). Les règles de bonne gestion de la data et de l'IA appliquées à soi-même ne suffisent pas. D'où l'importance de disposer de clauses à insérer au fil des contrats pour garantir que les principes d'un usage maîtrisé des données (et dorénavant de l'IA) seront respectés tout au long de la chaîne de la fabrication et de la mise en œuvre du service public.

L'équipe de Data Publica avait publié en 2020, avec le soutien de la Banque des Territoires, un clausier sur la donnée territoriale. Il reposait sur l'expérience et les travaux de quelques collectivités pionnières. Mais les administrations qui ont recours à ces clauses sont dorénavant nombreuses, et de toutes tailles. Le cadre juridique a aussi connu des évolutions notables. Il était important de faire cette mise à jour. Concernant l'intelligence artificielle, la matière est plus mouvante, voire incertaine. Mais nos équipes mesurent chaque jour l'importance pour les administrations publiques de fixer des règles et de poser des garde-fous. Les collectivités veulent à juste titre contrôler, et parfois limiter ou interdire, l'usage d'IA non souveraines, qui mettraient en péril les principes et les valeurs du service public.

Produire ce clausier sur la data et l'IA constitue une prise de risque tant le sujet est volatile. Mais nous l'assumons, fidèles en cela aux valeurs du collectif Data Publica : faire prévaloir l'intérêt général et protéger les principes de l'action publique. Nous assumons donc quelques clauses qui seront parfois jugées trop prudentes ou excessives. Et nous pouvons attester que toutes ont déjà eu, ici ou là, leur utilité.

Pour conclure, nous proposons trois recommandations aux utilisateurs de ce clausier.

D'abord, un point de méthode : prenez votre temps pour découvrir ces clauses et lire les éléments de contexte que nous proposons. Si certains points peuvent paraître ardus, ils sont tous issus de l'expérience concrète de collègues dans d'autres territoires. Ils ont tous leur utilité.

Ensuite, une précaution : ce clausier fournit des modèles, mais il vous faudra les adapter. Chaque projet et chaque contrat ont leurs spécificités, prenez le temps de les intégrer.

Enfin, une évidence. Les clauses sont une condition nécessaire mais pas suffisante pour garder la maîtrise des données (et des IA) : faites en sorte de pouvoir contrôler l'exécution de vos clauses ; ce qui signifie prévoir des tests et des vérifications avec les agents des métiers comme avec les experts de la direction des systèmes d'information.

Ce clausier est le fruit d'une co-production avec les Interconnectés, que nous remercions chaleureusement pour avoir engagé cette collaboration et pour en assurer la diffusion.

Nous tenons également à remercier les équipes du Sicoval, de La Rochelle, Nantes, Terres des Confluences, Lacq-Orthez et Aix-Marseille pour leur participation et leurs précieux retours.

Nul doute que vous serez nombreux à vous saisir de ce document. Bonne lecture !

Jacques Priol
Président de CIVITEO

civiteo
Stratégie data & IA

Schéhérazade Abboub
Avocate associée

alerion
AVOCATS

PARTIE 1

D'UN DROIT PUBLIC DE LA DONNÉE À L'ÉMERGENCE D'UN DROIT DE L'IA PUBLIQUE ?

LA CONSTRUCTION PROGRESSIVE D'UN RÉGIME JURIDIQUE DE LA DONNÉE PUBLIQUE

Dans beaucoup de collectivités, le sujet de la data comme enjeu juridique a émergé avec les obligations réglementaires de protection des données personnelles. L'entrée en vigueur du RGPD[1] en 2018 a placé sur le devant de la scène la nécessité de protéger les données des habitants, et les sanctions à défaut de le faire.

La même année sont entrées en vigueur les principales dispositions de la loi pour une République numérique, dite « loi Lemaire[2] ». Votée en 2016, elle oblige depuis octobre 2018 les collectivités de plus de 3 500 habitants à publier leurs données au titre de « l'open data par défaut ». Certes, il existe quelques exemptions : données couvertes par le secret des affaires, protégées par des droits d'auteur ou soumises à un régime de propriété intellectuelle, ou encore des données personnelles non anonymisables à effort raisonnable. Mais l'objectif du législateur est bien de « libérer » de façon massive des données pour renforcer la transparence de l'action publique et stimuler l'innovation dans les territoires.

Cette double injonction, entre ouverture et protection des données, a historiquement structuré les premières politiques de la donnée des territoires. Certaines collectivités particulièrement volontaristes avaient d'ailleurs anticipé la loi. Rennes Métropole est souvent citée pour avoir été la première (dès 2010) à créer un portail d'accès à la donnée ouverte, rapidement suivie par Nantes, Lille ou Bordeaux ou encore les départements de Loire-Atlantique et de Gironde.

La fin des années 2010 est aussi celle des premiers grands projets de smart city ou ville intelligente. Dijon Métropole est ainsi devenu le premier territoire métropolitain français à confier la gestion de plusieurs fonctions urbaines et leur pilotage par la data à un groupement d'opérateurs privés. Depuis, de nombreux élus de la France entière ou venus de l'étranger ont visité le poste de commandement de la ville intelligente dijonnaise. Mais ils sont sans doute moins nombreux à savoir que Dijon a fait œuvre d'innovation juridique en créant dans son marché public un chapitre entier dédié à la gouvernance des données issues du contrat. D'autres ont suivi, et il est dorénavant acquis que les données de gestion des marchés publics ou des concessions de service public sont la propriété des acheteurs et des autorités concédantes.

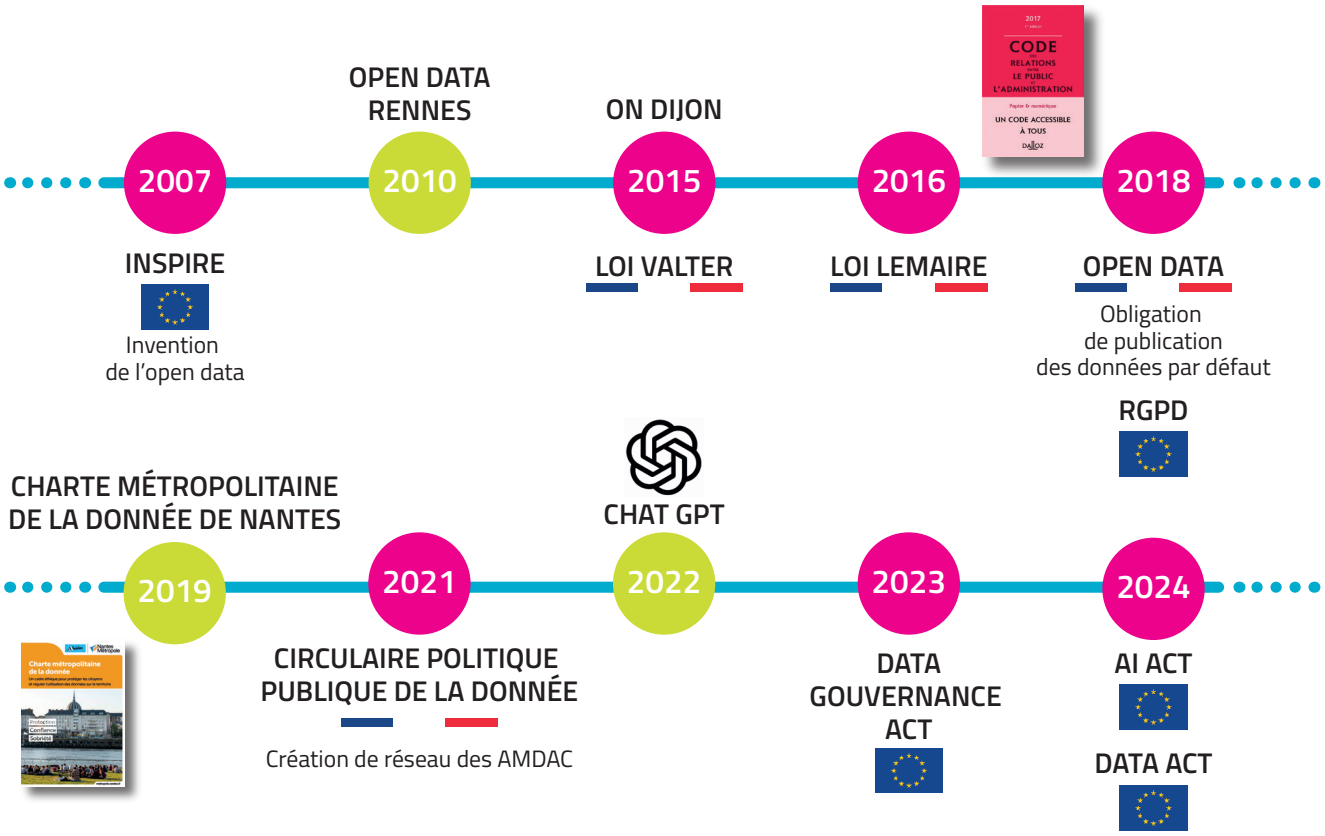
1 • *Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données*

2 • *Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique*

D'autres éléments juridiques sont arrivés de Bruxelles. À compter de 2020, une stratégie européenne sur les données se construit progressivement. Elle vise à favoriser, à l'échelle du marché commun, le partage et la circulation des données. Elle définit la notion d'espaces de données européens (dataspace), qui peuvent réunir des acteurs publics ou privés dans une dynamique de partage et de valorisation conjointe de leurs data[3].

Entré en vigueur en septembre 2023, le Data Governance Act[4], prévoit un traitement particulier pour les données qui revêtent un caractère d'intérêt général. Les acteurs privés (comme les particuliers d'ailleurs) sont incités à faire preuve d' « altruisme en matière de données ». L'idée est de permettre aux acteurs publics de disposer des données utiles à l'accomplissement de leurs missions d'intérêt général. Les exemples sont nombreux. Combien de maires rêvent de disposer des données d'AirBnb ou Booking pour ajuster leurs politiques touristiques (ou immobilières) ? Combien d'équipes en charge des plans de circulation lorgnent sur les données de Waze ? Dans certains cas, un autre règlement (le Data Act[5]) prévoit la possibilité pour les pouvoirs publics de « réquisitionner » des données d'entreprises lorsque cela apparaît indispensable à la gestion d'une urgence climatique ou de sécurité publique.

Bref, depuis la directive Inspire de 2007 sur les données géographiques, le droit public de la donnée et le droit de la donnée publique se construisent pas à pas. Et si en 2026 beaucoup de choses restent mal ou peu définies, un certain nombre de jalons ont été posés.



Source : civiteo

3 · *Data et IA : Les Nouvelles Règles du Jeu en Europe, 2024, Les Interconnectés* https://www.interconnectes.com/documents/9da97714-f519-f011-8b3d-000d3a236aa0/data-et-ia-les-nouvelles-regles-du-jeu-en-europe-2024-

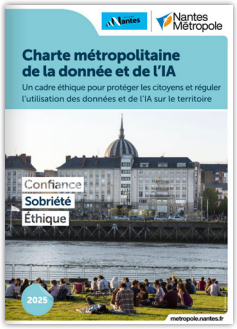
4 · *Règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données*

5 · *Règlement (UE) 2023/2854 du Parlement européen et du Conseil du 13 décembre 2023 concernant des règles harmonisées portant sur l'équité de l'accès aux données et de l'utilisation des données*

L'APPROPRIATION PAR LES COLLECTIVITÉS LOCALES

Les collectivités locales, et tout particulièrement les intercommunalités, se sont rapidement saisies du sujet. Comment garantir la maîtrise et la qualité des données du service public ? Quel équilibre trouver entre protection et transparence ? Sur quelles bases engager le dialogue avec les opérateurs privés ? Plusieurs territoires ont opté pour la publication de « chartes » ou de « stratégies » par lesquelles ils fixent les priorités et encadrent la façon dont les territoires vont gérer et valoriser leurs données. Et ces documents d'orientation, dont la valeur juridique demeure indicative, vont rapidement être annexés à des actes et déclinés en « clauses data » opposables à des tiers.

NANTES MÉTROPOLE, LA PREMIÈRE CHARTE DE LA DONNÉE (2019)



Dès 2019, la charte métropolitaine de la donnée de Nantes énonce des principes de protection de la vie privée et de maîtrise des données publiques au service d'un « intérêt métropolitain ». Elle aborde de nombreux autres points, notamment la transparence et des actions volontaristes d'open data et de publication d'algorithme. Elle anticipe déjà l'arrivée de l'intelligence artificielle en encadrant son recours pour des prises de décision individuelle. Élaborée en partenariat avec la Ville de Montréal, engagée dans une démarche similaire, la charte nantaise en inspirera de nombreuses autres.

À noter : cette charte a été l'objet d'une mise à jour en juin 2025 pour intégrer les travaux récents menés par la collectivité en matière d'intelligence artificielle[7].

ANGERS LOIRE MÉTROPOLE, UNE STRATÉGIE DE LA DONNÉE AU SERVICE DU TERRITOIRE INTELLIGENT (2023)

Angers a été la première métropole à se doter d'une « stratégie de la donnée ». Ce document de référence, voté par le Conseil métropolitain en 2023, fixe des priorités quant aux usages de la donnée : data et gestion de l'eau, data et déchets, data pour des économies d'énergie, la data et les politiques sociales… Elaborée de façon participative, sa rédaction a impliqué plus de 200 personnes (élus, services, partenaires et citoyens).

Votée dans le contexte du déploiement d'un ambitieux programme de ville intelligente, la stratégie angevine intègre et décline un certain nombre de principes juridiques, au premier rang desquels la protection des données des habitants et la transparence à travers l'information des usagers et l'open data.

6 • *Charte métropolitaine de la donnée et de l'IA, Nantes Métropole, 2025.* https://www.calameo.com/nantes/read/0045904585ea8a3b2ae83

LES « 10 LOIS DE LA DATA ET DE L'IA » DE MONTPELLIER MÉDITERRANÉE MÉTROPOLE (2024)

La Stratégie de la donnée et de l'intelligence artificielle de la Métropole de Montpellier présente la caractéristique d'avoir été élaborée avec le concours d'une véritable convention citoyenne (pour son volet IA).

Cette stratégie intègre deux documents juridiques : une « charte interne » et un document de communication vers le grand public « Les 10 lois de la data et de l'IA » de la collectivité. De nombreux points juridiques sont affichés comme de véritables axes de travail qui définissent la politique de la donnée montpelliéraine : protection de la vie privée, sobriété numérique (et numérique responsable), transparence et open data…

L'ADOPTION DE CHARTES PAR DES COLLECTIVITÉS DE TOUTES TAILLES

L'appropriation des sujets data ne se limite pas qu'aux plus grandes collectivités. Ainsi, de plus en plus de communes et d'intercommunalités de taille moyenne ont adopté une doctrine data, sous forme de charte : le Grand Chambéry, la Communauté de communes des Vallées de Thônes (CCVT) …

Ce mouvement bénéficie dans certains cas de l'appui de plus grands territoires. Ainsi, en 2022, la Région Bourgogne-Franche-Comté publie un guide visant à aider les collectivités, et notamment les petits territoires et les communes rurales, à s'emparer des enjeux data.

Publié dans le cadre d'un appel à projets Territoires Intelligents et Durables visant à identifier la façon dont les communes du territoire de la Région s'emparent des sujets data, ce document pédagogique aborde les principaux aspects techniques, juridiques et organisationnels de la gestion des données. Nourri d'exemples de projets territoriaux, le guide propose des recommandations pratiques pour lancer diverses démarches axées autour de la donnée (création d'un portail d'open data, organisation d'une gouvernance de la donnée, conduite d'expérimentation, collaboration avec d'autres territoires, …).

En 2023, les Interconnectés publient le **Guide des chartes territoriales de la donnée.** Ce document fournit aux collectivités les outils pour construire leurs propres chartes en fonction de leurs objectifs et des besoins de leurs territoires. Il met également en avant l'expérience des territoires pionniers en la matière et explique, de façon concrète, ce que sont les chartes territoriales dans toute leur diversité.

Ces documents sont le reflet de priorités politiques. Ils s'articulent avec les autres politiques menées en matière de numérique (stratégie numérique responsable[7], médiation numérique, etc.). Ils donnent à voir les priorités d'un territoire en matière de données. Les objectifs ainsi fixés se déclinent ensuite en plans d'action et en processus de management pour les mettre en œuvre. Il s'agit de définir des moyens, de préparer des feuilles de route, de structurer la « fonction data », d'organiser le pilotage du « cycle de vie de la donnée » au sein de la collectivité.

7 · *L'adoption d'une stratégie numérique responsable est devenue une obligation pour les communes de plus de 50 000 habitants depuis le 1er janvier 2025, en application de la loi n° 2021-1485 du 15 novembre 2021 visant à réduire l'empreinte environnementale du numérique en France (loi REEN).*

LES « CLAUSES DATA »

C'est ici qu'interviennent les « clauses data » c'est-à-dire la déclinaison juridique des principes énoncés dans des chartes ou des stratégies. Les clauses juridiques permettent de passer d'une déclaration d'intention à la possibilité d'un contrôle.

Les débuts sont parfois modestes. Il s'agit ici d'annexer une charte à un cahier des charges ou à une convention de subvention.

Mais progressivement les choses se précisent : définition des données concernées, conditions de récupération des données (régularité, format, modalités techniques…). Opposables à des tiers, ces clauses se retrouvent dans des contrats publics aux côtés des clauses RGPD dont la CNIL a abondamment et très utilement fait la promotion. Les choses s'affinent au fur et à mesure des expériences, notamment sous l'impulsion des villes et des intercommunalités les plus connectées : clauses sur l'hébergement, réversibilité (c'est-à-dire la récupération complète des données par l'acteur public), propriété intellectuelle…

Les clauses data concernent les prestataires (notamment informatiques), les délégataires, mais aussi les partenaires (associations subventionnées, conventions entre collectivités…).

En 2021, la Banque des territoires publie le Guide des bonnes pratiques contractuelles et recommandations pour la mise en place d'une gouvernance de la donnée territoriale[8], qui propose des clauses data clés en main à disposition de collectivités de toute taille pour maîtriser les données dans les contrats de la commande publique.

Le présent guide en constitue une véritable mise à jour en 2026.

8 • https://www.banquedesterritoires.fr/gestion-des-donnees-territoriales

LA « RÉVOLUTION DE L'IA »

Depuis l'irruption de ChatGPT fin 2022, la diffusion massive du recours à l'IA est un phénomène majeur qui concerne l'ensemble de notre société, service public local y compris. Courant 2026, plus de 3 collectivités sur 4 (de plus de 3 500 habitants) auront commencé à utiliser de façon quotidienne l'IA[9].

L'utilisation de l'IA repose sur un usage massif des données : données du territoire mais aussi données des usagers, données administratives, données internes, données d'entreprises parfois protégées, données couvertes par des droits d'auteur… L'arrivée de l'IA bouleverse complètement un cadre juridique qui était en voie de stabilisation. Des risques nouveaux apparaissent : biais et erreurs, discrimination algorithmique, enjeu de souveraineté, déresponsabilisation des agents, manque de transparence vis-à-vis des usagers… Et à l'évidence les textes nationaux ne sont pas d'un grand secours.

Dans ce contexte, la réglementation européenne (AI Act[10]) a l'immense mérite d'affirmer qu'en Europe le recours massif à l'IA ne peut en aucun cas bafouer nos droits fondamentaux. C'est la raison pour laquelle elle interdit purement et simplement certains usages (comme la notation sociale algorithmique « à la chinoise » par exemple). Mais ceci n'est pas suffisant pour les quelques collectivités qui commencent à utiliser de l'IA et souhaitent en encadrer l'usage, par leurs agents mais aussi très vite par leurs prestataires.

À l'image des travaux menés depuis plusieurs années sur la donnée, quelques administrations locales ont commencé à structurer des stratégies de déploiement de l'IA et cherchent des leviers juridiques (notamment pour la commande publique) afin de sécuriser leurs pratiques et de garantir une intégration maîtrisée de l'IA dans les processus de fabrication de l'action publique.

Le présent document s'inscrit dans cette dynamique. Il propose un clausier dédié d'abord à la donnée puis à l'IA avec une double ambition.

Ce document se veut aussi actuel que possible tandis que tout va très vite en matière d'innovation technologique. Les équipes de Data Publica et des Interconnectés ont souhaité rassembler, actualiser et partager ici des exemples de « clauses data » et de « clauses IA » qui ont été récemment adoptées par des territoires pionniers.

Ce document a été rédigé pour être accessible. Il n'est pas réservé aux grandes collectivités. Il n'est pas réservé aux juristes. Bien sûr, certains souhaiteront aller plus loin et souhaiteront décliner de façon détaillée et adaptée à chaque situation locale les éléments rassemblés ici. Et c'est tant mieux.

Mais l'ambition du présent clausier est de fournir des exemples et des repères utiles au plus grand nombre pour encadrer et garantir une utilisation de plus en plus massive mais maîtrisée des données, et permettre aux collectivités de garder le contrôle du déploiement de systèmes d'IA choisis et non subis, aussi souverains que possibles, aussi responsables que voulus, aussi transparents que nécessaires et au service de l'intérêt général.

9 · *Baromètre de L'Observatoire Data Publica 2025, Observatoire Data Publica*
https://observatoire.data-publica.eu/wp-content/uploads/2025/11/Observatoire-Data-Publica-Barome%CC%80tre-2025.pdf

10 · *Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle. Pour un résumé des dispositions du règlement : Data et IA : Les Nouvelles Règles du Jeu en Europe, 2024, Les Interconnectés*
https://www.interconnectes.com/documents/9da97714-f519-f011-8b3d-000d3a236aa0/data-et-ia-les-nouvelles-regles-du-jeu-en-europe-2024-

PARTIE 2

CLAUSIER DATA

1. GARANTIR LA SOUVERAINETÉ DE LA COLLECTIVITÉ SUR SES DONNÉES

1.1 LE STATUT DES DONNÉES DU CONTRAT

L'article L. 300-2 du Code des relations entre le public et l'administration (CRPA) définit les informations publiques ou documents administratifs comme l'ensemble des informations contenues dans les documents produits ou reçus dans le cadre d'une mission de service public, **que ce soit par l'État, les collectivités territoriales, ou toute personne publique ou privée chargée d'une telle mission.**

Sont considérés comme documents administratifs **tous les documents produits ou reçus dans le cadre d'une mission de service public.**

Il est donc expressément reconnu que les données issues de l'ensemble des services publics, y compris ceux exploités par des opérateurs privés, constituent des documents administratifs, des informations publiques ou des données publiques.

Ainsi, les données produites dans le cadre de contrats de concession ou de marchés publics sont bien des données publiques dès lors qu'elles sont issues d'une mission de service public, même si certains opérateurs privés ont pu soutenir le contraire.

CLAUSE GÉNÉRALE

Les données produites, collectées, traitées ou gérées par l'Administration ou par le contractant pour son compte dans le cadre de ses activités de service public ont le statut de « données publiques » ou de « documents administratifs ».

1.2 PROPRIÉTÉ DES DONNÉES DU CONTRAT

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 contractants de l'administration chargés de l'exploitation d'un service public.

En ce qui concerne les contrats de Concession, 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 retour 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.

En ce qui concerne 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 l'administration dispose d'un droit d'accès aux dites données tout au long de l'exécution du contrat et qu'au terme de ce dernier, lesdites données reviennent gratuitement à la personne publique dans un format ouvert dont l'Administration pourra imposer le standard et interopérable et doivent être détruites par le contractant.

CLAUSE GÉNÉRALE

Les données visées à l'article 1.1 en ce qu'elles sont nécessaires au fonctionnement du service public sont réputées appartenir à l'Administration dès l'origine.

CAS PARTICULIER DES CONCESSIONS : Les données visées à l'article 1.1 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 contractant s'engage à permettre à l'Administration d'accéder librement à ces données à tout moment de l'exécution du Contrat. À l'issue du Contrat, le contractant s'engage à remettre gratuitement à l'Administration toutes les données visées au premier alinéa du présent article et à apporter la preuve de leur destruction dans un délai de trois mois [éventuellement à ajuster/adapter en fonction de l'objet du Contrat] après le terme du Contrat. Les modalités d'accès aux dites données seront discutées entre les Parties afin que l'Administration puisse y accéder sans difficulté.

Le contractant devra apporter la preuve de leur destruction à l'Administration par le biais d'une attestation horodatée dans un délai de 24h avant le terme du Contrat.

Attention, ne pas oublier d'ajouter selon CCAG applicable : cet article s'applique par dérogation à l'article 48.2.3 du CCAG travaux / 26 et 37.2.3 du CCAG – FCS / 28, 37 et 46.2.3 du CCAG-TIC / 26, 31 et 35.2.3 du CCAG-PI / 40.2.3 du CCAG-Maîtrise d'œuvre.

1.3 HÉBERGEMENT ET CONDITIONS DE STOCKAGE DES DONNÉES DU CONTRAT

Le fait d'imposer des règles strictes imposant le stockage des données dans l'Union européenne répond aux enjeux de souveraineté européenne.

Toutefois, le principe d'un hébergement national ou encore local peut être contesté au regard du droit de la concurrence. Imposer des règles strictes liées au stockage des données en France, voire sur le territoire, peut constituer une barrière à l'entrée pour certains opérateurs.

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).

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

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

ÉVOLUTION LÉGISLATIVE EN COURS

Une proposition de loi n°2258 du 18 décembre 2025 envisage d'introduire un nouvel article dans la loi n°2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique (SREN) applicable aux régions, départements et communes dont la population est supérieure à 30.000 habitants et aux communautés urbaines, aux communautés d'agglomération ainsi qu'aux métropoles.

Il s'agit d'imposer à ces administrations, lorsque sont traitées des données d'une sensibilité particulière, de faire appel à un service d'informatique en nuage fourni par le prestataire privé mettant en œuvre des critères de sécurité et de protection des données garantissant notamment la protection des données traitées ou stockées contre tout accès par des autorités publiques d'États tiers non autorisé par le droit de l'Union européenne ou d'un État membre.

Cela ne concerne toutefois que les données d'une sensibilité particulière, au sens de la loi SREN.

TIE BREAK : UNE INITIATIVE POLITIQUE POUR LA CONSTRUCTION D'UNE SOUVERAINETÉ NUMÉRIQUE DES TERRITOIRES

Les interconnectés
RÉSEAU DES TERRITOIRES INNOVANTS

Si le sujet de la souveraineté numérique locale n'a pas encore fait l'objet d'une réponse règlementaire, certains territoires n'ont pas attendu pour agir. Rassemblées sous la bannière des Interconnectés, de France urbaine et d'Intercommunalités de France, 40 collectivités travaillent de concert pour mener le projet « Trajectoire d'indépendance européenne numérique (Tie Break) ».

Lancé en avril 2025, ce projet part du constat que 84% des solutions numériques utilisées par les collectivités ne sont pas européennes, ce qui représente une dépendance économique évaluée à 1,5 milliard d'euros… Dont l'écrasante majorité part en destination des États-Unis. La volonté des territoires de prendre leur indépendance vis-à-vis des acteurs américains est exacerbée par le retour de Donald Trump à la Maison-Blanche.

En réaction, les territoires engagés dans TIE Break ont construit un outil d'autodiagnostic en accès libre, qui permet à chaque collectivité d'évaluer son taux de dépendance aux solutions non européennes.

Plus ambitieux encore : le projet vise à constituer une bibliothèque de solutions souveraines, basées notamment sur des travaux en open source et des logiciels développés par la Dinum et l'ANCT.

Il s'agit également d'identifier comment mobiliser le levier de la commande publique, en donnant leurs chances à des entreprises françaises et européennes novatrices, là où « les cahiers des charges sont rédigés pour que des géants du numérique puissent seulement y répondre[12] » selon Caroline Zorn, vice-présidente de l'Eurométropole de Strasbourg, engagée dans la démarche. Un état de fait qui favorise les multinationales de la Silicon Valley.

Initiative ambitieuse, le projet TIE BREAK se pense au long cours. Francky Trichet, président des Interconnectés, reconnait que le travail « prendra du temps ». Mais l'ampleur de la besogne n'a d'égale que l'urgence pour les territoires de maîtriser leur souveraineté alors que le numérique devient un levier d'influence dans un contexte de relations internationales peu propice au développement de collaborations transatlantiques.

11 · *Les Interconnectés mettent le cap vers l'indépendance numérique, Localtis, 10 avril 2025, par Olivier Devillers*

En l'absence de législation nationale existante à ce sujet, la clause ci-dessous vient encadrer l'hébergement et le stockage des données du contrat.

CLAUSE GÉNÉRALE

Face aux enjeux de sécurité et de souveraineté ainsi qu'au niveau de sensibilité des données liés à l'objet du Contrat, l'Administration impose leur hébergement dans l'Union Européenne.

Le contractant devra apporter la preuve des conditions d'hébergement des données à première demande.

2. PROTÉGER LES DONNÉES

2.1 RÉGIME DE PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL

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 de traitement des données de ses propres services publics et a fortiori des données à caractère personnel. Pour le Conseil d'Etat, par exemple, 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.

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[12].

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 contractant il existera un risque juridique à ce que ce dernier se considère, 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 au contractant de l'Administration, 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…
- **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. »

À 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.

Étant précisé 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 des présentes clauses.

12 • *Conseil d'État, 12 mars 2014, n°354629.*

CLAUSE GÉNÉRALE

Dès lors que l'Administration 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, elle sera considérée comme responsable du traitement 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 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'Administration est considérée comme responsable du traitement, il reviendra au contractant, en qualité de sous-traitant, de garantir la confidentialité, l'intégrité et la disponibilité 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 contractant un quelconque droit de propriété sur lesdites données à caractère personnel.

Le contractant s'interdit de faire usage des données à caractère personnel collectées dans le cadre du Contrat aux fins de mettre en place et/ou recourir à l'intelligence artificielle.

Le contractant s'interdit, à l'expiration du présent Contrat de conserver les données visées au présent article. Le contractant devra apporter la preuve de leur destruction à l'Administration par le biais d'une attestation horodatée dans un délai de 24h avant le terme du Contrat.

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

Attention, ne pas oublier d'ajouter selon CCAG applicable : cet article s'applique par dérogation à l'article 5 du CCAG travaux / à l'article 5 du CCAG – FCS / 5 et 37 du CCAG-TIC / 5 et 31 du CCAG-PI / 5 du CCAG-MI / 5 du CCAG-MO.

2.2 PRINCIPE DE SOBRIÉTÉ DANS LA COLLECTE ET LA CONSERVATION DES DONNÉES

Dans un souci de répondre à de nouvelles préoccupations environnementales liées à un usage de plus en 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 ».

Si le droit de la commande publique a toujours été relativement peu contraignant quant à la mise en place de mesures en faveur de la sobriété numérique, plusieurs éléments récents tendent à préfigurer un infléchissement sur le sujet.

- **En premier lieu,** il convient de mentionner l'obligation d'adopter et de publier un schéma de promotion des achats publics socialement et écologiquement responsables pour les organismes acheteurs dont le montant total annuel des achats est supérieur à 100 millions d'euros hors taxes. Ce dispositif est prévu par l'article L. 2111-3 du CCP.
- **En deuxième lieu,** l'article 55 de la loi n° 2020-105 du 10 février 2020 relative à la lutte contre le gaspillage et à l'économie circulaire prévoit notamment au sein de son deuxième alinéa que :

> *« Lorsque le bien acquis est un logiciel, les administrations mentionnées au premier alinéa de l'article L. 300-2 du code des relations entre le public et l'administration promeuvent le recours à des logiciels dont la conception permet de limiter la consommation énergétique associée à leur utilisation. »*

- **En troisième lieu,** plusieurs rapports ont insisté ces dernières années sur la réduction de l'empreinte environnementale du numérique en France à travers les politiques publiques (Haut Conseil pour le Climat, Mission sénatoriale, Conseil national du numérique, ARCEP) ainsi que nombre de recommandations issues de la Convention Citoyenne pour le Climat.

Tel est également l'ambition de la loi n° 2021-1485 du 15 novembre 2021 visant à réduire l'empreinte environnementale du numérique en France.

- **En quatrième lieu,** à la suite de l'annonce par le gouvernement le 23 février 2021 d'une feuille de route « numérique et environnement » interministérielle, portée par le ministère de la Transition écologique, celui de l'Économie et le secrétaire d'État à la Transition numérique, un guide pratique a été publié le 29 avril 2021, intitulé « Guide pratique pour des achats numériques responsables ». Il contient des fiches pratiques d'achat responsable et des modèles de clauses s'adressant en priorité aux acheteurs de l'État, tout en précisant qu'il permet à tout agent public, acheteur du secteur privé ou citoyen « de trouver des ressources pour être acteur de ce changement ».
- **En dernier lieu,** depuis le 1er janvier 2025, les communes et EPCI de plus de 50 000 habitants doivent adopter une stratégie de sobriété numérique :
  - fixant des objectifs mesurables et des indicateurs de suivi,
  - couvrant notamment l'écoconception, le réemploi, la réparation, la gestion durable du matériel, la commande publique durable, et la réutilisation des données.

Sans prétendre à l'exhaustivité, une clause plus « généraliste » est proposée ci-dessous afin 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.

CLAUSE GÉNÉRALE

En fonction des projets mais également de la politique publique poursuivie par l'administration sur le sujet de la sobriété numérique, la clause suivante pourrait être insérée :

L'Administration impose à son contractant l'application d'un principe de sobriété dans la collecte et la conservation des données. L'Administration ainsi que le contractant s'engagent à collecter les seules données nécessaires à l'accomplissement des missions de service public et en limitent le stockage en volume et dans le temps.

Plus particulièrement, les Parties s'engagent à mettre en œuvre des mesures de réduction effective de l'empreinte environnementale des services numériques, conformément à la loi n°2021-1485 du 15 novembre 2021 et aux articles L. 33-16 et L. 38-5 du Code des postes et des communications électroniques.

À ce titre, elles s'engagent à :

- Réduire les émissions de gaz à effet de serre générées par les activités numériques liées au Contrat ;
- Renouveler, collecter, recycler et réemployer les équipements numériques (boîtiers de connexion, décodeurs, etc.) ;
- Développer des produits et services numériques éco-conçus, respectant le référentiel général d'écoconception (ARCEP, CSA, ADEME), notamment en matière de limitation des stratégies de captation de l'attention ;
- Publier des indicateurs clés de suivi des politiques mises en œuvre ;
- Mettre en place un mécanisme de contrôle et de suivi de la conformité des actions avec les objectifs de réduction ;
- Mener des actions de sensibilisation auprès des collaborateurs et partenaires aux usages numériques responsables.

Les Parties s'engagent à appliquer un principe de sobriété dans la collecte et la conservation des données : seules celles strictement nécessaires à l'exécution du Contrat peuvent être collectées, et leur conservation est limitée à la durée indispensable aux finalités poursuivies.

La durée de conservation de toutes les données personnelles ou non est 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 et historique).

Le contractant évalue annuellement les impacts de l'application de ce principe de sobriété dans la partie Gestion de la donnée de son rapport annuel à l'Administration qui dressera un état des lieux de la mise en œuvre de ce principe. Ce rapport détaillera notamment les modalités de conservation des données et plus particulièrement des données à caractère personnel.

2.3 SÉCURITÉ DES SYSTÈMES D'INFORMATION

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

À ce jour, et s'agissant des dernières recommandations publiées à ce sujet, il est recommandé de continuer 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 auxquelles l'acheteur public ou l'Autorité concédante peut décider de se soumettre volontairement.

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

CLAUSE GÉNÉRALE

1. Face aux enjeux de confiance, de souveraineté et de sécurité des systèmes d'information ainsi qu'au niveau de sensibilité des données liés à l'objet du Contrat, le contractant est tenu de respecter le cadre juridique applicable à la sécurité des systèmes d'information, à la sauvegarde des données et à la sécurité des acteurs critiques.

2. Conformément au cadre juridique rappelé ci-dessus, le contractant met en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque de cyberattaques.

   L'ensemble des mesures mises en œuvre sont décrites dans le cahier des normes techniques de cybersécurité fourni et mis à jour régulièrement par le contractant.

   Le contractant est notamment soumis aux obligations suivantes :

   - Obligation de prendre les mesures de sécurité nécessaires : le contractant est tenu à une obligation permanente de conseil et de mise en garde, relative aux matériels, logiciels et prestations fournies à l'Administration. Dans ce cadre, le contractant communique notamment à l'Administration toute information permettant d'améliorer le niveau de sécurité du système d'information et signale les difficultés et risques que certains choix peuvent entraîner dès lors que cette information relève des prestations objet du Contrat. Dans l'hypothèse où le contractant ne respecte pas cette obligation, il ne peut se prévaloir d'une incohérence dans le Contrat pour s'exonérer de sa responsabilité ;
   - Obligation de sensibilisation du personnel : Le contractant sensibilise son personnel, intervenant dans le cadre des prestations, à la sécurité de l'information, des systèmes d'information et à l'ensemble des mesures de sécurité définies par l'Administration ou s'imposant à ce dernier. Le contractant veille notamment à ce que son personnel intervenant dans le cadre des prestations respecte les stipulations du présent Contrat concernant la sécurité ;
   - Obligation de suivi des vulnérabilités et les incidents de sécurité détectés sur le système d'information du contractant : pour les prestations, produits et services fournis dans le cadre du Contrat, le contractant met à disposition un dispositif d'information dédié à la sécurité informatique (notamment flux RSS/ATOM, liste de diffusion par courriel ou autre). Ce dispositif vise à tenir l'Administration informée des événements et changements impactant la sécurité, notamment liés à la connaissance d'une vulnérabilité impactant le système (annonce de correctif, attaque en cours, violation de données à caractère personnel si le traitement de données est sous-traité au contractant), et des mesures correctives ou conservatoires à appliquer.

3. Le contractant s'engage à mettre à la disposition du responsable de l'Administration toutes les informations nécessaires pour démontrer le respect des obligations prévues aux textes susvisés pour permettre :

   - la réalisation d'audits, y compris des inspections, par l'Administration ou un autre auditeur qu'il a mandaté, et contribuer à ces audits ;
   - la mise en œuvre de la stratégie de sécurisation des informations de l'Administration ;
   - la coopération de l'ANSSI ou avec un cyber campus régional ;
   - une éventuelle certification (ISO 27001, SecNumCloud, etc).

3. GARANTIR LA TRANSPARENCE ET L'ACCESSIBILITÉ

3.1 LES CONDITIONS DE MISE A DISPOSITION ET DE RÉUTILISATION DES DONNÉES DU CONTRAT

S'agissant des conditions d'accès aux documents administratifs, il est prévu, aux termes de l'article L311-1 du CRPA 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).

Cela implique que la qualification d'informations publiques au sens juridique ouvre des droits :

- à l'Administration dans le cadre du contrat ;
- aux tiers / usagers du service public.

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.

Les dispositions de l'article D. 312-1-3 du code des relations entre le public et l'administration précité énonce les catégories de documents concernées.

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.

L'administration 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) (1) et celles qui n'y sont pas prévues et qui devront faire l'objet d'une homologation (2).

1 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.

2 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 :

- La description des informations publiques (données, logiciel…) dont la réutilisation doit être spécialement encadrée,
- Les raisons motivées de cette volonté d'encadrement spécifique,
- Les explications montrant l'inadéquation des licences proposées,
- Le texte de la licence souhaitée,
- 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).

CLAUSE GÉNÉRALE

La clause proposée ci-dessous pourra être précisée par l'Administration qui pourra l'adapter afin d'imposer la communication des données sous un format ouvert dont elle pourra imposer le standard.

En vue de la réutilisation des informations publiques, le contractant fournira les données gratuitement sous format ouvert, accessible et les outils et/ou méthodes permettant d'extraire et d'exploiter librement tout ou partie des données et bases de données liées à l'exécution du service public.

On entend par 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 relatives à l'exécution de la Convention.

L'Administration permettra à des tiers de réutiliser librement les données publiques diffusées sur sa plate-forme accessible à l'adresse suivante : [à compléter] et ce conformément aux dispositions du code des relations entre le public et l'administration.

Attention, ne pas oublier d'ajouter selon CCAG applicable : cet article s'applique par dérogation à l'article 48.2.3 du CCAG travaux / 26 et 37.2.3 du CCAG – FCS / 28, 37 et 46.2.3 du CCAG-TIC / 26, 31 et 35.2.3 du CCAG-PI / 40.2.3 du CCAG-Maîtrise d'œuvre.

3.2 L'INCLUSION ET L'ACCESSIBILITÉ NUMÉRIQUE

Le Référentiel Général d'Amélioration de l'Accessibilité (RGAA) met en place une obligation d'accessibilité aux services de communication au public en ligne des organismes suivants :

- **Les personnes morales de droit public ;**
- **Les personnes morales de droit privé délégataires d'une mission de service public,** ainsi que celles créées pour satisfaire spécifiquement des besoins d'intérêt général ayant un caractère autre qu'industriel ou commercial et dont :
  - Soit l'activité est financée majoritairement par une ou plusieurs personnes mentionnées aux 1° et 3° et au présent 2 de l'article 47 de la loi n° 2005-102 du 11 février 2005 pour l'égalité des droits et des chances ;
  - Soit la gestion est soumise à leur contrôle ;
  - Soit plus de la moitié des membres de l'organe d'administration, de direction ou de surveillance sont désignés par elles ;
- **Les personnes morales de droit privé constituées par une ou plusieurs des personnes** mentionnées aux 1° et 2° de l'article 47 de la loi n° 2005-102 du 11 février 2005 pour l'égalité des droits et des chances pour satisfaire spécifiquement des besoins d'intérêt général ayant un caractère autre qu'industriel ou commercial ;
- **Les entreprises à compter d'un seuil de chiffre d'affaires de 250 millions d'euros** calculé pour chaque personne sur la base de la moyenne du chiffre d'affaires annuel réalisé en France des trois derniers exercices comptables clos antérieurement à l'année considérée.

CLAUSE GÉNÉRALE

La clause proposée ci-dessous a vocation à prendre en compte les prescriptions sus-rappelées du RGAA, auquel le contractant de l'Administration doit se conformer.

Le contractant s'engage à concevoir un Outil/Projet garantissant une appropriation fluide et progressive par les Agents, ainsi que, le cas échéant, par les usagers du service public. À ce titre, il veillera à faciliter l'accès et l'utilisation de la solution livrée, notamment par la mise à disposition de supports clairs et accessibles et par la proposition de modalités d'accompagnement au changement. Le contractant s'engage à fournir un Livrable explicitant la prise en main de l'Outil/Projet (notamment via des tutos ou des "read me").

Ces actions devront s'inscrire dans le respect des orientations fixées par la feuille de route en matière d'inclusion numérique, et, le cas échéant, prévoir la formation des agents et/ou usagers conformément au plan de formation de l'Administration.

Le contractant veillera également à ce que les Livrables soient conçus dans une logique d'accessibilité, en conformité avec les recommandations du Référentiel Général d'Amélioration de l'Accessibilité (RGAA), ou tout autre cadre équivalent reconnu.

VILLE ET AGGLOMÉRATION DE LA ROCHELLE, LE CLAUSIER COMME LEVIER D'UNE POLITIQUE NUMÉRIQUE RESPONSABLE ASSUMÉE

Au sein de la Ville et de l'Agglomération de La Rochelle, le numérique est piloté par un pôle numérique responsable, mutualisé entre les deux collectivités. Nos actions sont structurées depuis 2024 autour d'une stratégie de numérique responsable et de six feuilles de route thématiques.

Chaque achat intègre systématiquement des critères environnementaux et sociaux, qui seront formalisés dans le futur SPASER (Schéma de Promotion des Achats Socialement et Écologiquement Responsables).

Pour adresser notre ambition numérique responsable, la DSI impose une annexe spécifique dans ses marchés, avec un minimum de 10 % de la notation dédiée à ces enjeux. Ces critères et clauses s'appuient notamment sur les obligations réglementaires existantes, telles que la loi AGEC et la loi REEN, et intègrent des exigences en matière de sobriété, d'impact environnemental et de responsabilité sociale.

Dans le cadre d'un marché pour la mise en accessibilité de nos sites internet, nous avons intégré audits, élaboration du schéma pluriannuel, déclarations d'accessibilité, formation des équipes et accompagnement à la mise en conformité de l'ensemble de nos services numériques. Grâce à cette démarche, nous faisons progresser notre politique d'achat en matière d'accessibilité numérique, en intégrant des exigences renforcées au bénéfice de nos usagers comme de nos agents.

Finalement, l'enjeu est (toujours) pour une DSI de bien analyser les besoins et de proposer une solution technologique adaptée et de ne pas partir trop vite vers une solution d'IA. Les processus de gouvernance, d'analyse et de gestion des besoins numériques sont encore plus essentiels qu'avant.

David BERTHIAUD
Directeur de la transformation numérique,
Ville et agglomération de La Rochelle

4. FAVORISER L'INNOVATION TERRITORIALE

4.1 RÉVERSIBILITÉ DES OUTILS TECHNOLOGIQUES

Les dispositions de l'article 38.4 du CCAG TIC définit précisément le concept de réversibilité. Elle reste néanmoins 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'enjeu 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 de territoire connecté et durable. 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 de territoire connecté et durable « 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 contractant.

CLAUSE GÉNÉRALE

N.B. : dans la mesure où la question des formats et de l'interopérabilité varie selon les secteurs et les projets, nous recommandons aux administrations d'adapter cette clause.

La réversibilité intervient lorsque la relation contractuelle cesse à son terme normal ou anticipé quelle qu'en soit la cause.

La réversibilité a pour objectif de permettre à l'Administration de récupérer l'ensemble des données et informations contenues dans les solutions développées par le contractant 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 contractant du Contrat.

Ainsi, en cas de cessation de la relation contractuelle, quelle qu'en soit la cause, le contractant s'engage à restituer gratuitement, à la première demande de l'Administration formulée par lettre recommandée avec accusé de réception et dans un délai de 4 jours à la date de réception de cette demande, l'ensemble des données du Contrat sous un format aisément réutilisable dans un environnement équivalent.

Le contractant s'engage à ce que l'Administration 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 contractant.

Attention, ne pas oublier d'ajouter si CCAG-TIC applicable : Cet article s'applique par dérogation à l'article 42 du CCAG TIC

4.2 CLAUSES DE PROPRIÉTÉ INTELLECTUELLE RENFORCÉE

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, d'un logiciel, voire d'une plateforme de territoire connecté et durable.

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 accordée 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.

De la même manière, prévoir des clauses relatives à la réversibilité permet de 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 surtout des données qui y étaient contenues.

Ces prérequis en matière de droits de propriété intellectuelle et de réversibilité ont conduit certaines collectivités à considérer qu'elles étaient titulaires des droits de propriété intellectuelle sur l'ensemble des composants, des briques logicielles et des équipements sur la base desquels est déployé le projet de territoire connecté et durable.

De cette façon, les collectivités demeurent libres ensuite de les mettre à disposition au profit de collectivités ou d'entités tierces. On parle alors d'« essaimage » de la plateforme de territoire connecté et durable.

Prévoir des clauses relatives aux droits de propriété intellectuelle permet à la collectivité de maîtriser davantage la gouvernance des données de ses contrats.

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

La rédaction de clauses relatives aux droits de propriété intellectuelle nécessitera néanmoins 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 (contrat 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 territoire connecté et durable.

Étant 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'exemples 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.

Des clauses de propriété intellectuelle renforcées doivent être prévues dès lors que le Contrat abouti à l'élaboration d'un nouvel outil technologique (plateforme, logiciel, objets connectés, maquette BIM, …) et ce afin que l'administration se préserve des droits de propriété intellectuelle afin de pouvoir librement disposer de l'outil technologique développé au terme du contrat.

Attention, les clauses qui suivent fixent essentiellement le principe applicable. En fonction du choix qui sera réalisé par l'Administration, elles nécessitent d'être complétées par un cahier des clauses de propriété intellectuelle afin de déroger aux principes figurant notamment dans les CCAG et qui ne sont pas nécessairement favorables aux administrations.

CLAUSE GÉNÉRALE

OPTION 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'Administration sous l'égide du présent Contrat.

Dès lors, les Parties conviennent ce qui suit :

- Le contractant entend céder à l'Administration, 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 contractant ne peut en aucun cas solliciter de rémunération supplémentaire.

OPTION 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'Administration et du contractant sous l'égide du présent Contrat.

Dès lors, les Parties conviennent ce qui suit :

- Le contractant entend céder à l'Administration, 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'Administration accepte que les Résultats soient exploités librement par le contractant, en dehors de [l'ensemble du territoire français / le monde entier].

Option à négocier : En contrepartie de l'investissement humain et financier de l'Administration dans la recherche et le développement des Résultats, le contractant s'engage à faire bénéficier l'Administration, à titre gracieux sous la forme d'une concession non-exclusive à durée indéterminée de tous perfectionnements et améliorations que le contractant aurait réalisé ou fait réaliser à partir de Résultats.]

Le prix de la cession est inclus dans le prix du Contrat et le contractant ne peut en aucun cas solliciter de rémunération supplémentaire.

OPTION 3

L'octroi d'une licence ou d'un droit d'usage par le contractant à l'Administration

Le contractant consent à faire bénéficier l'Administration, 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.

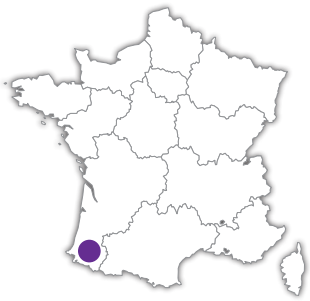
Le transfert ainsi consenti sur ces éléments comprend notamment au bénéfice de l'Administration :

- 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'Administration se réserve la possibilité de sous-licencier ou concéder tout ou partie des droits transférés par les contractants 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.

FAIRE DE LA COMMANDE PUBLIQUE UN OUTIL DE COHÉRENCE



Dans notre communauté de communes, nous disposons d'une feuille de route numérique validée au niveau politique et d'une volonté forte de faire circuler la donnée. Depuis trois ans, nous intégrons des clauses data dans nos marchés (urbanisme, déchets, médiathèque, ...). Nous visons spécifiquement à garantir l'accès aux données et l'interopérabilité des flux entre nos applications métiers et nos services partagés, notamment nos outils SIG.

Cette démarche se heurte parfois à des résistances de prestataires : on négocie, on patiente, on s'adapte pour maintenir une continuité de service. Nous travaillons désormais à systématiser ces clauses types avec le service dédié à la commande publique, afin de sensibiliser l'ensemble des agents à ces critères et d'éviter que se multiplient des outils en silos, incapables de croiser les données produites à l'échelle de la collectivité.

Au-delà de l'interopérabilité et de la réversibilité, un troisième impératif s'impose : l'agilité. Il ne suffit pas de poser des critères techniques dans les marchés. Encore faut-il aller au contact des agents pour comprendre finement leurs usages et leurs besoins réels.

C'est cette connaissance terrain qui permet ensuite d'identifier les fournisseurs véritablement alignés avec ces exigences. Cette posture d'écoute continue fait de nous des partenaires utiles, et non de simples prescripteurs de normes techniques.

Muriel HARGUINDÉGUY
Responsable de service
Statistique et information géographique,
Communauté de communes de Lacq-Orthez

PARTIE 3

CLAUSIER IA

Les clauses qui suivent en matière d'IA sont articulées autour d'un principe général (la collectivité doit pouvoir décider des usages de l'IA qui impactent la gestion du service public) et de principes spécifiques (IA et RGPD par exemple).

Elles visent à garantir la souveraineté numérique, notion qui renvoie non seulement à des enjeux nationaux et européens mais également à celui de la maîtrise des collectivités sur les données qu'elles produisent et les outils qu'elles utilisent.

Pour chaque enjeu, un rapide texte explique les raisons qui peuvent inciter à proposer une clause puis un exemple de clause est proposé.

1. LE REFUS DE L'IA SUBIE

1.1 LE STATUT DES DONNÉES DU CONTRAT

La démocratisation des outils d'IA et la course à l'innovation poussent de nombreuses entreprises à utiliser de l'IA. Lorsqu'elles travaillent pour le service public, elles ne signalent pas toujours le recours à l'IA, faisant courir de nombreux risques aux collectivités : fuite de données, atteintes à la vie privée, biais et erreurs notamment.

Ceci concerne en particulier les entreprises de service public ou les éditeurs de logiciels qui introduisent l'IA subrepticement, par le biais de mises à jour, sans que la collectivité ne consente à devenir utilisatrice du système d'IA. Mais ceci peut aussi concerner des structures de service : cabinets de conseil et bureaux d'études en particulier. La clause générale qui suit a vocation à protéger les collectivités contre le recours non sollicité (ou non validé) à l'IA.

PRINCIPE GÉNÉRAL

1 Définition

Constitue une intelligence artificielle tout outil utilisé par une machine afin de « reproduire des comportements liés aux humains, tels que le raisonnement, la planification et la créativité »(13) .

Par Intelligence Artificielle Générative, on entend un système informatique capable de générer des textes, des images, des sons, des vidéos et des modèles 3D par auto-apprentissage et capable de répondre à des interrogations en formulant une réponse sous une forme compréhensible directement par un humain.

13 • *Définition retenue par le Parlement européen*

2 Interdiction de l'Utilisation d'une IA non souveraine

De manière générale, le contractant s'engage à respecter la réglementation nationale et européenne en matière d'usage des outils d'IA.

Au titre de cette réglementation, est notamment strictement interdite toute utilisation de données de l'Administration, toute divulgation de données appartenant à l'Administration ou aux usagers du service public lors d'interactions avec un outil d'IAG non souverain, et à tout autre outil, application, service dont l'utilisation se verrait interdite.

Par outil d'IAG non souverain, la collectivité entend le recours à un outil de nature à compromettre le fonctionnement de la collectivité acheteuse et la continuité du service public par la divulgation non maîtrisée d'informations publiques sensibles et/ou leur transfert dans des pays tiers de l'Union européenne.

Une telle interdiction s'applique ainsi à tout type de données, base de données ou logiciel et quel que soit le sujet, par exemple, et sans que cela ne soit exhaustif : toute donnée financière, technologie propriété de l'Administration et/ou des usagers du service public, code de programme logiciel, droits de propriété intellectuelle, données fournisseurs et usagers.

Par ailleurs, toute utilisation de résultats d'un outil d'IA non souverain, en particulier toute intégration directe d'un résultat d'un outil d'IA non souverain dans le cadre du Contrat est strictement interdite.

En cas de non-respect du présent article, la collectivité se réserve le droit de résilier le contrat pour manquement aux obligations du présent Contrat. La collectivité se réserve également le droit d'engager des poursuites pénales et de demander des dommages et intérêts en raison du préjudice subi.

3 Demande d'agrément en cas d'utilisation d'une IA souveraine dans le cadre du contrat

Tout recours à un Système d'IA Souverain par le contractant est subordonné à l'autorisation exprès, écrite et préalable de la collectivité.

Le contractant s'engage à fournir toutes les informations concernant le système d'IA permettant à la collectivité de comprendre et de maîtriser son fonctionnement : données d'entraînement, modèle utilisé, lieu d'hébergement et outils de calcul…

Le contractant devra soumettre à la collectivité une demande justifiée présentant les bénéfices de l'utilisation dudit Système d'IA pour l'exécution du Contrat et l'absence d'alternative non basées sur l'IA. En particulier, le contractant devra garantir à la collectivité une intervention humaine dans le processus d'utilisation d'un Système d'IAG.

La collectivité disposera d'un délai de 15 jours pour examiner la demande. En l'absence de réponse à l'issue de ce délai, la demande sera réputée refusée.

Si le contractant souhaite recourir à un système d'IA en cours de contrat, il devra en informer la collectivité sans délai. La collectivité se réserve le droit de s'opposer à l'utilisation dudit Système d'IA.

4 Garanties en cas d'utilisation d'une IAG souveraine dans l'exécution du contrat

Le contractant garantit à la collectivité que les éléments fournis par celui-ci et notamment les Livrables ne comportent aucun élément susceptible d'être considéré comme contrefaisant ou portant atteint à un droit de propriété intellectuelle ou industrielle.

De la même manière, le contractant ne pourra faire usage des données à caractère personnel collectées dans le cadre de l'exécution du Contrat afin de recourir à de l'IA.

Le contractant garantit en conséquence la collectivité contre tout réclamation ou recours d'un tiers, en ce compris toute conséquence financière liée à de telles réclamations ou de tels recours.

Pour toutes questions ou préoccupations concernant l'utilisation appropriée des outils d'IA générative, ceux validés par l'Administration et ceux qui ne le seraient pas encore, le contractant pourra contacter le délégué à la protection des données de l'Administration

2. CLAUSES GÉNÉRALES

Le règlement sur l'intelligence artificielle[14] impose de nouvelles obligations en matière de conception et d'utilisation d'outils d'intelligence artificielle. Ces obligations sont opposables aux fournisseurs mais aussi aux utilisateurs de ces systèmes. Elles portent sur les données utilisées pour entraîner les modèles, sur le contrôle humain ou encore sur certains usages spécifiques (qualifiés à « hauts risques ») ou pour l'IA générative.

CLAUSES GÉNÉRALES

2.1 Garantie sur les données d'entraînement

Le contractant s'engage à mettre en œuvre un processus garantissant l'absence de biais dans les données d'entraînement, de validation et de test. Il se porte garant de la qualité et de l'exactitude des données d'entraînement.

2.2 Exigences de sécurité

Le contractant s'engage à se conformer aux exigences de sécurité posées par l'article 32 du RGPD et l'article 15 du règlement sur l'intelligence artificielle. Il informe la collectivité des certifications de sécurité dont il dispose et s'engage à les maintenir tout au long de l'exécution du Contrat.

L'enjeu de la cybersécurité en matière d'IA est étroitement lié à la sécurité des données. Ainsi, cette clause s'ajoute à celle prévue au point 2.3 de la partie 2 du présent clausier.

2.3 La nécessité d'un contrôle humain

Le système d'IA doit être conçu de façon à permettre un audit du système, pour chacune de ses finalités. Le prestataire doit être en mesure d'expliquer, sur demande, le fonctionnement de son système aux agents de la collectivité.

2.4 Explicabilité et transparence des systèmes d'IA

Quel que soit le système d'intelligence artificielle utilisé dans le cadre du contrat, le contractant s'engage à mettre préalablement à la disposition de la collectivité les éléments suivants :

Système de gestion des risques mis en œuvre

Description du système d'enregistrement des événements

Documentation technique du modèle décrite à l'article 11 du règlement européen sur l'intelligence artificielle

2.5 Explicabilité et transparence des systèmes d'IA générative

Le contractant s'engage, lorsque le système qu'il fournit relève de la catégorie des modèles d'IA à usage général tels que définis par l'article 3, point 63 du Règlement sur l'intelligence artificielle, à mettre à disposition de la collectivité une description du processus d'entraînement du modèle et des données d'entraînement, conformément au modèle fourni par le bureau de l'IA(15).

2.6 Évolutivité des systèmes d'IA

Compte tenu du caractère évolutif des Systèmes d'IA, le contractant s'engage à transmettre à la collectivité, notamment, toute mise à jour, évolution, ou tout changement apporté audit système d'IA et ce dès qu'il en a connaissance.

En cas de non-respect de cette obligation, la collectivité pourra mettre un terme à l'utilisation du système d'IA concerné.

14 · *Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle*

15 · https://digital-strategy.ec.europa.eu/fr/policies/ai-office

2.7 Obligations au terme du contrat

A l'issue du Contrat, le contractant devra remettre à la collectivité une documentation technique comprenant le descriptif détaillé des environnements techniques matériels et logiciels de développement, d'intégration et, le cas échéant, de fonctionnement ainsi que les documentations techniques de développement et de maintenance correspondantes.

En tout état de cause, le contractant s'engage à mettre en œuvre un contrôle effectif par des personnes physiques qui soit proportionné aux risques associés au système.

COMMUNAUTÉ D'AGGLOMÉRATION DE PARIS-SACLAY : DES CLAUSES QUI FONT LEURS PREUVES, JUSQUE DANS LES BUDGETS

L'agglomération a structuré sa stratégie numérique autour d'une Charte des données (2022) et d'une feuille de route IA (2024). Ces documents sont déclinés en ressources cadres à disposition des agents (règlement intérieur, guides managériaux et pratiques). C'est sur ce socle qu'a été coconstruit, fin 2025, un clausier numérique impliquant la direction numérique et la commande publique.

Le clausier couvre plusieurs impératifs : réversibilité, interopérabilité, localisation des données, transparence algorithmique, encadrement du recours à l'IA par les prestataires. Une clause sur l'IA frugale vise également à maîtriser l'empreinte environnementale des solutions retenues, même si son application concrète reste à ce stade difficile à mobiliser.

Sur le terrain, nous avons vu plusieurs avantages. Dans le cadre d'un projet de prévention des inondations, la clause de transparence algorithmique a contraint le prestataire à documenter et justifier ses modèles de calcul. Une exigence précieuse pour rendre compte des décisions techniques aux citoyens. Sur le suivi du PCAET, la convention de partenariat avec un institut de recherche a été encadrée pour garantir la récupération des modes de calcul en open data. Quant à la clause de sobriété des données, en limitant les volumes collectés et stockés, elle a généré des économies directes sur les coûts d'hébergement. Un argument concret pour convaincre les directions métiers de s'en saisir.

Finalement, l'enjeu n'est pas tant la rédaction des clauses que les processus qui les font vivre et la sensibilisation pour emporter l'adhésion en interne.

Alice BERKATE
Juriste Numérique / DPD
Direction Enjeux numériques et innovation territoriale,
Communauté d'agglomération de Paris Saclay

3. LES CLAUSES RGPD APPLICABLES EN CAS DE RECOURS À L'IA

Le traitement de données par des outils d'intelligence artificielle fait émerger de nouvelles préoccupations en matière de protection des données à caractère personnel.

Un processus de conformité au RGPD robuste peut en effet être remis en cause par l'utilisation d'IA au sein des collectivités, qui constituent de nouveaux traitements de données complexes. Ces clauses, à jour des dernières recommandations de la CNIL, visent à encadrer ces risques au sein des outils d'IA commandés par les collectivités.

Ces clauses ont vocation à s'ajouter à la clause sur la protection des données prévue au point 2.1 de la partie 2 du présent clausier ainsi qu' à l'annexe relative à la répartition des responsabilités dans le cadre du dispositif de protection des données à caractère personnel lorsque le contrat porte, tout ou partie, sur la fourniture ou l'utilisation d'un système d'IA.

3.1 RESPONSABILITÉ DE TRAITEMENT

Lorsqu'un système d'intelligence artificielle est fourni à la collectivité ou utilisé par un prestataire de services pour le compte de la collectivité, celle-ci constitue un responsable de traitement au regard du RGPD. En conséquence, elle est responsable de la mise en conformité du système.

Pour autant, le contractant pourra recevoir la qualification de sous-traitant s'il est amené à traiter des données personnelles. Le RPGD, en son article 28, lui impose alors des obligations particulières de transparence, de prise en compte des exigences de protection des données par défaut mais également d'alerte et de conseil envers la collectivité. Cela nécessite alors une collaboration durable et loyale entre le prestataire et la collectivité.

Le RGPD impose également de définir par un contrat de sous-traitance une répartition des rôles entre collectivités et prestataires. Un modèle de contrat de sous-traitance est inclus en annexe.

CLAUSE GÉNÉRALE

En fonction des opérations réalisées par le contractant, celui-ci ou ses prestataires pourront être qualifiés de sous-traitant au sens du RGPD.

Dans ces cas, le contractant s'engage à collaborer loyalement avec la collectivité pour définir leurs responsabilités afin d'assurer la conformité avec la réglementation applicable en matière de protection des données à caractère personnel.

3.2 CONFORMITÉ DES DONNÉES D'ENTRAÎNEMENT

L'entraînement des systèmes d'IA nécessite de constituer une grande base de données. Lorsque celle-ci inclut des données personnelles, il est nécessaire de s'assurer du respect des grands principes du RGPD. Une attention particulière est à porter à l'existence d'une finalité déterminée, prévue à l'article 5b du RGPD, qui dispose que les données personnelles collectées par un opérateur ne pourront être utilisées que pour un objectif déterminé à l'avance. Ce principe est mis en péril dans la mesure où nombre de fabricants d'IA sont tentés de récupérer des données personnelles récoltées à d'autres fins que la conception du système afin de faciliter son entraînement.

A ce sujet, la CNIL considère que l'entraînement d'une IA peut être justifié par la finalité prévue pour le déploiement du système[16]. Par ailleurs, les données d'entraînement doivent se cantonner à celles qui sont nécessaires au bon fonctionnement du système, en application du principe de minimisation des données. Cette clause transcrit ces exigences de conformité au RGPD, propres aux systèmes d'IA.

16 • *Fiches pratiques IA de la CNIL, fiche n° 2 : définir une finalité* https://www.cnil.fr/fr/definir-une-finalite-0

CLAUSE SUR LE RGPD ET LES DONNÉES D'ENTRAÎNEMENT

Le contractant s'assure de la compatibilité de la finalité de la récolte des données à caractère personnel utilisées dans l'élaboration du système avec l'entraînement du système d'intelligence artificielle.

Le contractant applique le principe de minimisation prévu par l'article 5, c) du Règlement général sur la protection des données dans la constitution de la base de données d'entraînement.

3.3 TRANSFERT DES DONNÉES

Les fournisseurs de systèmes d'IA peuvent être amenés, dans le cadre du contrat conclu avec la collectivité, à avoir accès à des données personnelles. C'est notamment le cas lorsque les agents de la collectivité ou ses administrés sont utilisateurs d'un système d'IA opéré par le contractant, et lui transmettent des données personnelles dans le cadre de leur utilisation.

Dans ces cas, il est impératif que ces données personnelles restent entre les seules mains des personnes autorisées à y avoir accès, dans la limite des finalités de traitement. Tout transfert de données à un tiers est alors proscrit, sauf exception prévue par le contrat de sous-traitance dans le respect du RGPD.

CLAUSE SUR LE TRANSFERT DES DONNÉES

Le contractant s'interdit tout transfert des données des utilisateurs du système d'IA à des tiers, sauf accord préalable de la collectivité.

3.4 INFORMATION DES PERSONNES CONCERNÉES

Les collectivités qui traitent des données à caractère personnel doivent informer chaque personne concernée de l'utilisation de leurs données, dans les conditions prévues aux articles 13 et 14 du RGPD. Ce principe s'applique notamment lorsqu'une intelligence artificielle est entraînée sur une base de données incluant des données personnelles des administrés.

L'information doit en principe être donnée individuellement à chaque personne. Par exception, la CNIL prévoit que si l'information individuelle requiert des efforts disproportionnés, la collectivité pourra se contenter de rendre publique l'information exigée[17], par exemple sur son site internet.

CLAUSE SUR L'INFORMATION DU PUBLIC

Lorsque le système a été entraîné ou testé sur des données à caractère personnel issues d'usagers du service public, le contractant s'engage, avec l'aide de la collectivité, à informer les personnes concernées :

- Du traitement de leurs données
- De la durée de conservation de ces données
- De la finalité et de la base légale du traitement
- Du ou des destinataires des données
- De leurs droits d'accès, de rectification, d'effacement, à la limitation, portabilité et d'opposition
- De leur droit d'introduire une réclamation auprès de la CNIL

17 • *Fiches pratiques IA de la CNIL, fiche n° 9 : informer les personnes concernées*
https://www.cnil.fr/fr/ia-informer-les-personnes-concernees

4. PRÉSERVATION DES DROITS DE PROPRIÉTÉ INTELLECTUELLE

Les intelligences artificielles mettent au défi la régulation en matière de propriété intellectuelle de deux manières.

Dans un premier temps, au stade de la conception des systèmes : la quantité massive de données ingérée par les intelligences artificielles dans le cadre de leur apprentissage pousse fréquemment les fabricants à utiliser des données couvertes par des droits d'auteurs.

Dans un second temps, au stade de l'utilisation de l'intelligence artificielle par la collectivité : la question de la titularité des droits de propriété intellectuelle des résultats produits par le système se pose.

Ces clauses visent à réduire ces risques.

Ces clauses ont vocation à s'ajouter à la clause sur la répartition des droits de propriété intellectuelle prévue au point 4.2 de la partie 2 du présent clausier lorsque le contrat porte, tout ou partie, sur la fourniture ou l'utilisation d'un système d'IA.

4.1 PROPRIÉTÉ INTELLECTUELLE DES DONNÉES D'ENTRAÎNEMENT

La question du respect des droits d'auteurs lors de l'entraînement d'un système d'IA fait couler beaucoup d'encre, dans la mesure où la réglementation n'offre pas à ce jour de cadre clair et précis. Le règlement sur l'intelligence artificielle à son article 53 exige des fabricants d'IA générative qu'ils mettent en place une politique de respect des droits d'auteurs, sans pour autant en préciser la méthode et les contours.

Le Conseil supérieur de la propriété littéraire et artistique, instance rattachée au ministère de la Culture et auteur d'un rapport sur le sujet, relève qu'en matière d'IA « la collecte et l'exploitation des données revêtent une importance majeure, mais s'effectuent dans des conditions qui ne garantissent pas le respect des valeurs et du droit de l'UE[18] ». Pour répondre à ces enjeux, la ministre de la Culture a organisé en juin 2025 une concertation entre représentants de fournisseurs d'IA et représentants d'ayants droit, afin d'identifier des pistes d'évolution de la législation[19]. Cette logique s'inspire de la pratique américaine, où de grands représentants d'ayant droit tels que Sony, Warner ou Universal ont commencé à conclure des accords avec des fabricants d'IA pour encadrer les conditions dans lesquelles les œuvres dont ils détiennent les droits peuvent servir à entraîner des systèmes d'IA.

En France, la possibilité d'utiliser des matériaux protégés par droit d'auteur pour l'entraînement de systèmes d'IA et les conditions qui permettent de le faire restent incertaines en l'absence de décisions de justice. La clause suivante vise à protéger les collectivités en développant une interprétation prudente du droit de la propriété intellectuelle.

CLAUSE SUR LA PROPRIÉTÉ INTELLECTUELLE ET LES DROITS D'AUTEUR

Le contractant s'engage à ne pas utiliser, pour l'entraînement de son système, de matériaux protégés par un droit d'auteur ou un droit de propriété industrielle, à moins de disposer des autorisations nécessaires à leur exploitation.

Le contractant s'engage à informer la collectivité de la présence de données et d'informations protégées par le droit d'auteur ou des droits de propriété industrielle dans la base de données d'entraînement du système, sur la base d'un modèle de résumé lisible et complet.

Pour cela, le contractant pourra utiliser le modèle de résumé établi par le rapport de mission relative à la mise en œuvre du règlement européen sur l'intelligence artificielle adopté par le Conseil supérieur de la propriété littéraire et artistique(20) ou tout autre outil à l'état de l'art.

18 · Rapport de mission relative à la mise en œuvre du règlement européen établissant des règles harmonisées sur l'intelligence artificielle, Conseil supérieur de la propriété littéraire et artistique, décembre 2024

19 · Concertation entre fournisseurs d'IA et ayants droit : un espace de dialogue et de négociation structuré mais un partage de la valeur encore insuffisant, Communiqué de presse, ministère de la Culture

20 · Disponible en annexe, page 37

4.2 RÉPARTITION DES DROITS DE PROPRIÉTÉ INTELLECTUELLE SUR LES RÉSULTATS DU SYSTÈME

Lorsque les agents ou les élus d'une collectivité génèrent du contenu à l'aide d'une intelligence artificielle, la question de savoir qui de la collectivité ou du fabricant du système est titulaire des droits sur le document peut se poser.

Ces clauses visent à clarifier la répartition des droits de propriété intellectuelle sur les contenus générés par intelligence artificielle et à reconnaître des droits pour la collectivité dont les données ont servi à produire de la valeur.

CLAUSE GÉNÉRALE SUR LA PROPRIÉTÉ INTELLECTUELLE DE LA COLLECTIVITÉ

OPTION 1

Cession de droits

Le contractant cède sur le territoire [français/européen] et pour une durée indéterminée, des droits de propriété intellectuelle sur les résultats du système [à titre exclusif / à titre non exclusif]. Le prix de la cession est inclus dans le prix du contrat.

La collectivité récupère l'ensemble des données et informations la concernant qui ont été fournies au système d'IA ou produites par ce dernier à la fin du Contrat.

La collectivité sera susceptible de mettre ces données en open data, dans les limites prévues par le code des relations entre le public et l'administration.

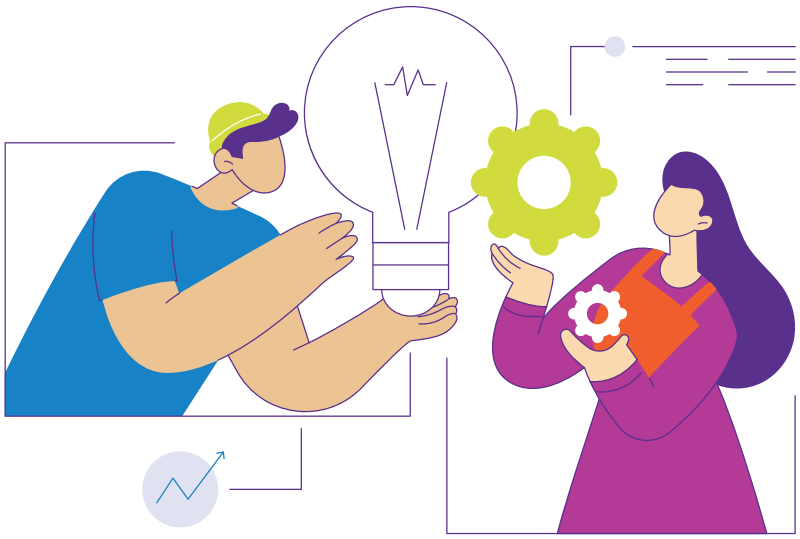
OPTION 2

Octroi d'une licence

Le contractant accorde, pendant la durée du Contrat et sans contrepartie financière, une licence d'utilisation des droits de propriété intellectuelle dont il est titulaire.

Cette licence d'utilisation comprend :

- Le droit de reproduire, 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



5. CLAUSES DIVERSES

Lorsqu'elles adoptent des doctrines IA, les collectivités prennent souvent des engagements plus volontaristes que la loi (actuelle). Ces engagements, pour être opérationnels, doivent être intégrés dans les contrats de la commande publique.

Ces clauses visent à fournir des outils pour différents types d'engagements éthiques fréquemment pris par les collectivités engagées dans des démarches de chartes ou de stratégies d'intelligence artificielle.

5.1 EXPÉRIMENTATIONS CONDUISANT À LA MISE EN PLACE DE SYSTÈMES D'IA DANS LE CADRE DU CONTRAT

Les collectivités peuvent, avant de déployer une intelligence artificielle à grande échelle, effectuer des tests des systèmes d'intelligence artificielle. Ces expérimentations, qui vont concerner un nombre restreint d'agents, devront cependant être encadrées et respecter la réglementation en matière de protection des données personnelles, d'encadrement des intelligences artificielles et de respect des droits de propriété intellectuelle.

Cette clause s'applique à ces phases d'expérimentation et impose au contractant de respecter un protocole spécifique aux besoins de la collectivité, qui sera déterminé avec cette dernière.

CLAUSE SUR LES EXPÉRIMENTATIONS

Dans l'hypothèse où les parties souhaiteraient expérimenter des Systèmes d'intelligence artificielle dans le cadre du Contrat, elles s'engagent par un protocole à définir ensemble les conditions de la mise en œuvre de tels dispositifs, de leur évaluation et de leur déploiement.

Le modèle de protocole et sa méthodologie d'élaboration seront fournis à la collectivité avant la mise en œuvre de toute expérimentation.

Le contractant s'engage, en cas d'utilisation approuvée par l'Administration de Systèmes d'IA à respecter l'ensemble des obligations imposées par la collectivité.

Étant précisé que dans l'hypothèse où une expérimentation dans le cadre d'un contrat public nécessiterait de déroger à l'un ou l'autre des principes du Contrat, le protocole encadrera la dérogation. Il limitera notamment la durée de conservation des données.

5.2 IMPACT ENVIRONNEMENTAL

Les outils d'intelligence artificielle ont une empreinte environnementale importante, due notamment à la quantité d'électricité nécessaire à leur fonctionnement mais également à l'eau potable utilisée pour refroidir les serveurs. À ce sujet, la loi REEN[21] impose aux collectivités de plus de 50 000 habitants d'établir une stratégie numérique responsable. Cependant, même pour les territoires qui ne sont pas soumis à cette obligation, l'impact du recours à des IA sur ses politiques en matière de transitions écologique est à prendre en compte.

De nombreuses initiatives dites d'« IA frugales » visent à réduire l'impact écologique des systèmes d'IA. Parmi celles-ci, le Référentiel général pour l'IA frugale publié par l'AFNOR[22] fait autorité. Il prévoit des mesures organisationnelles et techniques à mettre en œuvre pour réduire l'empreinte environnementale des systèmes. D'autres outils, tels que le calculateur green algorithms[23], permettent d'estimer l'empreinte écologique des systèmes d'intelligence artificielle, pour le mettre en balance avec les gains espérés.

La clause suivante impose au fabricant de réduire l'empreinte environnementale du système d'IA fourni et de transmettre une évaluation du coût environnemental du système à la collectivité.

21 · *Loi n° 2021-1485 du 15 novembre 2021 visant à réduire l'empreinte environnementale du numérique en France*

22 · *https://www.ecologie.gouv.fr/presse/publication-du-referentiel-general-lia-frugale-sattaquer-limpact-environnemental-lia*

23 · *https://calculator.green-algorithms.org/*

CLAUSE SUR L'IMPACT ENVIRONNEMENTAL

Le contractant s'engage à respecter les prescriptions du référentiel général pour l'IA frugale.

Les Parties conviennent que le niveau des engagements relatifs à l'IA frugale applicable au contractant sera déterminé en fonction des spécificités du Contrat.

En vertu de la méthodologie d'évaluation et de communication définie par le référentiel générale pour l'IA frugale, le contractant veille à utiliser l'IA de manière efficiente et raisonnée, en tenant compte des efforts nécessaires et des bénéfices attendus.

De surcroît, il s'efforce de prendre en considération les principaux impacts environnementaux de ses solutions tout au long de leur cycle de vie et s'engage à communiquer de façon claire sur ces sujets, en favorisant des pratiques responsables.

Le contractant s'engage également à fournir une évaluation de l'impact environnemental du système sur la base d'indicateurs ou de méthodes définis par la collectivité.

OPTION 1

Le contractant s'engage à fournir une pesée du système, à l'aide d'un outil à définir de type green algorithms *https://www.green-algorithms.org/*

OPTION 2

Le contractant s'engage à fournir les données concernant le système d'IA permettant à la collectivité de réaliser une pesée du système (à l'aide d'un outil à définir de type green algorithms) : données d'entraînement, modèle utilisé, lieu d'hébergement et outils de calcul…

5.3 EXISTENCE D'UNE VOIE DE RECOURS ALTERNATIVE

Les systèmes d'intelligences artificielles utilisés comme des outils d'aide à la décision publique peuvent commettre des erreurs. Celles-ci peuvent être dues à un mauvais entraînement du système ou résulter de son utilisation, par exemple lorsque le prompt n'est pas suffisamment précis ou n'inclut pas l'ensemble des éléments fondant la réponse.

Il est nécessaire que les usagers du service public puissent, dans ces hypothèses, demander le réexamen de leur situation sans qu'un outil d'intelligence artificielle soit utilisé. Cette clause vise à imposer cette exigence aux prestataires utilisant de l'IA dans le cadre de délégations de service public.

CLAUSE SUR L'EXISTENCE D'UNE VOIE DE RECOURS ALTERNATIVE

Dans l'ensemble des hypothèses où le contractant est susceptible de prendre des décisions assistées par IA de nature à affecter des usagers du service public, il s'engage à mettre en place une voie de recours permettant le réexamen des décisions par des personnes physiques en excluant tout recours à des systèmes d'IA.

5.4 NON-DISCRIMINATION

Les systèmes d'intelligence artificielle peuvent, en fonction de la façon dont ils sont entraînés, porter des biais qui risquent, dans le pire des cas, de générer des discriminations en fonction des bénéficiaires du système.

Lorsque les systèmes d'intelligence artificielle sont utilisés au bénéfice des usagers du service public, ce risque de discrimination doit être identifié et corrigé. Cette clause vise à engager la responsabilité du contractant en cas de présence avérée d'un risque de discrimination dans l'IA fournie à la collectivité ou utilisée pour son compte.

CLAUSE SUR LES BIAIS ET LES RISQUES DE DISCRIMINATION

Le contractant s'engage à mettre à disposition un système d'IA qui a été conçu de manière à ne pas discriminer l'utilisateur ou le bénéficiaire indirect du système selon son profil socio-économique réel ou présumé, et notamment en prenant en considération son genre, son origine ethnique, ses opinions politiques, son appartenance syndicale, son état de santé, son orientation sexuelle ou sa religion.

BORDEAUX MÉTROPOLE : LA COMMANDE PUBLIQUE POUR UN NUMÉRIQUE CHOISI

Bordeaux Métropole opère aujourd'hui un service numérique mutualisé pour 19 communes sur le territoire. En septembre 2023, la collectivité s'est dotée d'une politique numérique engagée qui vise à «agir pour un numérique choisi et non subi». L'ambition politique : garantir un juste équilibre entre la valeur des services numériques déployés et leurs impacts sociaux, éthiques et environnementaux. Sur l'IA, une démarche structurée est constituée et animée autour de quatre axes : Dialoguer, Former, Encadrer, Expérimenter. En décembre 2025, un cadre éthique et responsable en matière d'IA a été adopté, cadre fixant des lignes rouges et engagements pris dans la construction et utilisation en confiance d'IA.

Sur le volet achat, depuis 2025, un clausier data est constitué et positionné au sein des marchés pour garantir avec les fournisseurs la structuration des formats et modalités de partage de données. Sur l'IA, le clausier couvre, à date, deux dimensions : l'acquisition directe de solutions IA et tous services numériques qui intègrent ou vont intégrer demain de l'IA. Il décline sur le fond le cadre politique éthique et responsable IA en vigueur.

Le clausier n'est pas un empilement de clauses. Intégré à nos marchés, il se présente comme un mode d'emploi pour une IA de confiance. Il vise à préserver la maîtrise des décisions de la collectivité, à protéger les données comme bien commun, et à encourager transparence, explicabilité et sobriété numérique. Partagé dès le sourcing, il devrait aider à aligner les attentes, apprécier la maturité des offres et structurer les échanges avec les fournisseurs et éditeurs.

Jon HAUET
Chargé de mission Intelligence Artificielle au sein de Bordeaux Métropole

ANNEXE 1

MODÈLE D'ANNEXE RELATIVE À LA RÉPARTITION DES RESPONSABILITÉS DANS LE CADRE DU DISPOSITIF DE PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL

N.B : *Ce modèle d'annexe comporte une mise à jour issue de la décision d'exécution de la Commission n°2021/915 du 15 juin 2021 implémentant les clauses contractuelles types* [24]

ARTICLE 1 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 »).

ARTICLE 2 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]

Contacts pour l'exécution de cette annexe :

- Courriel du DPO : xxx@xxx.xx ;
- Contact du RSSI : xxx@xxx.xx

24 • Décision d'exécution (UE) 2021/915 de la Commission du 4 juin 2021 relatives aux clauses contractuelles types entre les responsables de traitement et les sous-traitants au sens de l'article 28, paragraphe 7, du règlement (UE) 2016/679 du Parlement européen et du Conseil et de l'article 29, paragraphe 7, du règlement (UE) 2018/1725 du Parlement européen et du Conseil.

Cette décision est venue mettre à jour les modèles de clauses contractuelles par la publication de deux nouvelles séries de clauses contractuelles types (CCT).

La première série de clauses contractuelles types est destinée à encadrer les transferts de données des responsables de traitement ou des sous-traitants de l'UE/EEE (soumis au RGPD) à des responsables de traitement ou des sous-traitants établis en dehors de l'UE/EEE.

La seconde série de clauses contractuelles types vise à encadrer les relations entre les responsables de traitement et leurs sous-traitants au sein de l'UE.

Ainsi, par cette décision, à compter du 27 décembre 2022, les anciennes clauses contractuelles types de la Commission ne pouvaient plus être utilisées.

ARTICLE 3 Obligations du sous-traitant vis-à-vis du responsable de traitement

3.1 - Engagements 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. Transferts internationaux :

a) Tout transfert de données vers un pays tiers ou une organisation internationale par le sous-traitant n'est effectué que sur la base d'instructions documentées du responsable du traitement ou afin de satisfaire à une exigence spécifique du droit de l'Union ou du droit de l'État membre à laquelle le sous-traitant est soumis et s'effectue conformément au chapitre V du règlement (UE) 2016/679 ou du règlement (UE) 2018/1725 ;

b) Le responsable du traitement convient que lorsque le sous-traitant recrute un sous-traitant ultérieur conformément à la clause 7.7 pour mener des activités de traitement spécifiques (pour le compte du responsable du traitement) et que ces activités de traitement impliquent un transfert de données à caractère personnel au sens du chapitre V du règlement (UE) 2016/679, le sous-traitant et le sous-traitant ultérieur peuvent garantir le respect du chapitre V du règlement (UE) 2016/679 en utilisant les clauses contractuelles types adoptées par la Commission sur la base de l'article 46, paragraphe 2, du règlement (UE) 2016/679, pour autant que les conditions d'utilisation de ces clauses contractuelles types soient remplies ;

11. L'obligation de veiller à ce que les données à caractère personnel soient exactes et à jour, en informant sans délai le responsable du traitement si le sous-traitant apprend que les données à caractère personnel qu'il traite sont inexactes ou sont devenues obsolètes ;

11 L'obligation d'assister le responsable de traitement lorsque ce dernier fait l'objet de demandes directes de la part d'usagers du service public concerné.

3.2 - 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 21 jours 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.

3.3 - 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.

3.4 - 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, après l'en avoir informé 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.

3.5 - 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 courriel. 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. Cette notification est adressée par mail au DPD [nom du DPD de l'Administration concernée] (xxx@xxxx.xx) et au RSSI [nom du RSSI de l'Administration concernée] de (xxx@xxxx.xx).

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.

3.6 - 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.

3.7 - Mesures de sécurité

a 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 :

- a) la pseudonymisation et le chiffrement des données à caractère personnel ;
- b) des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;
- c) 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 ;
- d) 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.

b 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 si cela est possible et/ou s'il existe].

[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].

Les mesures techniques et organisationnelles doivent faire l'objet d'une description concrète, et non pas générique visant à garantir un niveau de sécurité approprié, compte tenu de la nature, de la portée, du contexte et de la finalité du traitement, ainsi que des risques pour les droits et libertés des personnes physiques.

À titre d'illustration, ci-dessous quelques exemples de mesures possibles :

- mesures de pseudonymisation et de chiffrement des données à caractère personnel ;
- mesures visant à garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;
- mesures assurant de disposer de 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 ;
- procédures visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement ;
- mesures d'identification et d'autorisation de l'utilisateur ;
- mesures de protection des données pendant la transmission ;
- mesures de protection des données pendant le stockage ;
- mesures visant à garantir la sécurité physique des sites où les données à caractère personnel sont traitées ;
- mesures visant à garantir l'enregistrement des événements ;
- mesures visant à assurer la configuration des systèmes, y compris la configuration par défaut ;
- mesures de gouvernance et de gestion de l'informatique interne et de la sécurité informatique ;
- mesures de certification/assurance des procédés et produits ;
- mesures visant à garantir la minimisation des données ;
- mesures visant à garantir la qualité des données ;
- mesures visant à garantir une conservation limitée des données ;
- mesures visant à garantir la responsabilité ;
- mesures permettant la portabilité des données et garantissant l'effacement.

3.8 - 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.

3.9 - 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.

3.10 - 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.

3.11 - 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.

ARTICLE 4 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

ARTICLE 5 Non-respect des clauses et résiliation

1. Sans préjudice des dispositions du règlement (UE) 2016/679 et/ou du règlement (UE) 2018/1725, en cas de manquement du sous-traitant aux obligations qui lui incombent en vertu des présentes clauses, le responsable du traitement peut donner instruction au sous-traitant de suspendre le traitement des données à caractère personnel jusqu'à ce que ce dernier se soit conformé aux présentes clauses ou jusqu'à ce que le contrat dont il est titulaire soit résilié. Le sous-traitant informe rapidement le responsable du traitement s'il n'est pas en mesure de se conformer aux présentes clauses, pour quelque raison que ce soit.
2. Le responsable du traitement est en droit de résilier le contrat dans la mesure où il concerne le traitement de données à caractère personnel conformément aux présentes clauses si :
    - le traitement de données à caractère personnel par le sous-traitant a été suspendu par le responsable du traitement conformément au point a) et le respect des présentes clauses n'est pas rétabli dans un délai raisonnable et, en tout état de cause, dans un délai d'un mois à compter de la suspension ;
    - le sous-traitant est en violation grave ou persistante des présentes clauses ou des obligations qui lui incombent en vertu du règlement (UE) 2016/679 et/ou du règlement (UE) 2018/1725 ;
    - le sous-traitant ne se conforme pas à une décision contraignante d'une juridiction compétente ou de l'autorité de contrôle compétente/des autorités de contrôle compétentes concernant les obligations qui lui incombent en vertu des présentes clauses ou du règlement (UE) 2016/679 et/ou du règlement (UE) 2018/1725.

3. Le sous-traitant est en droit de résilier le contrat dans la mesure où il concerne le traitement de données à caractère personnel en vertu des présentes clauses lorsque, après avoir informé le responsable du traitement que ses instructions enfreignent les exigences juridiques applicables conformément à la clause 7.1, point b), le responsable du traitement insiste pour que ses instructions soient suivies.
4. À la suite de la résiliation du contrat, le sous-traitant supprime, selon le choix du responsable du traitement, toutes les données à caractère personnel traitées pour le compte du responsable du traitement et certifie auprès de celui-ci qu'il a procédé à cette suppression, ou renvoie toutes les données à caractère personnel au responsable du traitement et détruit les copies existantes, à moins que le droit de l'Union ou le droit national n'impose de les conserver plus longtemps. Le sous-traitant continue de veiller à la conformité aux présentes clauses jusqu'à la suppression ou à la restitution des données.

ANNEXE 2

MODÈLE D'ANNEXE RELATIVE À LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

N.B : *Ce modèle d'annexe proposé à l'ANSSI est inspiré du modèle de cahier des charges pris par arrêté du 18 septembre 2018 portant approbation du cahier des clauses simplifiées de cybersécurité*[25].

Elle nécessite donc d'être mise à jour car l'arrêté susvisé a désormais 5 années d'ancienneté.

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 contrat.

ARTICLE 2 Politiques de sécurité

Le cocontractant est tenu de respecter les prescriptions de la politique de sécurité des systèmes d'information (PSSI) de l'Administration.

ARTICLE 3 Contrôles et audits

L'Administration peut conduire ou mandater des contrôles et audits de sécurité informatique des fournitures, prestations, moyens utilisés et services proposés par le cocontractant, et de ses sous-traitants.

Les contrôles et audits peuvent être réalisés après avoir prévenu le Cocontractant dans un délai minimum de 15 jours sans accord préalable dès lors que les tests et sondes respectent les conventions techniques d'usage permettant de les identifier.

25 · *L'arrêté du 18 septembre 2018 portant approbation du cahier des clauses simplifiées de sécurité est venu fixer les dispositions assurant un cadre de sécurisation des systèmes d'information et des données associées par tout type de marché et n'est applicable qu'aux marchés qui s'y réfèrent.*

Cet arrêté a été pris face à la menace croissante autour de la cybersécurité et notamment la protection des données confiées à un prestataire.

L'arrêté prend désormais en compte les réglementations applicables à la protection des données à caractère personnel, aux hébergements de données et aux sous-traitances.

ARTICLE 4 Documentations

4.1. Dans le cadre de la revue formelle de sécurité de l'Administration, le Cocontractant 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. Il est demandé de fournir un document de type PAS (plan d'assurance qualité) contenant les éléments et pratiques de mise en œuvre des bonnes pratiques au sein de l'entité du Cocontractant.

4.2. Le Cocontractant 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 Cocontractant s'assure de la conformité desdits traitements au regard des normes juridiques en vigueur, sous réserve des dispositions spéciales du présent Contrat.

Le Cocontractant fournit à l'Administration l'aide nécessaire à la réalisation d'analyses d'impact relatives (PIA) à la protection des données à caractère personnel, et à la consultation préalable des autorités de contrôle.

4.3. Le Cocontractant fournit à première demande la documentation nécessaire à l'Administration 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 Cocontractant 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 Cocontractant porte à la connaissance de l'Administration 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 Cocontractant 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 surtout critique (standard CVE ⩾ 9).

5.2. La responsabilité du maintien en condition de sécurité du Cocontractant 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 Cocontractant 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 Cocontractant met à la disposition de l'Administration 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'Administration 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 Cocontractant 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 Cocontractant 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 Cocontractant 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'Administration à la faculté de se substituer au Cocontractant 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 Cocontractant 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 à l'état de l'art, 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 Cocontractant. Le Cocontractant est responsable du respect par ses sous-traitants de la présente annexe.

Sont à la charge du Cocontractant, 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 Cocontractant 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, HDS 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 Cocontractant est soumis à un devoir d'information de l'Administration. Le Cocontractant dès qu'il en a connaissance, transmet à l'Administration les non-conformités à la politique de sécurité et les défauts de sécurisation constatés.

10.2. L'Administration 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'Administration 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'Administration 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 Cocontractant 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 Cocontractant fournit la conformité à ces référentiels pour les services et objets numériques inclus dans l'objet du présent contrat. Le Cocontractant 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 Contrat 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, authentifiant nominatif 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

POUR ALLER PLUS LOIN

Conseil supérieur de la propriété littéraire et artistique (CSPLA)

Rapport sur la mise en œuvre du règlement européen établissant des règles harmonisées sur l'intelligence artificielle (modèle de résumé des données d'entraînement couvertes par le droit d'auteur p. 30)

https://www.culture.gouv.fr/nous-connaitre/organisation-du-ministere/conseil-superieur-de-la-propriete-litteraire-et-artistique-cspla/travaux-et-publications-du-cspla/missions-du-cspla/ia-et-transparence-des-donnees-d-entrainement-publication-du-rapport-d-alexandra-bensamoun-sur-la-mise-en-aeuvre-du-reglement-europeen-etablissant

Commission européenne

Modèle de résumé des données d'entraînement d'IA génératives

https://digital-strategy.ec.europa.eu/fr/library/explanatory-notice-and-template-public-summary-training-content-general-purpose-ai-models

POUR POURSUIVRE CES TRAVAUX

Les Interconnectés accompagnent tout au long de l'année les collectivités dans la mise en œuvre de leurs stratégies numériques :

- **La commission numérique** est l'instance stratégique commune des élus des Interconnectés, France urbaine et intercommunalités de France
- **Les groupes de travail Territoir'Prod** réunissent les agents des collectivités de toute la France. Ces groupes organisent le partage entre pairs et experts, animent et accompagnent la mise en œuvre des stratégies Data et IA sur le terrain.

REJOIGNEZ LA COMMUNAUTÉ !

www.interconnectes.com

datapublica
Data et IA pour l'intérêt général

Les interconnectés
RÉSEAU DES TERRITOIRES INNOVANTS

FRANCE URBAINE
MÉTROPOLES, AGGLOS ET GRANDES VILLES

INTERCOMMUNALITÉS DE FRANCE