CLAUSIER POUR UNE GOUVERNANCE DES DONNÉES

PRÉSENTATION DU CLAUSIER	3
1. LES EXIGENCES RÉGLEMENTAIRES POUR L'OPEN-DATA	4
CLAUSE TYPE – PROPRIÉTÉ ET EXPLOITATION DES DONNÉES PUBLIQUES	5
LE CHOIX DE LA LICENCE DE PUBLICATION	6
2. LES EXIGENCES RÉGLEMENTAIRES POUR LA PROTECTION DES DONNÉES PERSONNELLES	9
CLAUSES RGPD À INSÉRER DANS UN CONTRAT AVEC UN PRESTATAIRE	10
3. LES ARGUMENTS JURIDIQUES UTILISABLES POUR JUSTIFIER DE CATALOGUER LE PATRIMOINE DE DONNÉES D'UNE COLLECTIVITÉ	12
CLAUSE – CATALOGAGE DES DONNÉES PUBLIQUES	13
METHODE PROPOSEE POUR RÉALISER UN CATALOGAGE EN CAS D'ABSENCE DE CLAUSE AD HOC DANS LE CONTRAT	14
4. GESTION DE LA PROPRIÉTÉ INTELLECTUELLE DES DÉVELOPPEMENTS LOGICIELS	19
GESTION DE LA PROPRIÉTÉ INTELLECTUELLE DANS LE CADRE DES MARCHÉS PUBLICS	21
GESTION DE LA PROPRIÉTÉ INTELLECTUELLE DANS LE CADRE D'UN PROJET COLLABORATIF PUBLIC/PRIVÉ	24
CLAUSE CONTRACTUELLE UTILISABLE DANS LE CADRE D'UN PROJET COLLABORATIF PUBLIC/PRIVÉ	25
5. GESTION DES DONNÉES : ACCÈS, CO-FINANCEMENT ET PÉRENNISATION	28
6. LES EXIGENCES TENANT A L'HEBERGEMENT, A LA REVERSIBILITE DES DONNEES ET A LA SECURITE DES SYSTEMES D'INFORMATION	28
CLAUSE – HEBERGEMENT ET CONDITIONS DE STOCKAGE DES DONNEES	28
CLAUSE – REVERSIBILITE DES OUTILS TECHNOLOGIQUES	29
CLAUSE – SECURITE DES SYSTEMES D'INFORMATION	29
ANNEXES	32
Annexe 1 - Annexe de Sous-traitance RGPD	33

PRÉSENTATION DU CLAUSIER

Ce clausier présente cinq axes à prendre en compte dans les relations contractuelles entre collectivités et prestataires, comme des ingrédients de base nécessaires, d'une part, au respect des obligations réglementaires et, d'autre part, à la mise en œuvre d'une gouvernance des données.

1. Les exigences réglementaires pour l'**Open-data**
2. Les exigences réglementaires pour la **protection des données personnelles**
3. Les clauses contractuelles utilisables pour **cataloguer le patrimoine de données**

Ces 3 axes sont complémentaires et l'idéal est d'intégrer l'ensemble des clauses types dans les cahiers des charges que la collectivité rédige à l'attention de ses futurs prestataires, ainsi que dans les contrats signés avec les prestataires, formant une « clause de gestion des données » globale.

Un 4^{ème} axe vise à garantir l'autonomie de la collectivité dans la **gestion d'une plateforme logicielle de gestion de données** tout en laissant à l'entreprise privée qui l'a codée la possibilité de la pérenniser, en gérant habilement les droits de propriété intellectuelle.

Un 5^{ème} axe vise à soutenir la **mise en œuvre d'une gouvernance des données** par le cadrage de modalités d'accès, d'enrichissement et de pérennisation collective, ou encore par des modalités contractuelles destinées aux utilisateurs afin de favoriser les co-financement et ainsi la pérennisation d'un patrimoine de données.

Tous ces axes sont complémentaires et visent à donner des "clés" à la collectivité pour qu'elle ne soit pas bloquée a posteriori.

La philosophie qui pré-existe à la mise en œuvre d'une gouvernance des données est détaillée dans le livrable "Gouvernance des données" (à paraître), ce clausier est un outil au service de la mise en œuvre de cette gouvernance. Il est rédigé de manière à ce qu'une collectivité, ne sachant pas nécessairement ce qu'elle fera demain, puisse :

- être assurée de répondre aux **obligations réglementaires** ;
- ne pas être **bloquée par manque d'usage** de clauses juridiques de base ;
- se consacrer à des **projets collaboratifs** publics/privés dans un mode **gagnant/gagnant**.

1. LES EXIGENCES RÉGLEMENTAIRES POUR L'OPEN-DATA

Il n'existe pas de standard imposé pour la diffusion des jeux de données en ligne (hormis quelques exceptions : données de mobilité, subventions, etc.). Pour une même typologie de données, chaque administration peut utiliser différents formats. Le référentiel général d'interopérabilité (RGI) fixe les règles techniques permettant d'assurer l'interopérabilité des systèmes d'information et détermine notamment les répertoires de données, les normes et les standards qui doivent être utilisés par les autorités administratives. La version 2.0 du RGI a été publiée par arrêté du 20 avril 2016.

Le standard choisi doit en revanche répondre aux conditions suivantes : il doit être uniformisé (un format identique pour toutes les données regroupées au sein d'un même jeu de données) et chaque jeu de données doit être lisible par une machine. Il convient donc de privilégier les formats non-propriétaires (tel que le format CSV) lors de la publication pour que les données publiées soient effectivement ouvertes.

Un format propriétaire conditionne la possibilité d'utilisation des données à l'usage et l'achat de logiciels propriétaires. Un format ouvert est un format qui n'impose pas un logiciel spécifique pour ouvrir le fichier. Il garantit l'interopérabilité d'un fichier avec plusieurs outils, c'est-à-dire l'accès, la disponibilité, la gratuité et la durabilité des données.

Extrait du Référentiel général d'Interopérabilité (mis à jour le 18 décembre 2020) :

Syntaxique	Structuration de données	
Recommandé	JSON	JavaScript Object Notation
http://fr.wikipedia.org/wiki/JavaScript_Object_Notation JSON est un format de données textuelles dérivé de la notation des objets du langage JavaScript. Le principal avantage de JSON est qu'il est simple à mettre en œuvre par un développeur tout en étant complet. Il présente plusieurs avantages, tels que : <ul style="list-style-type: none">• il est peu verbeux (XML simplifié), ce qui le rend lisible plus facilement que XML aussi bien par un humain que par une machine ;• il reste facile à apprendre, car sa syntaxe est réduite et non extensible (bien que ne souffrant que de peu de limitations) ;• Ses types de données sont connus et simples à décrire.		
IETF	RFC 7159	

Le Format JSON-LD a l'avantage de pouvoir relier des données qui sont décrites dans différentes ontologies. Il fait référence pour relier toutes les données du web sémantique. C'est le format le plus abouti à ce jour pour lier les données et atteindre le plus haut niveau d'interopérabilité.

Afin de respecter les exigences de la Loi pour une République Numérique, notamment, et de favoriser le respect du RGI, les collectivités devraient inscrire dans leurs cahiers des charges et contrats signés avec les éditeurs de solutions logicielles de tout type, la clause suivante.

CLAUSE TYPE – PROPRIÉTÉ ET EXPLOITATION DES DONNÉES PUBLIQUES

Par « Données Publiques » au sens du présent contrat, nous entendons toute information représentée sous une forme conventionnelle et stockée numériquement, collectée, produite ou détenue dans le cadre de la prestation de service public pour les besoins de laquelle le logiciel ou la solution du titulaire est utilisé.

Les données produites, collectées, traitées ou gérées par l'Acheteur public ou par le Titulaire pour son compte dans le cadre de ses activités de service public et en lien avec ses compétences en ce qu'elles sont nécessaires au fonctionnement du service public sont réputées appartenir à l'Acheteur public dès l'origine. A l'issue du contrat, le titulaire s'engage à remettre gratuitement à l'Acheteur public toutes les données précédemment visées et à apporter la preuve de leur destruction.

Le Titulaire s'engage à permettre à l'Acheteur public d'accéder librement à ces données à tout moment de l'exécution du Marché public.^[SA1]

L'acheteur a engagé une politique en faveur de l'innovation et du développement des connaissances pour tous faisant une place prioritaire au logiciel libre et à la réutilisation des données publiques conformément à la loi pour une République numérique, n°2016-1321 du 7 octobre 2016 et au Livre III du Code des relations entre le public et l'administration, en vigueur au 09 octobre 2016.

Pour cela, l'acheteur permet aujourd'hui à des tiers de réutiliser librement les Données Publiques diffusées sur sa plateforme accessible à l'adresse suivante : « à préciser »

L'acheteur doit publier les Données Publiques générées par le présent contrat sous une des licences de réutilisation publique autorisées par la loi qui précisent les droits et les obligations rattachés aux données.

A cette fin, le titulaire s'engage à faire ses meilleurs efforts aux fins de fournir à l'acheteur, à sa demande et sans surcoût, les jeux de Données Publiques lui permettant d'être en conformité avec ses obligations légales notamment telles que définies ci-avant. Il est précisé que la demande de l'acheteur pourra intervenir à tout moment en cours d'exécution du marché et pourra être régulièrement renouvelée.

Ces jeux de Données Publiques devront être transmis au moyen de standards ouverts aisément réutilisables et exploitables par un système de traitement automatisé.

Les moyens standards ouverts sont ceux définis par l'article 4 de la LCEN du 21 juin 2004 : « Tout protocole de communication, d'interconnexion ou d'échange et tout format de données interopérable dont les spécifications techniques sont publiques et sans restriction d'accès ni de mise en œuvre » tels que les formats de type CSV, ODS, XML, KML et SHP ainsi que ceux mentionnés dans le Référentiel général d'interopérabilité (RGI)¹ (notamment le format JSON).

¹. https://www.numerique.gouv.fr/uploads/Referentiel_General_Interoperabilite_V2.pdf.

Étant convenu que ce format doit être **uniformisé** (un format identique pour toutes les données regroupées au sein d'un même jeu de données) et chaque jeu de données doit être **lisible par une machine**.

Dans le cas où la Donnée Publique est normalisée dans le cadre du présent contrat ou en cours de marché, le titulaire devra avoir recours au format convenu pour son transfert.

Le titulaire fournit également à l'acheteur toutes les informations nécessaires à la compréhension du modèle des Données Publiques (diagrammes UML, schémas XML, descriptions textuelles...).

Le titulaire reconnaît à l'acheteur le statut de producteur de la ou des bases de Données Publiques au sens de l'article L341-1 du code de propriété intellectuelle.

En toute hypothèse et notamment dans le cas où cette qualification ne serait pas retenue par un tribunal, le titulaire autorise à toutes fins utiles, le seul acheteur en tant que propriétaire des Données Publiques (ou un tiers désigné par celui-ci) à extraire et exploiter librement et gracieusement tout ou partie des Données Publiques notamment en vue de leur mise à disposition à titre gratuit à des fins de réutilisation et d'exploitation que ce soit à titre gratuit ou onéreux, seules ou incorporées dans une offre de service, et ce, pour le monde, sur tout réseau ou support et sans limite de temps.

Toute exploitation des Données Publiques par le titulaire en dehors des besoins imposés par le présent marché doit être expressément autorisée par l'acheteur.”

Pour aller plus loin

Le site de la CNIL qui apporte des informations multiples sur les modalités de diffusion des données : <https://www.cnil.fr/fr/queelles-sont-les-modalites-de-diffusion-en-ligne>

Le Référentiel général d'interopérabilité (RGI) V2, du 12 janvier 2016 - mis à jour le 18 décembre 2020 : <https://www.numerique.gouv.fr/publications/interoperabilite/>

Au-delà d'insérer une clause type dans le contrat de marché pour pouvoir disposer des données produites dans les logiciels, il s'agit surtout de s'interroger sur la volonté de mettre en œuvre une véritable politique de **gouvernance des données**. Cela passe obligatoirement par la compréhension et le choix de la **licence** de publication des données publiques qui sera la mieux adaptée..

LE CHOIX DE LA LICENCE DE PUBLICATION

Deux licences de publication des données en open-data sont reconnues conformes par décret pour la publication des données en France, la licence ODbL V1² et la Licence Ouverte V2³.

². <https://spdx.org/licenses/ODbL-1.0.html#licenseText>

Ces deux licences sont juridiquement très différentes. La licence Ouverte est très **permissive** et ne demande quasiment pas de contrepartie à l'octroi des droits. L'ODbL est une licence **réciproque** qui va exiger que les versions dérivées de la base de données (soit enrichissement substantiel⁴ du contenu ou structure de la base, soit extraction substantielle du contenu de la base de données au profit d'une autre) soient diffusées sous les termes de la même licence.

Par ailleurs la Licence ouverte V2 se focalise sur la notion **d'information** prise isolément : un document, une image, un acte administratif, un son, etc. La licence ODBL a une **approche globale de la base de données** même si la notion de contenu est présente. Elle n'est exploitable que pour les database (les documents PDF ne sont pas concernés par cette licence).

En cela les deux licences sont même assez **complémentaires** dans certains cas. Par exemple, lorsque le jeu de données ne constitue pas véritablement une base de données structurée mais plutôt un jeu de données voire un document isolé, il sera plus conforme d'utiliser la Licence ouverte. Cela n'empêchera pas d'utiliser la licence ODBL sur la base de données qui viendrait à accueillir lesdites données.

Le choix n'est donc **pas exclusif** l'une de l'autre. L'une s'intéresse au niveau micro (Licence ouverte) et la seconde au niveau Macro (ODbL). A noter que cela relève cependant d'un parti pris du législateur qui consiste à dire qu'il n'est pas possible de diffuser une information isolée sous une licence réciproque. La réciprocité ne se concevrait qu'au niveau de la base de données.

Cela reste bien un postulat imposé puisque des licences réciproques existent pour des données isolées. pour exemple nous pouvons prendre la licence **créative commons Attribution-ShareAlike 4.0 International**⁵ (CC-BY-SA 4.0). Laquelle n'est pas une licence autorisée par le décret précité mais elle peut le devenir sur **demande d'homologation** auprès d'ETALAB. Elle a par exemple été exceptionnellement homologuée pour les données de cartographie maritime à la demande du Service hydrographique et océanographique de la marine (SHOM).

Nous vous proposons un rapide tableau de comparaison des deux licences :

	Licence Ouverte V2	Licence ODbL V1
Objet	Porte sur une 'information en particulier ou un jeu d'informations publiques	Porte plus généralement sur la base de données d'informations publiques en

³ www.etalab.gouv.fr/wp-content/uploads/2017/04/ETALAB-Licence-Ouverte-v2.0.pdf

⁴ La licence ODBL précise sur ce point : « *Substantiel* » - Signifie substantiel en termes de quantité ou de qualité ou d'une combinaison des deux. L'extraction ou la réutilisation répétée et systématique de parties non substantielles du contenu peut équivaloir à l'extraction ou à la réutilisation d'une partie substantielle du contenu.

⁵ <https://creativecommons.org/licenses/by-sa/4.0/>

		tant qu'ensemble organisé
Mécanisme	Permissif	Réciproque
Autorisé	<ul style="list-style-type: none"> ★ Usage commercial ★ Usage privé ★ Redistribution ★ Modification 	<ul style="list-style-type: none"> ★ Usage commercial ★ Usage privé ★ Redistribution ★ Modification
Interdit	<ul style="list-style-type: none"> ★ Tenir l'éditeur de la base de données pour responsable 	<ul style="list-style-type: none"> ★ Sous-licencier ★ Tenir l'éditeur de la base de données pour responsable
Obligations	<ul style="list-style-type: none"> ★ Informer de la source et de la date de mise à jour. 	<ul style="list-style-type: none"> ★ Rediffuser sous la même licence

Si une collectivité souhaite hériter des **contributions tierces** d'acteurs ayant exploité ses données et bénéficier ainsi d'une dynamique collaborative, il est préférable qu'elle utilise la licence **ODbL**, car celle-ci lui permet de pouvoir potentiellement réutiliser les données qu'elle a mise à disposition, après leur enrichissement par un tiers qui aura donc été contraint de diffuser sa base sous les termes et conditions de cette même licence.

En revanche, si elle pense que l'essentiel est que ses données soient **réutilisées** par des tiers, la Licence Ouverte laisse le choix à ces tiers de choisir la licence sous laquelle les données qu'ils auront réutilisées et potentiellement enrichies seront re-publiées. La licence est dite **permissive** et ne comporte pas de barrière de réutilisation, notamment dans les contextes commerciaux.

Pour aller plus loin

www.data.gouv.fr/fr/pages/legal/licences

2. LES EXIGENCES RÉGLEMENTAIRES POUR LA PROTECTION DES DONNÉES PERSONNELLES

Le RGPD est un cadre réglementaire strict qui permet à la collectivité de protéger les **données personnelles** qu'elle détient, mais qui lui permet aussi d'appliquer des **règles de sécurité** plus largement à **toutes les données qu'elle détient**.

Dans ce chapitre, l'objectif est de donner aux collectivités les clauses et documents prêts à l'emploi, pour qu'elles soient en règle et que leurs sous-traitants le soit aussi.

Au-delà des articles à insérer dans un contrat avec un prestataire de la collectivité, il est nécessaire de lui faire remplir plusieurs documents contractuels afin de pouvoir garantir le respect des **obligations réglementaires** de la collectivité. Son prestataire "sous-traitant" étant lui-même soumis à des obligations réglementaires.

En effet, il est stipulé dans le Règlement Général sur la Protection des Données personnelles (RGPD), à l'attention d'un prestataire « sous-traitant » :

- Lorsque vous intervenez en tant que sous-traitant dans la mise en œuvre d'un traitement de données personnelles, vous devez offrir à votre client « des 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 présent règlement et garantisse la protection des droits de la personne concernée » (article 28 du règlement européen).
- Obligation : mettre à la disposition de votre client toutes les informations nécessaires pour démontrer le respect de vos obligations et pour permettre la réalisation d'audits (sur la base, par exemple, du référentiel de la CNIL pour la délivrance de labels en matière de procédure d'audit).
- **Peut être sanctionné le fait de ne pas mettre à la disposition de son client les informations permettant de démontrer le respect de ses obligations ou pour permettre la réalisation d'audits ;** (Articles 82 et 83 du règlement européen).

Pour aller plus loin

- https://www.cnil.fr/sites/default/files/atoms/files/rgpd-guide_sous-traitant-cnil.pdf
- <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000024742533>

CLAUSES RGPD À INSÉRER DANS UN CONTRAT AVEC UN PRESTATAIRE

Il existe deux types de traitements de données à caractère personnel différents. Le **premier** concerne les traitements que la collectivité et le prestataire organisent pour leur **propre compte** dans le cadre ou pour les besoins de l'exécution du contrat en tant que responsable de traitement. Dans ce cas, la [CNIL recommande](#) la rédaction d'une clause renvoyant chaque partie à ses responsabilités de type :

“Le titulaire s’engage à veiller au respect des règles légales en vigueur en matière de protection des données à caractère personnel pour les traitements effectués dans l’exécution de ses missions dont il est seul responsable de traitement.”

Le **second** type de traitement concerne ceux que le prestataire gère pour le compte de la collectivité en tant que **sous-traitant** et nécessite une contractualisation au sens de l'[article 28 du RGPD](#) .

“Les dispositions, engagements et obligations des Parties sont prévus au sein de l’Accord de Protection des Données annexé au présent Contrat.” (Cf. Annexe 1).

Pour compléter le contrat d'usage du logiciel et assurer le respect des obligations réglementaires de la collectivité et exigences de sécurité selon l'état de l'art en vigueur, il est également possible d'utiliser une clause d'engagement de confidentialité (datée, signée et complétée) ;

Un modèle d'Annexe sous-traitance RGPD est fourni en annexe du présent guide.

Pour rappel, en matière de sécurité la CNIL recommande :

- d'exiger la communication par le titulaire de sa politique de sécurité des systèmes d'information ;
- d'assurer et de documenter l'effectivité des garanties offertes par le titulaire sous-traitant en matière de protection des données.

Par exemple, les parties peuvent mettre en œuvre les moyens suivants (en les encadrant contractuellement si nécessaire) :

- audits de sécurité,
- visite des installations,
- certifications de l'organisme,
- certification des compétences du DPO.

En pratique une grille d'exigences de sécurité devrait figurer dans les documents du marché et participer de la sélection du candidat. L'application de cette grille doit ensuite être vérifiée en cours d'exécution du contrat afin de déterminer la conformité aux

engagements de sécurité pris.

Il est également recommandé à l'acheteur responsable de traitement et au titulaire sous-traitant d'imposer à leurs employés une obligation contractuelle de confidentialité et de s'assurer que ceux-ci sont sensibilisés aux grands principes de la protection des données.

Il est nécessaire, enfin, de limiter les accès aux seules personnes habilitées en raison de leurs fonctions, et en distinguant les différentes opérations qui peuvent être effectuées sur les données (consultation, modification, suppression, export, etc.).

Pour aller plus loin, consultez le guide de la sécurité des données personnelles de la CNIL⁶.

Enfin, il est important de préciser au marché autant que possible les modalités précises de la communication des données pour éviter toute mauvaise surprise et principalement les points suivants :

- nature
- délai
- coût
- format

Exemple simplifié (car dépendant du marché) :

“Le titulaire s’engage à remettre gratuitement l’ensemble des données traitées dans le cadre du marché au format XML sous 30 jours calendaires à compter du terme dudit marché.”

⁶ <https://www.cnil.fr/fr/securite-des-donnees>

3. LES ARGUMENTS JURIDIQUES UTILISABLES POUR JUSTIFIER DE CATALOGUER LE PATRIMOINE DE DONNÉES D'UNE COLLECTIVITÉ

Pour mettre en œuvre une gouvernance des données, une collectivité a besoin d'avoir une bonne connaissance des données dont elle dispose et des règles d'usage qui sont liées à ces données. Afin de connaître son patrimoine de données, elle peut être amenée à s'équiper d'une solution d'exploration de son système d'information (exemple : pose de sondes).

En l'absence d'obligation contractuelle, plusieurs fondements juridiques peuvent permettre à la collectivité de justifier auprès d'un éditeur de sa légitimité à récupérer toutes les métadonnées et données produites par le biais de logiciels.

ARGUMENTS >>>>>	Arguments tirés d'une obligation légale directe						Arguments indirects mais incitatifs		
	option B avant 1/4/21 (CCAG TIC 2009) Art.B.38.1.3. = Cession de PI sur Base de données inclue dans les résultats	Droit d'usage des connaissances antérieurs (CCAG TIC 2009)	Cession de PI automatique depuis CCAG TIC 1 ^{er} avril 2021	Droit d'usage des connaissances antérieurs (CCAG 2021)	RGPD. Obligation de mise à disposition des informations perso.	articles L. 3131-2 et s. CCP Régime des biens de retour	Respect de la loi OPEN DATA	Faible atteinte au secret + standard non Propriétaire recommandé RGI	Confidentialité assurée par accord de confidentialité
Si développement sur mesure	Si option B stipulée		X		Si données personnelles	Si contrat de concession	X	X	Solution hébergée par l'éditeur
Si logiciel standard		X		X	Si données personnelles	Si contrat de concession	X	X	Solution hébergée par l'éditeur

Matrice d'usage des différents arguments juridiques en fonction du profil du marché public en cause

Les arguments juridiques proposés en bleu permettent d'arguer de véritables **droits opposables** au titulaire du marché. Les arguments juridiques en orange quant à eux sont destinés à **convaincre** du peu de risque de la démarche et du bien fondé de la demande.

Il demeure qu'une clause dédiée à la question de l'intégration d'une sonde dans la base de donnée de la solution du titulaire du marché demeure la meilleure solution pour éviter toute ambiguïté. Afin de demeurer **technologiquement neutre** il sera même préférable de viser "tout moyen ou technologie visant à faciliter le catalogage de ses données afin d'améliorer la connaissance de son patrimoine de données par la collectivité acheteuse".

Un modèle de clause adaptable à votre situation vous est proposé ci-dessous.

CLAUSE – CATALOGAGE DES DONNÉES PUBLIQUES

L'acheteur s'est engagé dans une démarche de catalogage des données de son système d'information dans l'objectif de la mise en conformité RGPD et la mise en œuvre d'une

gouvernance des données facilitées par une meilleure connaissance de son patrimoine de données.

La Titulaire s'engage donc, à la demande de l'acheteur :

- A installer ou exécuter sur ces équipements d'hébergement tout moyen ou technologie visant à faciliter le catalogage de ses données afin d'améliorer la connaissance de son patrimoine de Données Publiques par la collectivité acheteuse ;
- à fournir toute documentation technique permettant de rendre possible ou de faciliter l'interopérabilité avec la solution logicielle objet du présent marché en vue de l'indexation ou du catalogage des Données Publiques ;
- à collaborer à la mise à disposition de manière manuelle ou automatisée de toute information à sa disposition permettant de rendre possible ou de faciliter l'indexation ou le catalogage de l'intégralité des Données Publiques.

Si une technologie tierce est utilisée

Plus particulièrement, l'acheteur utilise, au jour de la signature du présent contrat, l'outil « à préciser » de la société « à préciser » qui fonctionne grâce à « à préciser » (par exemple : des sondes d'indexation paramétrées permettant d'analyser et d'identifier les métadonnées des applications).

Pour ce faire, les options techniques possibles sont « à préciser », par exemple :

- par la pose d'une sonde sur une machine ayant accès à la base de données et la configuration de cette sonde. Une fois exécutée, cette sonde permet la récupération des informations dans un fichier JSON que le titulaire devra transmettre de manière sécurisée à l'acheteur ;
- par la saisie manuelle par le titulaire d'un fichier JSON transmis par l'acheteur.

Pour de plus amples informations, toute la documentation technique est disponible sur demande auprès de l'acheteur.

Ce traitement permet la récupération du nom des tables ainsi que le nom des colonnes et des métadonnées liées sur les bases de données suivantes : « à préciser ».

L'acheteur s'engage à conserver confidentielles, au sens du présent contrat, les informations récoltées concernant le modèle conceptuel de données ainsi que la structure de la base de données et à n'en faire aucune utilisation autres que celle strictement nécessaire à l'exploitation des Données Publiques concernées dans le cadre de la fourniture de la ou des missions de service public dont l'Acheteur a la charge.

En cas d'une mise à jour majeure du logiciel du titulaire ou d'évolution de la base de données et des traitements de données qui lui sont associées, l'acheteur pourra demander au titulaire une nouvelle itération du catalogage des données.

METHODE PROPOSEE POUR RÉALISER UN CATALOGAGE EN CAS D'ABSENCE DE CLAUSE AD HOC DANS LE CONTRAT

La méthode proposée pour réaliser un catalogage avec des contrats antérieurs à l'usage de la clause ci-dessus, est l'envoi d'un courrier type, puis, le cas échéant, l'envoi d'un deuxième courrier (qui peut être signé par un avocat) rappelant tous les fondements légaux. Les éditeurs de solutions logicielles pouvant parfois être réservés sur l'usage de sondes notamment, pour lire la base de données de leur logiciel. Le rappel des obligations réglementaires et l'usage des différents cadres légaux selon le type d'objection rencontrée, peut s'avérer très utile.

Les courriers-types pour réaliser un catalogage de données de la collectivité, sont présentés ci-dessous, avec une possibilité d'usages de clauses différentes selon le type d'objection rencontrée de la part d'un éditeur.

Cela implique au préalable d'avoir choisie une méthode technique pour identifier les données présentes dans le système d'informations (exemple : pose de sondes, indexation,...). Le catalogage de données permet grâce aux métadonnées d'identifier le panel disponible de données présentes dans le système d'information, mais aussi leur redondance, et facilite ainsi leurs traitements ultérieurs (partage, ouverture, protection,...).

Cette démarche facilite aussi, avec une animation autour de ce patrimoine de données désormais connu, l'émergence de croisement de données, de nouveaux indicateurs de mesures, de nouveaux services à valeur ajoutée pour la collectivité et pour les habitants/usagers/citoyens de son territoire.

Corps du premier « courrier type »

Madame, Monsieur,

La « *collectivité* » a lancé une démarche de catalogage des données de son système d'information dans l'objectif de mieux maîtriser son patrimoine de données et de répondre à ses obligations légales de diffusion publique de celle-ci.

Cette demande intervient dans le cadre de la bonne exécution de vos obligations contractuelles.

Concrètement, « *préciser la solution technique* » sur les bases de données des applications métiers, SaaS, utilisées par les services « *de la collectivité* ». Cette solution sert à faire remonter les métadonnées sur l'état des données disponibles et devant être rendues accessibles au titre d'une

obligation légale.

Pour pouvoir avancer dans notre objectif, je vous remercie de bien vouloir générer cette solution technique sur les bases de données de la collectivité qui sont hébergées chez vous. Le guide méthodologique, ci-joint, détaille la marche à suivre. Cette action est unique. Elle ne sera pas à renouveler sauf si le modèle de base de données devait évoluer.

Le format de fichier utilisé pour cet export, le JSON, permet une exploitation des informations ainsi harmonisées.

Il vous est demandé de déposer le fichier issu de ce sondage sur la plateforme d'échanges sécurisés qui sera fournie par notre service « *à préciser* ». Après le dépôt des résultats sur la plateforme sécurisée de la collectivité, la solution technique devra être supprimée ainsi que le compte qui aura été paramétré pour son exécution.

La pose de cette solution technique est simple et rapide. Elle ne perturbe en rien votre système. Notre prestataire « *à préciser* » est à votre disposition pour toute question technique complémentaire « *coordonnées* ».

Notre service « *à préciser* », en charge du pilotage du projet reste à votre disposition pour son bon déroulement « *coordonnées* ».

Je vous remercie de bien vouloir réaliser ces diligences au plus tard le « *date à préciser* ».

Corps du deuxième « courrier type »

Madame, Monsieur,

Nous faisons suite à votre réponse négative / votre absence de réponse à notre courrier en date du « à préciser » vous invitant à l'installation d'une solution technique « à préciser » afin de permettre l'export des informations nécessaires à la gestion de ses données par « la collectivité » au moyen d'un format de fichier harmonisé.

Nous vous rappelons que cette demande découle d'une obligation légale instaurée par les principaux textes suivants :

- Loi n° 2015-991 du 7 août 2015 portant nouvelle organisation territoriale de la République, dite « loi NOTRe » ;
- Loi n° 2015-1779 du 28 décembre 2015 relative à la gratuité et aux modalités de la réutilisation des informations du secteur public, dite « loi VALTER » ;
- Décret n° 2016-360 du 25 mars 2016 relatif aux marchés publics ;
- Loi n°2016-1321 du 7 octobre 2016 pour une République numérique.

Par ailleurs, le référentiel général d'interopérabilité (RGI) fixe les règles techniques permettant d'assurer l'interopérabilité des systèmes d'information et détermine notamment les répertoires de données, les normes et les standards qui doivent être utilisés par les autorités administratives. La version 2.0 du RGI a été publiée par arrêté du 20 avril 2016. Le format JSON y est expressément mentionné comme l'un des formats de données permettant l'application de la loi une interopérabilité effective. Ceci suppose que la structuration de la donnée y est simple pour pouvoir être facilement repris par un autre système.

Nous rappelons que l'intérêt de la solution technique « à préciser » est de ne pas avoir à passer par des formats de données propriétaire peu ou pas réutilisable.

Votre refus met donc la collectivité locale dans l'impossibilité de répondre à ses obligations légales de par l'impossibilité de maîtriser le corpus de données qu'elle détient et de métadonnées liées.

Ajouter ici, selon les objections de l'éditeur un/des articles du tableau ci-dessous

Nous vous réitérons donc la demande d'export des données. **Tout refus constituera une violation du contrat de marché public donnant droit à la résiliation de plein droit pour faute de celui-ci.** Le présent courrier vaut à ce titre mise en demeure de déférer à la demande sous 15 jours tel que stipulé à l'article XX du contrat de marché public nous liant.

La pose de cette solution technique « à préciser » est simple et rapide. Elle ne perturbe en rien votre système. Notre prestataire « à préciser » est à votre disposition pour toute question technique complémentaire « coordonnées ».

Notre service « à préciser » en charge du pilotage du projet reste à votre disposition pour son bon déroulement « coordonnées ».

Je vous remercie de bien vouloir réaliser ces diligences au plus tard le « date à préciser ».

Situations rencontrées Argument opposé par le titulaire	Réponse spécifique en cas de refus / argumentaire juridique
La divulgation de secret ou savoir-faire	L'argument consistant à opposer la protection de la confidentialité de votre savoir-faire technique interne est inopérant en l'espèce pour les raisons listées ci-après : 1/ Cet argument vient protéger les données et non les éventuels actifs du producteur de la base de données. 2/ Le format de fichier servant à l'exportation peut n'être porteur que du minimum d'informations nécessaire à la compréhension des données mais ne comporte pas la structure de la base de données proprement dite

	<p>(attention ce n'est pas le cas avec de nombreux formats de fichiers modernes, par exemple le XML et toutes ses variantes comme le GML ou City-GML).</p> <p>3/ Dans tous les cas la collectivité est tenue à une obligation de confidentialité sur les informations échangées aux termes de l'article 5.1.1 du CCAG TIC version 2009. Une obligation de confidentialité similaire à été signée entre la collectivité et le prestataire qui déploie la solution technique. Vos intérêts sont donc protégés le cas échéant.</p> <p>4/ La structure de base de données ou la base de données (même vide), si elle est préexistante à l'exécution du contrat, rentre dans la catégorie des connaissances antérieures au sens du CCAG TIC version 2009, . Or, aux termes de l'article 36 dudit CCAG TIC (ou de son équivalent dans la version 2021), le titulaire « <i>concède à titre non exclusif au pouvoir adjudicateur et aux tiers désignés dans le marché, le droit d'utiliser de façon permanente ou temporaire, en tout ou partie, par tout moyen et sous toutes formes les connaissances antérieures strictement nécessaires pour utiliser les résultats pour les besoins découlant de l'objet du marché. Ce droit comprend le droit de reproduire, de dupliquer, de charger, d'afficher, de stocker, d'exécuter, de représenter les connaissances antérieures pour utiliser les résultats</i> ». (Article 36).</p> <p>Aussi la collectivité est en toute hypothèse légitime à demander à accéder à ces informations dont elle a besoin pour remplir les obligations légales qui découlent de l'exécution du contrat.</p>
<p>Des développements spécifiques avec cession de la PI</p>	<p>Aux termes du contrat signé avec la collectivité pour la fourniture du service vous avez accepté de céder à titre exclusif la propriété intellectuelle des résultats du marché, au nombre desquels figurent les informations demandées y compris tout savoir-faire de conception matérialisé dans la base de données. La demande consiste donc en la stricte application de vos obligations contractuelles. (<i>cf. partie dédiée du guide</i>)</p>
<p>L'hébergement par la collectivité + maintenance par éditeur</p>	<p>Dans ce cas, la question peut se poser des conséquences de déploiement de la technologie en termes de fonctionnement de la solution de l'éditeur. Si par exemple les sondes sont de nature à perturber le fonctionnement de la base de données, son autorisation ou à tout le moins sont information préalable nous semblent nécessaires. Si au contraire l'intervention de catalogage est totalement indolore et purement observationnelle il n'y a pas de raison évidente d'en informer le titulaire.</p> <p>Le critère à surveiller n'est donc plus l'atteinte à un quelconque savoir-faire mais plutôt la perturbation du bon fonctionnement de la solution qui peut impacter la mission et la responsabilité d'un titulaire devant a priori en assurer le maintien en condition opérationnelle.</p>
<p>La collectivité est responsable de traitement de données</p>	<p>Aux termes du règlement général sur la protection des données, officiellement appelé règlement UE 2016/679 du Parlement européen et du Conseil du 27 avril 2016, la collectivité est qualifiée de Responsable de traitement et votre société est qualifiée de sous-traitant. A ce titre vous</p>

personnelles	<p>devez assister la collectivité dans son maintien en conformité à la loi.</p> <p>Pour rappel « <i>Peut être sanctionné le fait [pour le sous-traitant] de ne pas mettre à la disposition de son client les informations permettant de démontrer le respect de ses obligations ou pour permettre la réalisation d’audits ; (Articles 82 et 83 du règlement européen)</i> »</p>
Une entreprise de transport	<p>En matière de transports publics, les entreprises concessionnaires doivent, conformément aux dispositions de l’article L. 1115-1 du code des transports, diffuser certaines données « librement, immédiatement et gratuitement en vue d’informer les usagers et de fournir le meilleur service » comme les tarifs, les horaires, l’évolution de la fréquentation, etc.</p> <p>La demande formulée par la collectivité s’inscrit là encore dans cette nécessité de cataloguer l’information pour pouvoir la rendre disponible.</p>
Un contrat de concession de services publics	<p>Les bases de données du concessionnaire, bien que régies par les articles L.3131-2 et suivants du Code de la commande publique lorsqu’elles sont « indispensables » à l’exécution du service public, peuvent être qualifiées de biens de retour dès lors qu’elles sont nécessaires à celui-ci.</p> <p>[SI DSP] En matière de délégation de service public, la base de données relève spécifiquement de la catégorie juridique des biens de retours, c’est-à-dire des biens nécessaires à la continuité du service public après le terme de la délégation.</p> <p>Le Conseil d’Etat a pu préciser (CE Ass 21 décembre 2012, Commune de Douai, req. n° 342788) que le délégataire est tenu de fournir à la collectivité délégante toute information utile sur les biens de la délégation, afin de lui permettre d’exercer son contrôle sur le service public concédé. Votre société, en tant que délégataire, est donc tenue de transmettre au délégant, à sa demande, un inventaire des biens de la délégation.</p>

4. GESTION DE LA PROPRIÉTÉ INTELLECTUELLE DES DÉVELOPPEMENTS LOGICIELS

Lorsqu’une collectivité commande des développements logiciels spécifiques, ou qu’elle co-réalise un service dans le cadre d’un projet partenarial public/privé, la question se pose de savoir si elle va acquérir de la propriété intellectuelle (exclusive ou non-exclusive) pour son usage futur. Cette question est d’autant plus fondamentale lorsqu’elle concerne la mise en œuvre d’une architecture de données ou d’une plateforme logicielle de gestion de données quel qu’en soit le périmètre fonctionnel.

La réflexion est fondamentale car :

- La réalisation d'un code peut être liée à des **connaissances antérieures**, ce qui implique de savoir quel est l'impact de ces connaissances antérieures sur les développements à réaliser,
- Les **coûts** engagés pour détenir la **propriété intellectuelle exclusive** sont plus importants que dans le cadre d'une cession de droits à titre non exclusif (l'entreprise et la collectivité ont dans ce cas les mêmes droits),
- **L'évolution** de la solution logicielle et sa **diffusion** ne sont pas nécessairement garanties si la collectivité est seule à détenir les droits de propriété intellectuelle. Le fait que le titulaire conserve la propriété de la solution et l'édite peut permettre une **mutualisation** des coûts de maintenance,
- La **gestion des droits d'exploitation** de la solution reste à traiter, à la fois pour les connaissances antérieures, et les développements réalisés dans un cadre contractuel commun (projet public/privé), ou dans le cadre d'un marché.
- Le fait de développer le logiciel en **open-source** ne supprime pas la nécessité de gérer les droits de propriété intellectuelle.

Dans le cadre des marchés publics, c'est le **CCAG-TIC** qui encadre les conditions de transfert de la propriété intellectuelle de développements logiciels et les droits d'exploitation dans les marchés publics. Celui-ci a évolué en **2021**, **intégrant par défaut une cession de propriété intellectuelle des résultats du marché**.

Retenons que d'une manière générale, tout résultat issu d'un marché de technologies de l'information a **vocation à être diffusé**. Cela concerne autant le **code source** d'un développement logiciel sur commande⁷, que la **donnée** issue de l'exploitation d'une solution logicielle existante ; ou encore les **algorithmes** utilisés pour les besoins du service public objet d'un marché⁸. Aussi, l'enjeu pour l'acheteur, avant toute considération stratégique et financière, sera de bien considérer les **obligations** qui sont les siennes en matière de communication et de diffusion des documents et informations publiques dans le cadre du marché considéré. De cette analyse découlent potentiellement des **obligations légales** qui imposeront à l'acheteur d'obtenir les droits nécessaires au respect de ces obligations.

Notons encore que le **périmètre minimum des droits de propriété intellectuelle** à acquérir sera déterminé, en miroir, par le contenu des **licences** de diffusion prescrites par le législateur pour lesdits documents et informations.

⁷ Article D323-2-1 CRPA

⁸ Article L311-3-1 CRPA : "Sous réserve de l'application du 2° de l'article L. 311-5, une décision individuelle prise sur le fondement d'un traitement algorithmique comporte une mention explicite en informant l'intéressé. Les règles définissant ce traitement ainsi que les principales caractéristiques de sa mise en œuvre sont communiquées par l'administration à l'intéressé s'il en fait la demande."

Cerema x Shift Avocats CC-by-nc

GESTION DE LA PROPRIÉTÉ INTELLECTUELLE DANS LE CADRE DES MARCHÉS PUBLICS

Nous nous focalisons tout d'abord sur la **version antérieure du CCAG-TIC 2009**, dans le cadre des marchés publics, car nombre de projets en cours sont encore régis par cette version.

1. Le CCAG-TIC (2009)

Dans sa précédente version (CCAG-TIC 2009), il existait deux options possibles pour la gestion des droits de propriété intellectuelle, Article 38, option A et option B, à défaut de précision, c'était l'option A qui s'appliquait :

- a. L'option A : Concession de droits d'utilisation sur les résultats qui ne permettait pas de récupérer des droits de propriété intellectuelle sur les développements logiciels réalisés

Article 38. A - Le titulaire du marché concède, à titre non exclusif, au pouvoir adjudicateur et aux tiers désignés dans le marché, le droit d'utiliser ou de faire utiliser les résultats, en l'état ou modifiés, de façon permanente ou temporaire, en tout ou partie, par tout moyen et sous toutes formes. Cette concession ne vaut que pour les besoins découlant de l'objet du marché et pour la France. Dans l'hypothèse d'une publication sur internet, les droits sont concédés pour le monde entier.

Cette concession des droits couvre les résultats, à compter de leur livraison et sous condition résolutoire de la réception des prestations.

Le droit d'utiliser les résultats ne couvre pas les exploitations commerciales des résultats.

Le pouvoir adjudicateur et les tiers désignés dans le marché ne deviennent pas, du fait du marché, titulaires des droits afférents aux résultats dont la propriété des inventions nées, mises au point ou utilisées à l'occasion de l'exécution du marché.

Le prix de cette concession est forfaitairement compris dans le montant du marché.

- b. L'option B qui permettait de récupérer des droits de propriété intellectuelle sur les développements logiciels réalisés

Article 38 B : Résultats protégés par un droit de propriété littéraire et artistique.

Le titulaire du marché cède au pouvoir adjudicateur les droits patrimoniaux des droits d'auteur ou des droits voisins des droits d'auteur afférents aux résultats pour le(s) territoire(s), la durée, les modes

d'exploitation des droits cédés et le prix définis dans les documents particuliers du marché.

Cette cession des droits couvre les résultats une fois divulgués, à compter de leur livraison, sous condition de la réception des prestations.

Ces droits comprennent l'ensemble des droits patrimoniaux de reproduction et de représentation et notamment d'adaptation, d'arrangement, de correction, de traduction, d'incorporation afférents aux résultats ainsi que le droit de distribuer les résultats à des fins commerciales pour les modes d'exploitation prévus dans les documents particuliers du marché.

Pour les modes d'exploitation prévus dans les documents particuliers du marché, le droit de reproduction comporte, si nécessaire, le droit de reproduire les résultats, sans limitation de nombre, en tout ou partie, en l'état ou modifiés, par tous procédés et sur tout support y compris pour les supports non prévisibles ou inconnus à la date de signature du marché, en vue d'une exploitation notamment à titre commercial, sous réserve d'une rémunération à convenir pour les modes d'exploitation futurs, non connus au jour de la signature du marché.

Pour les modes d'exploitation prévus dans les documents particuliers du marché, le droit de représentation et de distribution comporte si nécessaire le droit de communication au public et de mise à disposition du public des résultats, en tout ou partie, en l'état ou modifiés, par tous moyens, modes et procédés y compris non prévisibles ou inconnus à la date de signature du marché, en vue d'une exploitation notamment à titre commercial, sous réserve d'une rémunération à convenir pour les modes d'exploitation futurs, non connus au jour de la signature du marché.

Les codes sources et la documentation nécessaires à la mise en œuvre des droits sur les résultats sont livrés, sur support exploitable, en même temps que le code objet. Les codes sources sont confidentiels.

Dès lors que la collectivité souhaite, à l'issue d'un développement logiciel, ou bien après une première phase de développement (expérimentation), pouvoir bénéficier des résultats, et potentiellement des évolutions techniques qui pourraient être faites sur le résultat de l'expérimentation par l'entreprise, l'usage de l'option B est un pré-requis.

En effet, l'option B impliquant la cession de droits de propriété intellectuelle à la collectivité, cette cession de droits peut alors être "négociée" sous la forme d'une cession "à titre non exclusif" au lieu d'une d'une cession exclusive, afin de négocier les suites des conditions d'exploitation de la solution logicielle développée.

Ceci se règle par le biais d'un contrat d'exploitation des résultats, ce contrat permettant alors à l'entreprise de garder les mêmes droits que la collectivité, moyennant par exemple,

l'engagement d'enrichir le logiciel des évolutions qu'elle ferait par ailleurs en diffusant le logiciel sur d'autres territoires.

Les développements réalisés, s'ils sont tributaires de connaissances antérieures, le droit d'usage de ces connaissances antérieures, ou les conditions de leur cession doit alors avoir été traité en amont, dans le cahier des charges de la collectivité et dans la relation contractuelle lors de la signature du marché, ou faire l'objet d'une négociation avant la fin du marché en cours.

2. Extrait du CCAG-TIC (2021), chapitre 7, Articles 43 à 46 :

Par défaut le CCAG-TIC 2021 assure à l'acheteur une **cession** des droits sur les résultats du marché de nature à lui permettre une **exploitation sans contrainte**. La notion de **résultat** est entendus au sens large et l'on y retrouve toutes les œuvres soumises au droit d'auteur classique (documents préparatoires, tels que plans, études préalables ou spécifications etc.), les logiciels, les bases de données, les algorithmes, données, brevet, marque, nom de domaine, compte de réseau sociaux.

Le **périmètre** des droits cédés est quant à lui suffisamment **large** mais la cession n'en est pas **exclusive**. L'exclusivité est réservée par exception aux résultats ayant pour objet d'identifier l'acheteur, de promouvoir ses produits ou services et ceux qui ne peuvent pas être réutilisés en raison de leur confidentialité. Plus généralement, le titulaire s'interdit de procéder à tout dépôt ou réservation de marque ou de signes distinctifs (y compris noms de domaine ou comptes de réseaux sociaux) pouvant générer un risque de confusion avec l'acheteur.

Concernant les résultats protégés par un droit de propriété industrielle relatif à des inventions ainsi que les connaissances techniques pouvant consister en un savoir-faire confidentiel, le titulaire concède à l'acheteur une licence d'utilisation non exclusive des droits de propriété intellectuelle afférents à ces résultats pour les finalités compatibles avec la nature du marché et sans limite territorial ou de durée.

L'article 46.2.3 prévoit le régime des données intégrées ou générées dans le cadre du marché comme étant confidentielles et **appartiennent exclusivement à l'acheteur**. Le titulaire ne dispose que d'un accès aux données dans le cadre de l'exécution du marché aux seules fins de son exécution. Le titulaire s'interdit aussi d'en faire un quelconque usage, direct ou indirect, en dehors des prestations du marché, sauf autorisation préalable et expresse de l'acheteur.

Le titulaire conserve la propriété de ses savoir-faire et méthodes utilisés pour réaliser les résultats. L'acheteur autorise le titulaire à exploiter ou publier, y compris à titre commercial, les résultats créés dans le cadre du marché et non soumis à cession exclusive au profit de l'acheteur. Si des connaissances antérieures transmises par l'acheteur sont nécessaires à l'exploitation des résultats, l'autorisation de l'acheteur est nécessaire et une redevance peut être demandée. Le titulaire s'engage par ailleurs à ce que l'exploitation des résultats ne porte pas atteinte aux droits ou à l'image de l'acheteur, ni ne viole la confidentialité due à l'acheteur. A noter que, le cas échéant, la publication mentionne que les résultats ont été financés par l'acheteur.

Les cessions des droits sur les différents objets sont accompagné des obligations permettant leur exercice :

- transmission du code source pour les logiciel
- transmission des fichiers sources et natifs dans un format ouvert pour les autres œuvres (créations graphiques, images, films, musique, etc.)

L'ensemble des cessions de droits et des supports matériels en permettant l'exercice est cédé pour un prix réputé inclus dans le prix du marché.

En conclusion :

Dans le cas de projets antérieurs au CCAG-TIC 2021, dès lors que l'option B a été choisie, les résultats d'un projet commun d'un développement logiciel, par exemple d'une « plateforme de données », dédiée à un métier (exemple : la gestion d'un port) ou transverse aux métiers de la collectivité, il est utile d'avoir les **droits de propriété intellectuelle de part et d'autre**, pour garantir que le solution évolue avec des fonds privés et publics, et s'assurer qu'elle soit pérennisée par l'entreprise privée tout en s'assurant que la collectivité soit aussi indépendante de l'entreprise privée, si elle le souhaite.

L'idéal étant de pérenniser la relation contractuelle par un **contrat d'exploitation** des résultats au profit du titulaire et à titre non exclusif. Cela peut notamment permettre d'octroyer des **droits** au titulaire qui sont dérogoratoires aux droits concédés via les licences open sources et libres promues par le législateur. Dès lors, le titulaire détiendra, à travers ce contrat, un avantage concurrentiel sur ses éventuels concurrents qui se seraient emparés de la solution dans sa version sous licence libre / ouverte. Cela peut être incitatif à une exploitation commerciale garante d'une évolution du produit dans le temps.

Attention cette rétrocession de droits non exclusifs sur le logiciel au profit du titulaire doit répondre à certaines conditions et notamment d'avoir un minimum de contrepartie pour ne pas constituer une cession à un prix en dessous du prix réel du bien.

A noter :

Rappelons que même si le code logiciel a été développé en **open-source**, il est quand même nécessaire de **traiter le sujet de la propriété intellectuelle** à part entière car **seul le propriétaire** des droits peut **décider de la licence** sous laquelle était publiée le code open-source, et lui seul peut décider de changer de licence.

Dans le cadre des **marchés passés depuis le CCAG-TIC 2021**, il faut prendre soin de bien détailler **quelles connaissances sont apportées par le titulaire et par l'acheteur** et quels résultats feront l'objet d'une cession de droits à titre non-exclusif, et quels résultats feront l'objet d'une cession de droit exclusive.

GESTION DE LA PROPRIÉTÉ INTELLECTUELLE DANS LE CADRE D'UN PROJET COLLABORATIF PUBLIC/PRIVÉ

Un projet collaboratif doit faire l'objet d'un **accord de consortium** qui régit les conditions de développement de code logiciel.

Cet accord de consortium doit idéalement prévoir d'emblée la rédaction d'un **contrat d'exploitation à l'issue du projet**, celui-ci devant régler les modalités d'exploitation des résultats, dès lors que ceux-ci ne sont pas précisément connus au départ du projet collaboratif, ou que leurs modalités d'exploitation ne sont pas complètement définies, la dimension innovante qui préexiste étant une part importante du projet collaboratif et laissant de la place à l'inconnu. L'accord de consortium règle en revanche la question des connaissances antérieures.

La clause de cession des droits à titre non exclusif, à insérer dans un contrat d'exploitation des résultats à l'issue d'un projet public/privé est la suivante.

CLAUSE CONTRACTUELLE UTILISABLE DANS LE CADRE D'UN PROJET COLLABORATIF PUBLIC/PRIVÉ

Article 1 : Cession des droits de propriété intellectuelle de « l'entreprise qui a codé » sur le Logiciel au bénéfice de « la collectivité »

La cession des droits de propriété intellectuelle « *entreprise qui a codé* » sur le Logiciel au bénéfice de « la *collectivité* » est réalisée en contrepartie de l'investissement humain et financier de « la *collectivité* » dans la recherche et le développement du Logiciel, l'« *entreprise qui a codé* » cède à « la *collectivité* », qui l'accepte, l'intégralité de ses droits de propriété intellectuelle sur le Logiciel.

Les droits listés ci-après sont expressément cédés à « la *collectivité* » à titre non-exclusif par l'« *entreprise qui a codé* », pour le monde entier et pour toute finalité, pour toute exploitation à titre gratuit ou onéreux et ce pour toute la durée de protection du Logiciel, notamment au titre du droit d'auteur prévu par le Code de la Propriété Intellectuelle. Ils incluent le droit de concéder des sous-licences à des tiers sur tout ou partie de ces mêmes droits, et ce, sans autorisation préalable.

Pour satisfaire aux dispositions de l'article L.131-3 du Code de la Propriété Intellectuelle et conformément à son article L.122-6, il est précisé que ces droits de propriété intellectuelle cédés par l'« *entreprise qui a codé* » sur le Logiciel, selon les conditions du Contrat, comprennent :

a. Droit de reproduction et d'adaptation

Le droit de reproduction et d'adaptation comporte le droit de réaliser ou d'autoriser les opérations suivantes :

- de reproduire, de numériser et d'adapter tout ou partie du Logiciel, individuellement ou ensemble, avec d'autres œuvres, en toutes langues et pour tout pays, sous tout format actuel ou futur, connu ou inconnu, destinée à tout support et/ou moyen et/ou réseau de communication ;
- de reproduire ou faire reproduire, tout ou partie du Logiciel, individuellement ou ensemble, sur tout support magnétique, optique ou autre, de manière mécanique, analogique, numérique, électronique ou autre, et sur tout support

connu ou inconnu, actuel ou futur, et notamment mais de manière non limitative, sur CD, DVD, etc. Ce droit comprend toute opération de reproduction et d'adaptation réalisée par tout procédé connu ou inconnu, actuel ou futur et notamment toute opération temporaire ou permanente de stockage, de transmission et de téléchargement (en upload et download) ;

- d'adapter et de faire évoluer tout ou partie du Logiciel, individuellement ou ensemble, le droit de réaliser de nouvelles versions du Logiciel, ou de nouveaux développements à partir du Logiciel, le droit de modifier, arranger, assembler, condenser, transcrire, mixer, migrer chacun des éléments du Logiciel, individuellement ou ensemble, pour tout public, en tout langage, sur toute plate-forme technique et par le biais de tout support et/ou moyen et/ou réseau de communication.
- de charger, d'afficher, d'exécuter, de transmettre ou le stockage du Logiciel dans la mesure où ces opérations nécessitent leur reproduction.

b. Droit d'exploitation

Le droit d'exploitation comporte le droit de réaliser ou d'autoriser les opérations suivantes :

- d'exploiter tout ou partie du Logiciel, individuellement ou ensemble, et de ses adaptations par tout moyen, notamment mais de manière non limitative, la vente ou la location (licence) pour l'usage privé ou public, en tout format, par tout procédé, sur tout support, et sur toute plateforme technique, connus ou inconnus, actuels ou futurs, à titre temporaire ou définitif, auprès de tout public et par le biais de tout support et/ou moyen et/ou réseau de communication ;
- de mettre ou de faire mettre en circulation dans le monde entier tout ou partie des reproductions de tout ou partie du Logiciel, individuellement ou ensemble, et de ses adaptations pour la vente, la location, le prêt pour l'usage public et l'usage privé du public, et de manière générale, par 5/45 tout moyen de communication au public par le biais de tout support et/ou moyen et/ou réseau de communication.

c. Droit de représentation et de communication

Le droit de représentation et de communication comporte le droit de réaliser ou d'autoriser les opérations suivantes :

- de représenter et de faire représenter tout ou partie du Logiciel, individuellement ou ensemble, et de ses adaptations en toutes langues et en tout pays, sur toute plate-forme et selon toute norme technique, actuelle ou future, connue ou inconnue ;
- de communiquer au public tout ou partie du Logiciel, individuellement ou ensemble, ou de ses adaptations par tout procédé, payant ou non,

direct ou indirect, connu ou inconnu, actuel ou futur, par fil ou sans fil et sur tout réseau de diffusion des données, connu ou inconnu, actuel ou futur. Ce droit comprend notamment la diffusion sur tout réseau de communication, par voie hertzienne, par câble, par satellite, par télédiffusion et de manière générale, par tout moyen, sur tout réseau et selon tout protocole de télécommunication, actuel ou futur, connu ou inconnu, tel que, mais de manière non limitative, GSM, DCS 1800 ou 1900, UMTS, Wi-Fi, Wi-Max, BlueTooth, Wap, etc ;

- de diffuser tout ou partie du Logiciel individuellement ou ensemble, sur des réseaux internes ou privés, notamment d'entreprises, par toute personne de droit public ou privé, à titre gratuit ou onéreux.

Article 2 : Transmission du Savoir-Faire par « entreprise qui a codé » sur le Logiciel au bénéfice de « la collectivité ».

En toute hypothèse, « l'entreprise qui a codé », devra transmettre le Savoir-Faire à « la collectivité » ou à toute personne désignée par cette dernière, avec laquelle la collectivité aurait contractualisé. La transmission du Savoir-Faire devra se faire à première demande de la collectivité et dans les meilleurs délais. La transmission devra permettre une reconstruction à l'identique et une exploitation effective du Logiciel dans sa version en exploitation au jour de la demande. La transmission implique la formalisation d'une documentation remplissant cet objectif ainsi qu'une formation raisonnable des personnels désignés par la collectivité.

5. GESTION DES DONNÉES : ACCÈS, CO-FINANCEMENT ET PÉRENNISATION

Les collectivités sont soumises à l'obligation légale d'**ouvrir les données d'intérêt général** qu'elles produisent mais aussi celles qu'elles **achètent**. Pour autant ces données peuvent nécessiter des **moyens conséquents pour être mises à disposition** en ligne dans des conditions d'usage correctes (données géographiques, images satellitaires,...). La collectivité peut donc créer un **service d'accès à la donnée**, pour faciliter l'usage des données et le cas échéant facturer l'accès à ce service.

Aux termes de l'article L324-1 du Code des relations entre le public et l'administration, la réutilisation d'informations publiques est gratuite. Toutefois, les administrations mentionnées au premier alinéa de l'article L. 300-2 peuvent établir une **redevance de réutilisation** lorsqu'elles sont tenues de couvrir par des **recettes propres une part substantielle** des coûts liés à l'accomplissement de leurs missions de service public. Cette part a été fixée à **25% minimum**. C'est-à-dire que si les coûts de cette administration **sont couverts à plus de 75% par des subventions publiques** elle ne peut pas exiger de redevance.

Aussi on peut estimer que les collectivités qui ne sont pas des administrations publiques ayant pour objet et activité "statutaire" de produire de la données, elles ne peuvent être amenées à recevoir des subventions en contrepartie d'une activité qui n'est que l'accessoire de leur activité principale. Ce critère serait donc rempli.

Reste que "le produit total du montant de cette redevance, évalué sur une période comptable appropriée" ne doit pas dépasser "le montant total des coûts liés à la collecte, à la production, à la mise à la disposition du public ou à la diffusion de leurs informations publiques".

6. LES EXIGENCES TENANT A L'HEBERGEMENT, A LA REVERSIBILITE DES DONNEES ET A LA SECURITE DES SYSTEMES D'INFORMATION

Les principes relatifs aux données publiques sont fixés par le législateur qui n'a toutefois pas pu envisager l'ensemble des situations nécessitant la protection de ces données.

Les présentes clauses viennent pallier les carences du cadre légal et réglementaire.

CLAUSE – HEBERGEMENT ET CONDITIONS DE STOCKAGE DES DONNEES

Face aux enjeux de sécurité et de souveraineté des données liés à l'objet du Contrat, l'Acheteur public fixe les règles d'hébergement de ses données.

Afin de garantir la sécurité des données du Contrat, l'acheteur public impose leur hébergement dans l'Union Européenne.

CLAUSE – REVERSIBILITE DES OUTILS TECHNOLOGIQUES

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

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

Ainsi, en cas de cessation de la relation contractuelle, quelle qu'en soit la cause, le Titulaire s'engage à restituer gratuitement, à la première demande de l'Acheteur public formulée par lettre recommandée avec accusé de réception et dans un délai de 48 heures à la date de réception de cette demande, l'ensemble des données visées à l'article de la présente convention. L'Acheteur dispose d'un outil de description des métadonnées dont le Titulaire devra respecter les préconisations afin de transmettre l'ensemble de ces données [joindre descriptif technique].

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

CLAUSE – SECURITE DES SYSTEMES D'INFORMATION

1. Face aux enjeux de confiance, de souveraineté et de sécurité des systèmes d'information liés à l'objet du Contrat, le Titulaire est tenu de respecter le cadre juridique applicable :

- à la sécurité des systèmes d'information, à travers le respect, notamment du Référentiel général de sécurité approuvé par arrêté du 13 juin 2014 (NOR : PRMD1413745A) et du règlement eIDAS du 23 juillet 2014 ;
- aux données à caractère personnel à travers le respect, notamment des dispositions du Règlement (UE) 2016/679 du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données et de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

- A l'open data et notamment les dispositions du code des relations entre le public et l'administration ;
- A l'archivage et notamment les dispositions applicables du code du patrimoine ;
- A la sécurité des acteurs critiques et notamment les dispositions applicables du code de la défense pour les Opérateurs d'Importance Vitale (OIV) et celles de la Directive 2016/1148 du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union en cours de révision et transposée en droit français par la loi n°2018-133 du 26 février 2018 portant diverses dispositions visant à l'adaptation au droit de l'Union européenne dans le domaine de la sécurité (i) et par le décret n°2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de services numériques, il précise les modalités d'application de la loi du 26 février 2018 (ii) pour les Opérateurs de Services Essentiels (OSE).

2. Conformément au cadre juridique rappelé ci-dessus, le Titulaire 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 Titulaire.

3. Le Titulaire s'engage à mettre à la disposition du responsable de l'Acheteur public 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'Acheteur public ou un autre auditeur qu'il a mandaté, et contribuer à ces audits ;

4. Au terme normal ou anticipé du contrat, le Titulaire s'engage à :

- Détruire toutes les données du Contrat ou
- A renvoyer toutes les données du Contrat à l'Acheteur public ou
- A renvoyer les données du Contrat au nouveau cocontractant désigné par l'Acheteur public.

Le renvoi doit s'accompagner de la destruction de toutes les copies existantes dans les systèmes d'information du Titulaire.

Une fois détruites, le Titulaire doit justifier par écrit de la destruction.

Auteurs :

- Gérald Sadde - Shift Avocat
- Sophie Houzet - Cerema

Contribution :

- Scheherazade Abboub
- Julien Hautemaniere - Cerema

ANNEXES

Annexe 1 - Annexe de Sous-traitance RGPD

ACCORD DE SOUS-TRAITANCE (DATA PROCESSING AGREEMENT)

Collectivité Responsable de
traitement :

A compléter, dater et signer par le prestataire du service proposé

Thème :	<u>Protection et exigences de sécurité des données personnelles</u>
Nom du service proposé :	
Société :	
Contact :	<p><i>Veillez indiquer ici les coordonnées de la personne qui a complété ce document au sein de votre société et qui répondra aux demandes de compléments que la CNIL ou la collectivité pourraient être amenées à formuler</i></p> <p>Nom, Prénom :</p> <p>Service / Fonction :</p> <p>Adresse :</p> <p>Code postal / Ville :</p> <p>Adresse électronique :</p> <p>Téléphone :</p>
	<p>A : Le :</p> <p>Signature du représentant légale</p>

Autres Contacts :	<p><i>Si dans votre société il existe DPO/DPD (Data Protection Officer /Délégué à la Protection des Données) autre que la personne précisée ci-dessus, veuillez indiquer les coordonnées de chaque personne et préciser leur fonction</i></p> <p>Qualité, Nom, Prénom :</p> <p>Service / Fonction :</p> <p>Adresse électronique :</p> <p>Téléphone :</p>
Contacts de la collectivité	<p>Qualité, Prénom, Nom :</p> <p>Fonction :</p> <p>Adresse électronique :</p> <p>Téléphone :</p> <p><i>Répétez ci plusieurs contacts</i></p>

1. Préambule

Cet accord de sous-traitance (ci-après abrégé le « **DPA** ») définit les droits et obligations du Responsable de Traitement et le Sous-traitant lorsque ce dernier traite des données à caractère personnel pour le compte du Responsable de Traitement.

Le DPA a été élaboré pour s'assurer du respect par les Parties de l'article 28(3) du règlement européen 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel (le « **RGPD** »).

Dans le cadre de la fourniture de ses services, le Sous-traitant traitera des données à caractère personnel pour le compte du Responsable de Traitement conformément aux stipulations convenues dans ce DPA.

Le DPA a primauté sur toute autre stipulations similaires contenues dans d'autres accords conclus entre les Parties.

Trois annexes sont jointes à ce document et font partie intégrante du DPA :

§ **L'Annexe A** qui contient des informations détaillées sur le traitement de données à caractère personnel, notamment la finalité et la nature du traitement, le type de données à caractère personnel, les catégories de personnes concernées et la durée du traitement.

§ L'**Annexe B** qui contient les règles imposées par le Responsable du Traitement autorisant le Sous-traitant à recourir à des sous-traitants ultérieurs ainsi que la liste des sous-traitants ultérieurs autorisés par le Responsable de Traitement.

§ L'**Annexe C** qui contient les mesures de sécurité minimales à mettre en œuvre par le Sous-traitant.

Le DPA ne dispense pas le Sous-traitant des obligations auxquelles il est soumis en vertu du RGPD ou d'une autre législation.

2. Les droits et obligations du Responsable de Traitement

Le Responsable de Traitement est chargé de veiller à ce que le traitement de données à caractère personnel respecte le RGPD (conformément à l'article 24 du RGPD), les dispositions applicables au sein de l'UE ou des Etats membres en matière de protection des données à caractère personnel ainsi que les stipulations du DPA.

Le Responsable de Traitement a le droit et le devoir de prendre des décisions sur les finalités et les moyens du traitement de données à caractère personnel.

Le Responsable de Traitement est notamment chargé de veiller à ce que le traitement de données à caractère personnel que le Sous-traitant est chargé d'effectuer, dispose d'une base légale.

3. Le Sous-traitant doit agir sur instructions

Le Sous-traitant traite les données à caractère personnel uniquement sur instructions documentées du Responsable de Traitement, à moins que le droit de l'Union européenne ou de l'Etat Membre auquel le Sous-traitant est soumis ne l'exige.

Ces instructions sont précisées en **Annexe A**.

Des instructions ultérieures peuvent également être données par le Responsable de Traitement pendant toute la durée du traitement des données à caractère personnel, mais ces instructions doivent toujours être documentées et conservées par écrit, y compris sous forme électronique.

Le Sous-traitant informe immédiatement le Responsable de Traitement si les instructions données par le Responsable de Traitement contreviennent au RGPD ou au droit de l'Union

européenne ou au droit de l'Etat membre applicable en matière de protection des données à caractère personnel.

En préalable à toute modification des opérations de traitement, le Sous-traitant devra solliciter l'accord du Responsable de Traitement. En cas d'accord du Responsable de Traitement, une réponse écrite (courrier ou courriel) d'engagement devra être retournée par le responsable du Sous-traitant.

En cas de création de copie de données pour ces opérations, il sera demandé au Sous-traitant, après usage des données transférées, de détruire toutes les copies de données inutiles. Le Sous-traitant devra avertir le Responsable de Traitement par courriel de l'opération de destruction.

Pour tout test (développement d'interface, peuplement de base de données...), les données utilisées devront être anonymisées ou pseudonymisées.

Le transfert de données vers des tiers ou sous-traitant ultérieurs autorisés ne pourra s'effectuer qu'après autorisation du Responsable de Traitement et selon l'un des canaux suivants :

- o [compléter avec les moyens de transfert / accès autorisés]

La transmission du mot de passe garantissant la confidentialité du transfert devra s'effectuer via un canal de nature différente de celui ayant servi à la transmission des données (par téléphone ou sms).

4. Confidentialité

Le Sous-traitant n'accorde l'accès aux données à caractère personnel traitées au nom du Responsable de Traitement qu'aux personnes placées sous son autorité et qui se sont engagées à respecter un engagement de confidentialité ou qui sont soumises à une obligation légale de confidentialité appropriée et uniquement lorsqu'elles ont besoin de connaître le contenu desdites données.

La liste des personnes à qui l'accès a été accordé fait l'objet d'un réexamen périodique. Sur la base de ce réexamen, cet accès aux données à caractère personnel peut être retiré s'il n'est plus nécessaire, et les données à caractère personnel ne sont alors plus accessibles à ces personnes.

5. Sécurité du traitement

Compte tenu de l'état de l'art, des coûts de mise en œuvre et de la nature, de l'étendue, du contexte et des finalités du traitement ainsi que du risque de probabilité et de gravité variables

pour les droits et libertés des personnes physiques, le Responsable de Traitement et le Sous-traitant mettent en œuvre des mesures techniques et organisationnelles appropriées pour assurer un niveau de sécurité adapté au risque.

Le Responsable de Traitement évalue les risques pour les droits et libertés des personnes physiques inhérents au traitement et met en œuvre des mesures pour atténuer ces risques.

Les mesures techniques et organisationnelles mises en œuvre par le Sous-traitant sont spécifiées en **Annexe C**.

6. Sous-traitants ultérieurs

Le Sous-traitant doit satisfaire aux exigences spécifiées à l'article 28, paragraphes 2 et 4 du RGPD pour pouvoir engager un autre sous-traitant (ci-après désigné "**sous-traitant ultérieur**").

Le Sous-traitant a l'autorisation générale du Responsable de Traitement pour engager des sous-traitants ultérieurs, c'est-à-dire que le Sous-traitant informe par écrit le responsable du traitement de tout changement prévu concernant l'ajout ou le remplacement de sous-traitants secondaires **au moins quinze (15) jours à l'avance**, donnant ainsi au responsable du traitement la possibilité de s'opposer à ces changements avant d'engager le(s) sous-traitant(s) ultérieurs(s) concerné(s).

La liste des sous-traitants ultérieurs déjà autorisés par le responsable du traitement figure en **Annexe B**.

Lorsque le Sous-traitant engage un sous-traitant ultérieur pour effectuer des activités de traitement spécifiques pour le compte du Responsable de Traitement, les mêmes obligations en matière de protection des données que celles énoncées dans le présent DPA s'imposent à ce sous-traitant ultérieur par le biais d'un contrat ou d'un autre acte juridique en vertu du droit de l'Union Européenne ou d'un État membre, et doit notamment garantir la mise en œuvre de mesures techniques et organisationnelles appropriées de telle sorte que le traitement réponde aux exigences du présent DPA et du RGPD.

Il incombe donc au Sous-traitant d'exiger que le sous-traitant ultérieur respecte *a minima* des obligations similaires auxquelles le Sous-traitant est soumis en vertu du présent DPA et du RGPD.

Si le sous-traitant ultérieur ne remplit pas ses obligations en matière de protection des données, le Sous-traitant reste entièrement responsable envers le Responsable du traitement en ce qui concerne le respect des obligations du sous-traitant ultérieur.

7. Transfert de données vers des pays tiers ou des organisations internationales

Le titulaire du marché doit communiquer la liste de tous les lieux de stockage de données (site d'hébergement principal, sites secondaires, sites de réplication, sites de secours, sites de sauvegarde...).

Tout transfert de données à caractère personnel vers des pays tiers ou vers des organisations internationales par le Sous-traitant ne doit avoir lieu que sur la base d'instructions documentées du Responsable de Traitement et doit toujours se faire conformément au chapitre V du RGPD.

L'existence d'un transfert de données vers des pays tiers ou vers des organisations internationales et l'outil de transfert prévu au chapitre V du RGPD sur lequel il se fonde sont indiqués en **Annexe B**.

8. Assistance apportée au Responsable de Traitement

En prenant en considération la nature du traitement couvert par le DPA, le Sous-traitant assiste le Responsable de Traitement par des mesures techniques et organisationnelles appropriées, et pour autant que cela soit possible, dans l'accomplissement des obligations du Responsable de Traitement de répondre aux demandes d'exercice des droits des personnes concernées tel que prévu au chapitre III du RGPD.

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 entre le responsable de traitement et le sous-traitant avant la collecte de données.

En outre, compte tenu de la nature du traitement et des informations dont il dispose, le Sous-traitant assiste le Responsable de Traitement pour s'assurer le respect des règles suivantes :

- a. l'obligation pour le Responsable de Traitement de notifier une violation de sécurité à l'autorité de contrôle compétente, conformément à l'article 33 du RGPD ;
- b. l'obligation pour le Responsable de Traitement de communiquer une violation de sécurité aux personnes concernées, conformément à l'article 34 du RGPD ;

c. l'obligation du Responsable de Traitement de procéder à une évaluation de l'impact des traitements envisagés sur la protection des données à caractère personnel (ci-après « **AIPD** »), conformément à l'article 35 du RGPD ;

d. l'obligation du Responsable de Traitement de consulter l'autorité de contrôle compétente avant de procéder au traitement lorsqu'une AIPD conclue que le traitement envisagé entraînerait un risque élevé en l'absence de mesures prises par le Responsable de Traitement pour atténuer le risque conformément à l'article 36 du RGPD.

9. Notification d'une violation de données à caractère personnel

En cas de violation de données à caractère personnel, le Sous-traitant doit, sans délai indu après en avoir eu connaissance, notifier le Responsable de Traitement de cette violation.

La notification du Sous-traitant au Responsable de Traitement doit, si possible, avoir lieu dans les quarante-huit (48) heures suivant la date à laquelle le Sous-traitant a eu connaissance de la violation des données à caractère personnel afin de permettre au Responsable de Traitement de respecter l'obligation qui lui incombe de notifier la violation à l'autorité de contrôle compétente.

Le Sous-traitant assiste le Responsable de Traitement pour notifier la violation des données à caractère personnel à l'autorité de contrôle compétente, ce qui signifie que le Sous-traitant est tenu d'aider le Responsable de Traitement à obtenir les informations devant être fournies à l'autorité de contrôle compétente conformément à l'article 33 (3) du RGPD et qui sont énumérées ci-dessous :

- a. La nature des données à caractère personnel, y compris, si possible, les catégories et le nombre approximatif de personnes concernées, ainsi que les catégories et le nombre approximatif de données à caractère personnel concernées ;
- b. les conséquences probables de la violation des données à caractère personnel ;
- c. les mesures prises ou proposées par le Responsable de Traitement pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures visant à atténuer ses potentiels effets négatifs.

10. Conservation, effacement et restitution des données

A la fin de la fourniture des prestations de services, le Sous-traitant est tenu de supprimer toutes les données à caractère personnel traitées pour le compte du Responsable de Traitement.

Les catégories de données ne sont pas conservées par les services gestionnaires au-delà de la durée de vie du dossier de la personne concernée, sans préjudice de dispositions législatives ou réglementaires propres à certaines catégories de données imposant une durée de conservation particulière ou la suppression de ces données.

Les systèmes doivent donc prévoir des fonctionnalités de suppression, d'archivage, ou encore d'anonymisation ou de pseudonymisation de ces données, lorsque leur durée de conservation est atteinte.

11. Archivage des données

Le service proposé doit permettre l'archivage légal c'est-à-dire la conservation définitive pour les données à caractère historique ou leur élimination au terme de la durée d'utilisation administrative (DUA), et ce, conformément aux préconisations du Service Interministériel des Archives de France (SIAF).

Le service proposé doit permettre a minima un export du Standard d'Échange de Données pour l'Archivage (SEDA) qui se compose d'une description des documents/données (bordereau de versement au format XML) et des documents/données elles-mêmes.

[Option si système d'archivage d'export connu] Le service proposé devra permettre d'archiver les données, vers un système d'archivage électronique de document. Le Responsable de traitement a conventionné avec le département de [xxxx] et la Région pour mettre en place un système d'archivage électronique dénommé [xxxx], s'appuyant sur le produit [xxxx] de l'[xxxx].

12. Audit et inspection

Le Sous-traitant met à disposition du Responsable de Traitement toutes les informations nécessaires pour démontrer le respect des obligations prévues à l'article 28 du RGPD, dans le présent DPA et autorise et participe aux audits, y compris les inspections, conduits par le Responsable de Traitement ou par un autre auditeur mandaté par le Responsable de Traitement.

Le Responsable de Traitement informe le Sous-traitant de la réalisation d'un audit quinze (15) jours avant la date prévue pour sa réalisation, en précisant, le cas échéant, le tiers auditeur mandaté pour cet audit. Le Sous-traitant peut formuler toutes réserves objectives à l'encontre du tiers auditeur mandaté (notamment si ce dernier est un concurrent).

En tout état de cause, tout audit ne peut être réalisé qu'après la signature d'un accord de confidentialité entre le Sous-traitant et le tiers auditeur.

Le Sous-traitant est tenu de fournir aux autorités de contrôle et leurs représentants qui, conformément à la législation applicable peuvent accéder aux locaux, un accès aux installations physiques du Sous-traitant sur présentation préalable de leur qualité.

13. Points de contact du Responsable de Traitement et du Sous-traitant

Les Parties peuvent se contacter en utilisant les coordonnées des points de contact indiqués en **Annexe A**.

Les Parties sont tenues de s'informer en permanence des modifications apportées à leur point de contact.

14. Entrée en vigueur – Durée

Le DPA entre en vigueur à sa date de signature par les parties.

Les Parties sont autorisées à solliciter une renégociation du DPA si des changements de législation ou des changements de situation s'appliquent.

Le DPA s'applique pour toute la durée de fourniture des prestations de services par le Sous-traitant.

Pendant la durée des prestations de services, le DPA ne peut pas être résilié à moins qu'un autre DPA régissant la fourniture des prestations de services ait été convenu entre les Parties.

Si la fourniture des prestations de services cesse et que les données à caractère personnel ont été détruites ou retournées au Responsable de Traitement, le DPA peut être résilié par notification écrite de l'une ou l'autre des Parties.

*

Date de signature : _____

POUR LE SOUS-TRAITANT :

**POUR LE RESPONSABLE DE
TRAITEMENT :**

Signature

Nom

Qualité

Signature

Nom

Qualité

Annexe A. Informations concernant le traitement

A.1. Traitement des données à caractère personnel

La présente Appendice a pour objet de décrire les opérations de Traitements confiées par le Responsable de Traitement, au Sous-traitant. La description des Traitements présentées ci-dessous concerne également les Traitements confiés par le Sous-traitant à ses Sous-traitants ultérieurs dans le cadre du Contrat.

Finalités du Traitement confié :

A titre d'exemple

- Inscription des utilisateurs.
- Création de profils ou de comptes utilisateurs.
 - Permettre l'exploitation par les utilisateurs.
 - Assurer le support technique et la maintenance.

Durée du Traitement confié :

- La durée du Traitement correspond à la durée des prestations confiées au sous-traitant.

Opérations réalisées par le Sous-traitant, ou ses Sous-traitants ultérieurs, le cas échéant :

Activités de traitement	Applicable	
Collecte de Données à caractère personnel	☐ Oui	☒ Non
Communication de fichiers contenant des Données à caractère personnel	☒ Oui	☐ Non
Consultation de données à caractère personnel	☐ Oui	☒ Non

Analyse de Données à caractère personnel (ex : <i>établissement de statistiques</i>)	☐ Oui	☒ Non
Organisation ou structuration de Données à caractère personnel	☒ Oui	☐ Non
Extraction / Récupération de Données à caractère personnel	☒ Oui	☐ Non
Adaptation ou modification de Données à caractère personnel	☐ Oui	☒ Non
Anonymisation, effacement ou destruction de Données à caractère personnel	☒ Oui	☐ Non
Rapprochement de Données à caractère personnel	☐ Oui	☒ Non
Test impliquant des Données à caractère personnel	☐ Oui	☒ Non
Hébergement/Conservation de données à caractère personnel	☒ Oui	☐ Non

Catégories de Personnes concernées par le Traitement :

Catégories de Personnes Concernées	Applicable	
	☒ Oui	☐ Non
	☒ Oui	☐ Non
	☒ Oui	☐ Non
	☐ Oui	☒ Non

Catégories de Données à caractère personnel traitées :

Catégories de données à caractère personnel	Applicable	
<p>Données d'identification</p> <p><i>Exemples : nom, prénom, date et lieu de naissance, copie d'une pièce d'identité, état-civil, identifiants internes ou de compte internet, etc.</i></p>	☒ Oui	☐ Non
<p>Données de contact</p> <p><i>Exemples : n° de téléphone, adresse postale, adresse de messagerie électronique, etc.</i></p>	☒ Oui	☐ Non
<p>Données sur la situation personnelle</p> <p><i>Exemples : vie maritale, nombre d'enfants, composition du foyer, présence d'animaux domestiques, etc.</i></p>	☐ Oui	☒ Non
<p>Données sur la situation professionnelle</p> <p><i>Exemples : profession, nom de l'entreprise, poste, catégorie socioprofessionnelle, revenus, etc.</i></p>	☒ Oui	☐ Non
<p>Données bancaires et commerciales</p> <p><i>Exemples : données relatives à la carte bancaire, au virement bancaire, au chèque, historiques des achats / ventes, reçus, factures, numéro de transaction, détail de l'achat / abonnement, etc.</i></p>	☐ Oui	☒ Non
<p>Données techniques et données de connexion</p> <p><i>Exemples : identifiants de connexion à un compte, données collectées à travers l'utilisation de cookies ou autres traceurs, données de traçabilité (journaux, etc.).</i></p>	☒ Oui	☐ Non
<p>Données sensibles (cf. article 9 du RGPD)</p> <p><i>Exemple : données de santé, données révélant l'appartenance syndicale, l'orientation sexuelles, les opinions politiques, religieuses, etc.</i></p>	☐ Oui	☒ Non

A.2. Points de contact

Les Parties peuvent se contacter mutuellement en utilisant les points de contact suivants :

<p>Point de contact du Sous-Traitant:</p> <p>Nom [NAME]</p> <p>Fonction [POSITION]</p> <p>Telephone [TELEPHONE]</p> <p>E-mail [E-MAIL]</p>	<p>Point de contact du Responsable de Traitement :</p> <p>Nom [NAME]</p> <p>Fonction [POSITION]</p> <p>Telephone [TELEPHONE]</p> <p>E-mail [E-MAIL]</p>
---	--

Annexe B. Sous-traitants ultérieurs autorisés et instructions relatives aux transferts de données vers des pays tiers ou des organisations internationales

B.1. Sous-traitants ultérieurs autorisés

Dès l'entrée en vigueur du DPA, le Responsable de Traitement autorise le Sous-traitant à recourir aux sous-traitants ultérieurs suivants :

NOM ET COORDONNÉES	DESCRIPTION DE L'ACTIVITÉ SOUS-TRAITÉE	EXISTENCE D'UN TRANSFERT DE DONNÉES (OUI/NON)	EN CAS DE TRANSFERT: DÉCISION D'ADÉQUATION APPLICABLE (ARTICLE 45 RGD) OU GARANTIES APPROPRIÉES PRISES (ARTICLE 46 RGD)

Le Responsable de Traitement autorise, dès l'entrée en vigueur du DPA, le recours aux sous-traitants ultérieurs mentionnés ci-avant pour les opérations de traitement confiées. Le Sous-traitant n'a pas le droit – sans l'autorisation écrite explicite du Responsable de Traitement – d'engager un sous-traitant ultérieur pour un traitement « différent » de celui qui a été convenu ou de faire exécuter le traitement décrit par un autre sous-traitant ultérieur.

B.2. Instructions sur le transfert de données à caractère personnel

Le Responsable de Traitement reconnaît et accepte le transfert de données à caractère personnel vers des pays tiers par les sous-traitants énumérés au point **B.1.**

Annexe C. Mesures de sécurité

A adapter en fonction de la sensibilité des traitements et des données mais il s'agit du référentiel CNIL.

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

Thème	Mesure
Pilotage de la sécurité au sein de l'organisation	Les objectifs généraux en matière de sécurité et de protection des données à caractère personnel sont identifiés, formalisés et validés par la direction.
Pilotage de la sécurité au sein de l'organisation	Les traitements de données à caractère personnel et les activités impliquant le traitement de données à caractère personnel sont recensés au sein de notre registre. Ce registre est mis à jour en cas de modification.
Pilotage de la sécurité au sein de l'organisation	Le système d'information sur lequel repose les traitements de données à caractère personnel est formalisé sous forme de schémas, permettant d'identifier les interconnexions et les flux de données. Ces schémas sont tenus à jour en cas de modification.
Pilotage de la sécurité au sein de l'organisation	Un plan d'action dédié à la sécurité permet de suivre la mise en œuvre des mesures techniques et organisationnelles retenues par l'organisation. Le plan d'action est tenu à jour régulièrement selon son avancement ou sa modification.
Pilotage de la sécurité au sein de l'organisation	L'organisation opère un contrôle périodique des mesures de sécurité afin d'en vérifier l'effectivité. Les contrôles visent en priorité les mesures mises en œuvre pour corriger des vulnérabilités identifiées ou prévenir la survenance d'incidents s'étant déjà

	produits.
Pilotage de la sécurité au sein de l'organisation	Mise en place d'une revue mensuelle avec la direction permettant la prise de décision et le suivi des enjeux actuels liés à la sécurité et propre à l'organisation.
Pilotage de la sécurité au sein de l'organisation	L'organisation a désigné une personne responsable de la sécurité des systèmes d'information (RSSI).
Pilotage de la sécurité au sein de l'organisation	L'organisation a désigné un délégué à la protection des données (DPO).
Pilotage de la sécurité au sein de l'organisation	Les objectifs généraux en matière de protection des données à caractère personnel sont consignés dans une politique générale de protection des données, portée par la direction et diffusée à l'ensemble des acteurs.
Pilotage de la sécurité au sein de l'organisation	L'organisation réalise périodiquement des audits de sécurité afin d'évaluer le niveau de sécurité du système d'information sur lequel repose les traitements de données à caractère personnel.
Encadrement contractuel de la sécurité	Une charte informatique ayant force contraignante (annexée au règlement intérieur) est adoptée par l'organisation et prévoit un rappel des règles relatif à la protection des données et les sanctions encourues en cas de non-respect.
Encadrement contractuel de la sécurité	Un engagement de confidentialité est inclus ou annexé au contrat de travail des salariés ayant vocation à manipuler des données à caractère personnel
Sensibilisation des collaborateurs	L'organisation sensibilise ses collaborateurs amenés à manipuler des données à caractère personnel aux risques liés aux libertés et à la vie privée des personnes.
Sensibilisation des collaborateurs	Les procédures d'exploitation en lien avec les données à caractère personnel sont tenues à jour et rendues disponibles à tous les collaborateurs concernés.
Sensibilisation des collaborateurs	L'organisation dispose de politique et outils de classification de l'information définissant plusieurs niveaux.

Sensibilisation des collaborateurs	L'organisation met en place des exercices et des simulations d'incidents en matière de sécurité informatique.
Authentification des utilisateurs	Chaque utilisateur est doté d'un identifiant qui lui est personnel et doit s'authentifier afin de contrôler son identité et ses accès.
Authentification des utilisateurs	L'authentification des utilisateurs basée sur des mots de passe est conforme aux recommandations de la CNIL.
Authentification des utilisateurs	Les utilisateurs sont sensibilisés aux stratégies de choix d'un mot de passe robuste (moyens mnémotechniques, utilisation d'un gestionnaire de mots de passe).
Authentification des utilisateurs	Les utilisateurs sont avertis qu'il ne faut pas divulguer son mot de passe à un autre utilisateur.
Authentification des utilisateurs	Les mots de passe sont chiffrés avec une fonction cryptographique robuste.
Authentification des utilisateurs	L'authentification multifacteur est mise en place pour certains utilisateurs (exemple : administrateurs) ou dans certains contextes (exemple : pour les accès en dehors du réseau de l'organisation).
Authentification des utilisateurs	Le nombre de tentatives d'accès est limité et conduit à un blocage d'accès temporaire en cas d'échecs.
Authentification des utilisateurs	Les mots de passe pour les administrateurs nécessitent une complexité/entropie plus élevée que les autres utilisateurs.
Authentification des utilisateurs	Les mots de passe des administrateurs doivent être régulièrement renouvelés.
Gérer les habilitations	L'organisation a défini des profils d'habilitation dans le système d'information en séparant les tâches et les domaines de responsabilité.
Gérer les habilitations	Les demandes d'habilitation doivent faire l'objet d'une validation par un responsable.
Gérer les habilitations	Les permissions d'accès sont supprimées sans délai lorsque les utilisateurs ne sont plus habilités à accéder à une ressource informatique.
Gérer les habilitations	Une revue régulière annuelle est effectuée pour toutes les habilitations au sein de l'organisation.

Gérer les habilitations	Une procédure d'arrivée (onboarding) et de départ (offboarding) des utilisateurs est mise en place.
Sécurité des postes de travail	Les sessions des utilisateurs sont automatiquement verrouillées en cas de non-utilisation du poste après un certain laps de temps.
Sécurité des postes de travail	Un pare-feu (firewall) logiciel est installé sur chaque poste de travail
Sécurité des postes de travail	Un antivirus mis à jour régulièrement est installé sur chaque poste de travail.
Sécurité des postes de travail	Les mises à jour de sécurité sont déployées au plus tôt et les mises à jour de failles critiques publiques sont réalisées sans délais.
Sécurité des postes de travail	Les droits des utilisateurs sont limités au strict minimum en fonction de leurs besoins.
Sécurité des postes de travail	Le stockage des données des utilisateurs est effectué sur un espace de stockage régulièrement sauvegardé et accessible via le réseau interne de l'organisation. Le stockage des données localement est déconseillé.
Sécurité des postes de travail	Les données présentes sur un poste de travail sont effacées de façon sécurisée avant de réaffecter ledit poste à un autre utilisateur.
Sécurité des postes de travail	Les utilisateurs sont sensibilisés aux risques liés à l'utilisation de supports amovibles.
Sécurité des postes de travail	L'exécution automatique (autorun) des supports amovibles lors de leur insertion sur un poste de travail est désactivée.
Sécurité des postes de travail	Les outils d'administration à distance doivent recueillir l'accord de l'utilisateur avant toute intervention d'assistance sur le poste de travail des utilisateurs.
Sécurité des postes de travail	L'utilisateur doit pouvoir constater l'existence d'une prise de main à distance de son poste de travail en cas d'assistance.
Sécurité des postes de travail	Seule l'exécution d'applications téléchargées depuis des sources sûres (liste blanche) est autorisée.
Sécurité des postes de travail	L'usage d'applications nécessitant des droits de niveau administrateur pour leur exécution est limitée.

Sécurité des postes de travail	Une solution d'analyse et de décontamination des supports amovibles avant chaque utilisation est mise en place.
Sécurité des postes de travail	Lorsqu'un poste de travail est compromis, l'organisation investigate pour trouver la source et déceler toute trace d'intrusion dans le reste du système d'information.
Sécurité des postes de travail	Une veille de sécurité est effectuée sur les logiciels et matériels utilisés dans le système d'information de l'organisme.
Sécurité des postes de travail	Les mises à jour critiques des systèmes d'exploitation sont déployées sans délai en programmant une vérification automatique hebdomadaire.
Sécurité des postes de travail	Les postes de travail sont fixés à du mobilier spécifique ou difficilement déplaçable (câble antivol).
Sécurité des postes de travail	Une liste de diffusion est transmise à l'ensemble des utilisateurs pour les informer de la conduite à tenir et de la liste des personnes à contacter en cas d'incident de sécurité ou de survenance d'un événement inhabituel touchant aux systèmes d'information de l'organisation.
Sécurité de l'informatique mobile	Les utilisateurs sont sensibilisés aux risques spécifiques liés à l'utilisation d'outils informatiques mobiles (vol de matériel, risques liés à la connexion aux réseaux publics, usage d'équipements personnels).
Sécurité de l'informatique mobile	Les contrôles d'accès font l'objet d'un chiffrement des flux d'information (VPN).
Sécurité de l'informatique mobile	Les utilisateurs sont incités à stocker leurs données sur des espaces de stockage partagé pour se prémunir de toute perte ou vol de matériel stockant des données.
Sécurité de l'informatique mobile	Les supports de stockage de l'informatique mobile font l'objet de moyens de chiffrement (chiffrement du disque dur, conteneurs chiffrés, etc.).
Sécurité de l'informatique mobile	Les smartphones nécessitent d'être déverrouillé par un code/une authentification biométrique et le verrouillage automatique est activé.
Sécurité de l'informatique mobile	Les utilisateurs sont informés qu'ils doivent notifier toute perte ou vol de leur matériel et savent à qui s'adresser.

Sécurité de l'informatique mobile	Les risques spécifiques à l'utilisation d'équipements personnels sur le lieu de travail (BYOD) sont identifiés et le BYOD n'est autorisé qu'en fonction des risques spécifiques.
Sécurité de l'informatique mobile	Un système de gestion des appareils mobiles (mobile device management)
Sécurité de l'informatique mobile	Un filtre de confidentialité est installé sur les écrans des postes de travail susceptibles d'être utilisés dans des lieux publics.
Sécurité de l'informatique mobile	Les utilisateurs sont sensibilisés aux mauvaises pratiques dans les lieux publics.
Protection du réseau informatique	Les accès Internet sont limités aux services nécessaires et ceux non nécessaires sont bloqués (ex. : P2P).
Protection du réseau informatique	Les réseaux Wi-Fi sont chiffrés conformément à l'état de l'art (WPA3 ou WPA 2 conformément aux recommandations de l'ANSSI).
Protection du réseau informatique	Les réseaux Wi-Fi publics sont séparés des réseaux internes.
Protection du réseau informatique	Les interfaces d'administration ne sont pas accessibles directement depuis internet et nécessitent une connexion à travers un VPN pour être réalisées à distance.
Protection du réseau informatique	L'administration des équipements réseau s'effectue de façon privilégiée avec un accès physique direct ou via le protocole SSH configuré conformément à l'état de l'art.
Protection du réseau informatique	Les flux réseaux sont limités au strict nécessaire et font l'objet d'un filtrage sur les flux entrants/sortants (pare-feu, serveur proxy).
Protection du réseau informatique	Le réseau est cloisonné afin de réduire l'impact en cas de compromission (réseau interne, réseau DMZ, Gateway).
Protection du réseau informatique	L'identification automatique de matériel est mise en place, sur la base d'une authentification des matériels (protocole 802.1X) ou des adresses MAC des matériels.
Protection du réseau informatique	Un système de détection d'intrusion (IDS) et de prévention d'intrusion (IPS) est déployé sur le réseau.
Sécurité des serveurs	Les services ou interfaces inutilisées sont désinstallées ou

	désactivées.
Sécurité des serveurs	L'accès aux outils et interfaces d'administration est limité aux seules personnes habilitées.
Sécurité des serveurs	Une politique spécifique de mots de passe est adoptée pour les administrateurs.
Sécurité des serveurs	Les mises à jour critiques sont installées sans délai.
Sécurité des serveurs	Des logiciels de détection et de suppression des programmes malveillants est installé et est régulièrement mis à jour.
Sécurité des serveurs	L'accès aux bases de données s'effectue par des comptes nominatifs.
Sécurité des serveurs	Les données stockées sur les serveurs font l'objet de sauvegardes régulières.
Sécurité des serveurs	L'intégrité et la capacité de restauration des données est testée régulièrement.
Sécurité des serveurs	Le protocole TLS est mis en œuvre pour tout échange de données sur Internet.
Sécurité des serveurs	La journalisation des événements système est mise en place.
Sécurité des serveurs	Le traitement de données sensibles est mis en œuvre dans un environnement dédié et isolé du reste du système d'information principal.
Sécurité des serveurs	Les opérations d'administration des serveurs se font sur un réseau dédié et isolé, accessible après une authentification forte.
Sécurité des serveurs	Les flux internes sont chiffrés autant que possible (TLS, IPsec, SSH).
Sécurité des serveurs	Les serveurs obsolètes mais essentiels sont isolés du reste du réseau et le traitement de données à caractère personnel sur ceux-ci est limité dans l'attente de leur remplacement ou mise à jour.
Sécurité des serveurs	Les traitements les plus critiques font l'objet d'une surveillance accrue, notamment par l'utilisation d'outils de détection des vulnérabilités (nmap, nessus, nikto, etc.) ou d'audits.

Sécurité des serveurs	L'accès physique et logique aux ports de diagnostic et de configuration à distance est restreint ou interdit.
Sécurité des serveurs	La version 1.3 de TLS est privilégiée ou la version 1.2. en suivant les recommandations de l'ANSSI.
Sécurité des sites web	Les flux d'échange de données sont sécurisés par l'utilisation du protocole TLS.
Sécurité des sites web	Les ports de communication sont strictement limités au nécessaire pour le bon fonctionnement des applications installées.
Sécurité des sites web	L'accès aux outils et interfaces d'administration est limité aux seules personnes habilitées.
Sécurité des sites web	Le nombre de composants mis en œuvre pour le service web est limité et une veille/mise à jour est réalisée sur ces composants.
Sécurité des sites web	Les informations renvoyées lors de la création d'un compte utilisateur, de la tentative de connexion de la réinitialisation d'un mot de passe sont limitées afin de ne pas renseigner un attaquant sur l'existence d'un compte associé à un identifiant.
Sécurité	Aucune donnée à caractère personnel ne transite dans une URL.
Sécurité	Les niveaux L1 et L2 des recommandations produites par l'OWASP sont respectées.
Sécurité	Les traitements les plus critiques font l'objet d'une surveillance accrue, notamment par l'utilisation d'outils de détection des vulnérabilité (nmap, nessus, nikto, etc.) ou d'audits.
Encadrement des développements informatiques	La protection des données à caractère personnel et la sécurité sont prises en compte dès la conception des applications et services.
Encadrement des développements informatiques	Les composants, bibliothèques et outils choisis sont sécurisés et reconnus comme tel par la communauté.
Encadrement des développements informatiques	Des mesures sont mises en œuvre pour contrer les attaques courantes qui visent les bases de données (telles que : injections de code SQL, scripts, etc.).

Encadrement des développements informatiques	Une réflexion est menée sur le développement des interfaces et des paramètres relatifs à la vie privée afin de respecter les principes de privacy-by-design et privacy-by-design.
Encadrement des développements informatiques	Avant toute mise à disposition ou mise à jour d'une application ou d'un service en ligne, des tests sont réalisés.
Encadrement des développements informatiques	Les développements informatiques et leur recettage sont réalisés dans un environnement informatique distinct de celui de l'environnement de production.
Encadrement des développements informatiques	Les développements informatiques sont réalisés sur des jeu de données fictifs ou anonymisées.
Encadrement des développements informatiques	Des tests de non-régression / une revue de code est réalisée avant la mise en production afin d'éviter l'apparition de sources de violation de données à caractère personnel.
Encadrement des développements informatiques	Appliquer les recommandations de la CNIL en matière de développement informatique (GUIDE RGPD).
Sécurité des locaux	Les accès aux locaux sont restreints au moyen de portes verrouillées.
Sécurité des locaux	Des alarmes anti-intrusion sont installées et leur fonctionnement est vérifié périodiquement.
Sécurité des locaux	Des détecteurs de fumée sont mis en place et inspectés annuellement.
Sécurité des locaux	Des moyens de lutte contre les incendies sont mis en place et inspectés annuellement.
Sécurité des locaux	Les clefs permettant l'accès aux locaux sont protégées.
Sécurité des locaux	Les zones de bâtiments sont distinguées selon les risques et un contrôle d'accès spécifique est dédié pour les salles à risque (coffre-fort, salle informatique).
Sécurité des locaux	Les personnes ou catégories de personnes autorisées à pénétrer dans chaque zone est tenue à jour et une revue périodique est effectuée.

Sécurité des locaux	Les règles et moyens de contrôle d'accès des visiteurs sont établies, notamment en prévoyant l'accompagnement des visiteurs dans les zones en dehors de l'accueil du public.
Sécurité des locaux	L'accès au réseau (prises dans les bureaux, baies de brassage) est protégé et restreint qu'aux équipements autorisés de s'y connecter.
Sécurité des locaux	Les matériels informatiques sont protégés physiquement par des moyens spécifiques (système anti-incendie dédié, surélévation contre les inondations, redondance électrique/climatisation).
Sécurité des locaux	Le personnel accédant aux zones à accès réglementé doit porter un moyen d'identification visible pour toutes les personnes (exemple : badge).
Sécurité des locaux	Les visiteurs ont un accès limité aux locaux, avec un badge visiteur et leur date et heure d'arrivée/de départ est consignée.
Sécurité des locaux	Les permissions d'accès aux zones sécurisées sont mises à jour régulièrement.
Sécurité des échanges avec l'extérieur	Les données devant être transmises sur un support physique font l'objet d'un chiffrement préalable.
Sécurité des échanges avec l'extérieur	Les pièces sensibles à transmettre via un réseau font l'objet d'un chiffrement préalable.
Sécurité des échanges avec l'extérieur	Un protocole garantissant la confidentialité et l'authentification du serveur destinataire (SFTP, HTTPS) est utilisé.
Sécurité des échanges avec l'extérieur	La confidentialité des secrets de chiffrement est assurée par leur transmission via un canal distinct.
Sécurité des échanges avec l'extérieur	Les fichiers provenant de l'extérieur sont ouverts seulement après analyse antivirus.
Encadrement de la sous-traitance	L'organisation fait appel uniquement à des sous-traitants présentant des garanties suffisantes.
Encadrement de la	Un accord de sous-traitance est prévu avec chaque sous-traitant

sous-traitance	conformément au RGPD.
Encadrer la maintenance et la fin de vie des matériels et logiciels	Les interventions de maintenance sont enregistrées dans une main courante.
Encadrer la maintenance et la fin de vie des matériels et logiciels	Les accès nécessaires à la télémaintenance sont ouverts à la demande du prestataire pour une durée adaptée à l'intervention puis refermés.
Encadrer la maintenance et la fin de vie des matériels et logiciels	Une clause de sécurité est insérée dans les contrats de maintenance effectuée par des prestataires accédant au système d'information.
Encadrer la maintenance et la fin de vie des matériels et logiciels	Un responsable de l'organisation est chargé d'encadrer les interventions des tiers.
Encadrer la maintenance et la fin de vie des matériels et logiciels	Les intervenants extérieurs ne sont pas laissés seuls dans les salles sensibles (coffre-fort, salle informatique).
Encadrer la maintenance et la fin de vie des matériels et logiciels	Les données des matériels sont supprimées de façon sécurisée avant leur mise au rebut, leur envoi en réparation ou en fin de contrat de location.
Journalisation	Un système de journalisation des activités métier des utilisateurs, des interventions techniques, des anomalies et des événements liés à la sécurité est mis en œuvre.
Journalisation	La journalisation des événements est conservée sur une période glissante comprise entre 6 mois minimum et un an maximum.
Journalisation	Les opérations de création, consultation, partage, modification et suppression de données sur les applications sont conservées, en y associant l'identifiant de l'auteur, la date, l'heure et la nature de l'opération ainsi que la référence des données concernées.
Journalisation	Les utilisateurs sont informés de l'existence de la journalisation.

Journalisation	Les équipements de journalisation et les informations journalisées sont protégés afin d'empêcher les opérations non autorisées.
Journalisation	La présence des journaux est vérifiée régulièrement et supervisée.
Journalisation	Les journaux sont analysés de manière active, en temps réel ou à court terme afin de détecter la survenance d'un incident.
Journalisation	Faire participer l'utilisateur à la surveillance des opérations faites sur son compte et ses données.
Journalisation	Mettre en place une enclave de collecte centralisant les journaux d'évènements de l'ensemble du système d'information afin d'empêcher leur altération.
Journalisation	Appliquer les recommandations de l'ANSSI en matière de mise en place d'un système de journalisation.
Sauvegardes	L'organisation effectue régulièrement des sauvegardes des données (sauvegardes incrémentales quotidiennes, sauvegardes complètes à intervalles réguliers).
Sauvegardes	L'organisation stocke au moins une sauvegarde sur un site géographiquement distinct du site d'exploitation.
Sauvegardes	Les données sauvegardées sont protégées avec le même niveau de sécurité que celles des serveurs d'exploitation.
Sauvegardes	Le canal de transmission utilisé pour les sauvegardes est chiffré.
Sauvegardes	L'intégrité des sauvegardes et la capacité de l'organisation à les restaurer sont testés régulièrement.
Sauvegardes	L'organisation applique la règle 3 - 2 - 1, consistant à disposer de 3 copies de données, stockées sur 2 supports différents dont 1 hors ligne.
Continuité et reprise d'activité	L'organisation a rédigé un plan de continuité (PCA).
Continuité et reprise d'activité	L'organisation a rédigé un plan de reprise d'activité.
Continuité et reprise d'activité	Les utilisateurs, prestataires et sous-traitants savent qui alerter au sein de l'organisation en cas d'incident.

Continuité et reprise d'activité	La restauration des sauvegardes et l'application du PCA/PRA est testée régulièrement.
Continuité et reprise d'activité	Un onduleur protège le matériel servant aux traitements essentiels.
Continuité et reprise d'activité	Une redondance matérielle des équipements de stockage est réalisée (type RAID).
Continuité et reprise d'activité	L'organisation a défini une organisation de gestion de crise.
Continuité et reprise d'activité	L'organisation réalise des exercices avec toutes les parties prenantes pour vérifier l'efficacité et l'assimilation des procédures mises en place.
Gestion des incidents et des violations	L'organisation analyse régulièrement les traces collectées par la journalisation.
Gestion des incidents et des violations	Les gestionnaires du dispositif de journalisation notifient dans les plus brefs délais l'organisation en cas d'anomalie ou d'incident de sécurité.
Gestion des incidents et des violations	Les utilisateurs sont informés de la conduite à tenir et de la liste des personnes à contacter en cas d'incident de sécurité ou de survenance d'un évènement inhabituel.
Gestion des incidents et des violations	L'organisation a établi une procédure détaillant les dispositifs de remontée des alertes et les actions à mener en cas d'incident avéré.
Gestion des incidents et des violations	L'organisation sait évaluer les risques pour les personnes engendrés par la violation.
Gestion des incidents et des violations	L'organisation tient un registre interne de toutes les violations de données à caractère personnel.
Gestion des incidents et des violations	L'organisation notifie à la CNIL dans les 72 heures les violations présentant un risque pour les droits et libertés des personnes et, informe les personnes concernées en cas de risque élevé.
Analyse de risques	L'organisation identifie les traitements de données à caractère personnel pour lesquels une AIPD est requise.

Chiffrement	L'organisation utilise des algorithmes de chiffrement reconnus et sûrs, tels que SHA-2/SHA-3, bcrypt,scrypt,Argon2, PBKDF2, AES, ChaCha20, RSA-OAEP, ECIES-KEM, DLIES-KEM, RSA-SSA-PSS, ECDSA.
Chiffrement	L'organisation utilise des tailles de clés suffisantes.
Chiffrement	L'organisation protège les clés secrètes, a minima par la mise en œuvre de droits d'accès restrictif et d'un mot de passe sûr.
Chiffrement	L'organisation tient à jour une procédure indiquant la manière dont les clés et certificats vont être gérés, notamment en cas d'oubli du mot de passe de déverrouillage.
Cloud	L'organisation cartographie les données et les traitements effectués dans le cloud et maintient à jour cette cartographie.
Cloud	L'organisation prend en compte les services cloud dans son analyse de risques (20) et dans sa continuité et reprise d'activité (18).
Cloud	L'organisation formalise les obligations de sécurité et la répartition des responsabilités avec ses fournisseurs dans un contrat (14).
Cloud	L'organisation vérifie que les acteurs impliqués dans la fourniture des services cloud maintiennent le niveau de sécurité recherché.
Sécurité du développement d'applications mobiles	L'organisation veille à minimiser les traitements de données à caractère personnel mis en œuvre.
Sécurité du développement d'applications mobiles	L'organisation sécurise les communications entre l'application mobile et les serveurs. Les secrets cryptographiques sont stockés par empaquetage au moyen d'API permettant l'utilisation des suites crypto (Hardware KeyStore d'Android, Secure Enclave d'Apple).
Sécurité du développement d'applications mobiles	L'organisation prend en compte la possibilité que le système d'exploitation effectue des sauvegardes automatiques des données personnelles.
Sécurité du développement d'applications	L'organisation recourt à un moyen d'authentification correspondant au niveau de sécurité recherché.

mobiles	
Sécurité de l'IA - Conception et apprentissage	Constituer une équipe de développement aux compétences pluridisciplinaires (analyse et ingénierie des données, interface et expérience utilisateur, contrôle qualité, administration des infrastructures informatiques, équipes métier), veiller à sa formation sur les bonnes pratiques de sécurité et sensibiliser aux vulnérabilités propres à l'IA.
Sécurité de l'IA - Conception et apprentissage	Mettre en œuvre une procédure obligatoire pour le développement et l'intégration continus, reposant sur des tests exhaustifs et robustes, des accès soumis à habilitation et à une authentification adaptée aux profils
Sécurité de l'IA - Conception et apprentissage	Vérifier la qualité des données et des annotations, la présence possible de biais, la fiabilité des sources de données, notamment afin d'éviter que les données ne puissent être manipulées par un tiers (ex. : empoisonnement).
Sécurité de l'IA - Conception et apprentissage	Éviter les copies, partielles ou totales, des bases de données et en restreindre l'accès et l'utilisation aux seules personnes habilitées pour des cas le nécessitant.
Sécurité de l'IA - Conception et apprentissage	Recourir à des données fictives ou de synthèse dans les autres cas, comme pour les tests de sécurité, l'intégration, ou pour certains audits.
Sécurité de l'IA - Conception et apprentissage	Construire un recueil documentaire à l'intention des développeurs et des utilisateurs du système.
Sécurité de l'IA - Conception et apprentissage	Vérifier la légitimité des utilisateurs du système lorsque celui-ci est rendu disponible en tant que service, afin d'éviter une tentative d'attaque telle qu'une attaque par inversion de modèle ou par déni de service.
Sécurité de l'IA - Conception et apprentissage	Prévoir un plan d'audit du système, portant sur les éléments logiciels, matériels, et sur les mesures organisationnelles telles que les procédures de supervision humaine du système d'IA.
Sécurité des API	Identifier les acteurs et leur rôle fonctionnel (détenteur de données, gestionnaire d'API, réutilisateur) afin d'organiser le périmètre d'attribution de chacun en matière d'accès aux API et aux données.

Sécurité des API	Limiter le partage aux données strictement nécessaires, uniquement aux personnes et pour les finalités prévues, en application du principe de minimisation.
Sécurité des API	Créer une séparation entre les appels aux fonctions courantes de l'API et ceux dédiés à son administration, pour lesquels une authentification robuste apparaît nécessaire.
Sécurité des API	Disposer de journaux pertinents afin de tracer les échanges et de détecter et réagir en cas d'une utilisation détournée de l'API, d'accès illégitime aux données, d'un dépassement de la capacité d'accès ou de tout autre comportement inhabituel
Sécurité des API	Maintenir à jour la documentation. Celle-ci doit inclure le format des requêtes et des données concernées par le partage afin de limiter le risque d'une erreur d'interprétation.
Sécurité des API	Avant la mise en production d'une API, vérifier sa résistance aux risques publiés par l'OWASP dans son Top 10 API.
Sécurité des API	Une version « bac à sable » de l'API devrait être mise à disposition afin de permettre des expérimentations et de tester les résultats attendus à partir de données fictives. Document référence