ANNEXE 2 : TRAITEMENT DES DONNÉES A CARACTÈRE PERSONNEL

La présente annexe (« l'annexe ») fait partie intégrante de la convention tripartite relative au dépôt et à la conservation sécurisée d'archives numériques dans le système d'archivage électronique de la plateforme SESAM pour les collectivités du département de la Somme (« la convention »).

Les présentes clauses ont pour objet de définir les conditions dans lesquelles l'Autorité d'archivage (ci-après « le sous-traitant ») s'engage à effectuer pour le compte de l'Autorité juridique (ci-après « le responsable de traitement ») les opérations de traitement de données à caractère personnel définies ci-après.

L'Autorité juridique est responsable de traitement, à ce titre elle définit les finalités, les moyens de collecte et de traitement des données à caractère personnel. L'autorité juridique délègue à l'Autorité d'archivage des activités de traitement définies ci-après.

Chaque partie s'engage à respecter la réglementation en vigueur applicable au traitement de données à caractère personnel et, en particulier, le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 applicable à compter du 25 mai 2018 (ci-après, « ***le règlement européen sur la protection des données*** »).

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

L'Autorité d'archivage est autorisée à traiter pour le compte de l'Autorité juridique les données à caractère personnel nécessaires pour fournir le ou les service(s) suivant(s) : Système d'archivage électronique (SAE) dénommé Système électronique sécurisé d'archivage mutualisé (SESAM), lequel a fait l'objet d'un agrément délivré par arrêté de la préfecture du Nord.

Les finalités du traitement sont :

- dépôt d'archives électroniques de l'Autorité juridique dans le SAE-SESAM ;
- conservation d'archives numériques courantes et intermédiaires de l'Autorité juridique dans le SAE-SESAM ;
- communication des archives transférées selon les délais de communicabilité applicables ;
- élimination des archives numériques visées par les Archives départementales de la Somme ;
- traitement des demandes de restitution partielle ou totale à l'initiative de l'Autorité juridique ou de l'Autorité d'archivage.

Les activités de traitement déléguées par le responsable de traitement sont celles prévues à l'article 6 de la convention.

Les finalités et moyens de traitements, les types de données à caractère personnel collectées et les catégories de personnes concernées sont déterminées par l'Autorité juridique, responsable de traitement.

Les activités de traitement sont effectuées par l'Autorité d'archivage pour le compte de l'Autorité juridique, responsable des traitements pour la durée prévue à la Convention.
Les contrats de dépôt mentionnés à l'article 4 de la convention de dépôt, précise, en cas de données à caractère personnel, les éléments fournis par l'Autorité juridique responsable du traitement :

- l'objet, la nature et la finalité du traitement ;
- le type de données ;
- les catégories de personnes ;
- la durée de conservation des données.

II. Obligations de l'Autorité d'archivage

L'Autorité d'archivage s'engage à :

1. traiter les données uniquement pour les seules finalités **définies par l'Autorité juridique** qui font l'objet de la sous-traitance.

2. traiter les données conformément aux instructions de l'Autorité juridique. Si l'Autorité d'archivage considère qu'une instruction constitue une violation du règlement européen sur la protection des données ou de toute autre disposition du droit de l'Union ou du droit des États membres relative à la protection des données, elle en informe immédiatement l'Autorité juridique, le délégué à la protection des données de l'Autorité juridique et tout autre personne désigné par l'Autorité juridique.

3. garantir la confidentialité des données à caractère personnel traitées.

4. veiller à ce que les personnes autorisées à traiter les données à caractère personnel :

- s'engagent à respecter la confidentialité ;
- reçoivent la formation nécessaire en matière de protection des données à caractère personnel.

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

6. Sous-traitance
L'Autorité d'archivage est expressément autorisée à faire appel à un autre sous-traitant (ci-après, « le sous-traitant ultérieur ») pour mener des activités de traitement de données à caractère personnel dans le cadre de la convention. La liste des sous-traitants ultérieurs est disponible sur demande auprès de l'Autorité d'archivage.

L'Autorité d'archivage s'engage à informer l'Autorité juridique de tout changement envisagé concernant l'ajout ou le remplacement de sous-traitants ultérieurs par courrier postal ou électronique dans les plus brefs délais. Cette information indique les activités de traitement sous-traitées, l'identité et les coordonnées du sous-traitant ultérieur. L'Autorité juridique dispose de la faculté, en cas d'objection, de procéder à la dénonciation de la convention dans les conditions prévues à l'article 9 – Durée et dénonciation de la convention.

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

7. Droit d'information des personnes concernées
Il appartient au responsable de traitement de fournir l'information aux personnes concernées par les opérations de traitement au moment de la collecte des données.

8. Exercice des droits des personnes
Dans la mesure du possible, l'Autorité d'archivage doit aider l'Autorité juridique à s'acquitter de ses obligations de donner suite aux demandes d'exercice des droits des personnes concernées : droit d'accès, de rectification, d'effacement et d'opposition, droit à la limitation du traitement, droit à la portabilité des données, droit de ne pas faire l'objet d'une décision individuelle automatisée (y compris le profilage).
Lorsque la demande de la personne concernée est adressée directement à l'Autorité d'archivage, cette dernière doit en informer l'Autorité juridique ainsi que le délégué à la protection des données de l'Autorité juridique dans les plus brefs délais. L'Autorité d'archivage, en qualité de sous-traitant, s'engage à ne pas donner droit à la demande sans instruction écrite de l'Autorité juridique (art. 28-3

a et 29 du Règlement européen sur la protection des données et art. 61 de la Loi Informatique et Libertés).

9. Notification des violations de données à caractère personnel
L'Autorité d'archivage s'engage à prendre toutes les mesures nécessaires pour remédier à une situation de violation de données à caractère personnel ou de plainte.

Ainsi, l'Autorité d'archivage s'engage à communiquer à l'Autorité juridique la survenance de toute faille de sécurité, perte de données et d'incident ayant des conséquences sur les droits et libertés des personnes concernées, ainsi que toute plainte qui lui serait adressée par tout individu concerné par le traitement réalisé dans le cadre des présentes. Cette communication devra être effectuée dans les plus brefs délais et au maximum quarante-huit heures après la découverte de la faille de sécurité ou suivant réception d'une plainte.

Cette communication devra être accompagnée de toute documentation utile afin de permettre à l'Autorité juridique d'agir en conséquence et de décider éventuellement, de notifier cette violation à l'Autorité de contrôle compétente.

10. Aide de l'Autorité d'archivage dans le cadre du respect par l'Autorité juridique de traitement de leurs obligations
L'Autorité d'archivage aide l'Autorité juridique pour la réalisation d'analyses d'impact relative à la protection des données et affairant à l'objet de la convention.

11. Mesures de sécurité
L'Autorité d'archivage et l'opérateur d'archivage technique mettent en œuvre des mesures de sécurité techniques et organisationnelles garantissant la confidentialité, l'intégrité et la sécurité des données à caractère personnel incluant la protection contre :

- les accès non autorisés ou contre la mise en œuvre de traitements contraires à la réglementation ;
- les destructions accidentelles ou malveillantes ;
- les atteintes à la confidentialité, la disponibilité ou à l'intégrité ;
- la diffusion ou l'accès non autorisée aux données à caractère personnel.

L'opérateur d'archivage technique et ses sous-traitants ultérieurs mettent en œuvre et / ou se conforment aux mesures techniques et organisationnelles suivantes :

- des mesures de sécurité physique destinées à empêcher les personnes non autorisées d'accéder à l'infrastructure SESAM dans laquelle les données des Autorités juridiques sont stockées ;
- des contrôles d'identité et d'accès au moyen d'un système d'authentification et d'une politique en matière de mots de passe ;
- un système de gestion des accès qui limite l'accès aux locaux, aux personnes ayant besoin d'y accéder dans l'exercice de leurs fonctions et dans le cadre de leurs responsabilités ;
- une surveillance continue par l'opérateur technique d'archivage des opérations et interventions réalisées, sur site ou à distance, par les sous-traitants ultérieurs sur le système d'information SESAM ;
- une architecture technique et fonctionnelle qui isole physiquement et/ou de façon logique les différentes Autorité juridiques les unes des autres ;
- des processus d'authentification des utilisateurs et des administrateurs fonctionnels basés sur des moyens d'authentification forte (certificat RGS** minimum), ainsi que des mesures visant à protéger l'accès aux fonctions d'administration fonctionnelles et techniques ;
- le chiffrement systématique des échanges de données ;
- la mise en œuvre de systèmes visant à prévenir et bloquer les tentatives d'intrusion à distance sur le système d'information SESAM ;
- des processus et des mesures de suivi de toutes les actions effectuées sur le système d'information SESAM ;

- la réalisation d'audits de sécurité et des tests de pénétrations réguliers du système d'information SESAM.

A ce titre, l'Autorité d'archivage tient à la disposition de l'Autorité juridique les documents relatifs à sa politique de sécurité des données.

12. Transfert des données
Les données à caractère personnel traitées en vertu des présentes ne font pas l'objet d'un transfert hors de France conformément à la réglementation en vigueur sur les archives publiques françaises.

13. Sort des données
L'Autorité d'archivage s'engage, au terme de la Convention ou en cas de rupture anticipée qu'elle que soit la cause, à détruire l'ensemble des données à caractère personnel traitées durant la convention, après les avoir restituées à l'Autorité juridique ou au prestataire désigné par cette dernière dans les conditions définies dans la convention. Cette restitution sera constatée par procès-verbal daté et signé par les Parties.
Une fois la restitution effectuée, l'Autorité d'archivage détruira les copies des données détenues dans ses systèmes informatiques dans un délai raisonnable qui ne devra pas excéder 4 mois maximum.

14. Délégué·e à la protection des données
L'Autorité d'archivage désignera un·e délégué·e à la protection des données et communiquera à l'Autorité juridique son nom et ses coordonnées, conformément à l'article 37 du règlement européen sur la protection des données.

15. Registre des catégories d'activités de traitement
L'Autorité d'archivage déclare tenir par écrit un registre de toutes les catégories d'activités de traitement effectuées dans le cadre des présentes et comprenant :

- le nom et les coordonnées du responsable de traitement pour le compte duquel elle agit, des éventuels sous-traitants et, le cas échéant, du délégué à la protection des données ;

- les catégories de traitements effectués pour le compte du responsable du traitement ;

- dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles.

16. Audit
L'Autorité d'archivage met à la disposition de l'Autorité juridique les informations nécessaires pour démontrer la conformité aux exigences du RGPD et mener des audits. Si les informations s'avèrent insuffisantes pour permettre de démontrer que les obligations prévues par le RGPD sont remplies, l'Autorité d'archivage et l'Autorité juridique se réunissent alors pour convenir des conditions opérationnelles, sécuritaires et financières d'un audit technique sur site.

L'audit doit permettre notamment de vérifier l'ensemble des mesures de sécurité et de confidentialité mises en œuvre par l'Autorité d'archivage et de s'assurer que ces mesures ne peuvent être contournées sans que cela ne soit détecté et notifié.

L'Autorité juridique s'engage à ne procéder à cet audit qu'en heures et jours ouvrés.

L'Autorité juridique s'engage à fournir à l'Autorité d'archivage une copie du rapport d'audit afin qu'elle puisse prendre en compte rapidement les non-conformités constatées et les mesures correctives proposées.

L'Autorité d'archivage s'engage à mettre en œuvre les mesures correctives nécessaires au traitement des non-conformités identifiées dans un délai et selon les conditions définies d'un commun accord.

Dans le cas ou des mesures correctives ne seraient pas applicables, l'Autorité d'archivage s'engage à justifier de l'impossibilité de mettre en œuvre les mesures et s'engage à proposer des mesures palliatives pour réduire les risques encourus.

III. Obligations de l'Autorité juridique

L'Autorité juridique s'engage à :

1. déposer auprès de l'Autorité d'archivage des données à caractère personnel collectées de manière licite, loyale, transparente et proportionnée par rapport aux finalités de traitement déterminées par le responsable de traitement ;
2. documenter par écrit toute instruction en vue des activités de traitement des données par l'Autorité d'archivage ;
3. veiller, au préalable et pendant toute la durée du traitement, au respect des obligations prévues par le règlement européen sur la protection des données de la part de l'Autorité d'archivage.

IV. Obligation de conseil de l'Autorité d'archivage

L'Autorité d'archivage s'engage à conseiller l'Autorité juridique sur l'application du Règlement Général de Protection des Données dès lors qu'elle considère qu'une non-conformité peut avoir un impact sur le respect des présentes clauses.

V. Communication à des tiers autorisés

L'Autorité d'archivage s'engage à informer sans délai l'Autorité juridique en cas de requête provenant d'une autorité administrative ou judiciaire demandant à avoir communication de données à caractère personnel entrant dans le périmètre de la convention et de ses annexes.
Dans le cas où la requête est reçue par l'Autorité juridique, l'Autorité d'archivage s'engage à mettre en œuvre les moyens permettant de répondre à la demande dans les délais exigés sur le périmètre des opérations de traitement sous-traitées.

VI. Devoir de coopération avec l'Autorité de contrôle compétente en matière de protection des données (CNIL)

L'Autorité d'archivage s'engage à coopérer avec l'Autorité de contrôle compétente en matière de protection des données (CNIL), notamment en cas de demande d'information qui pourrait être adressée par cette dernière, ou en cas de contrôle sur site ou à distance des opérations sous-traitées.
En cas de contrôle d'une autorité compétente chez l'Autorité juridique portant notamment sur les prestations réalisées par l'Autorité d'archivage, cette dernière s'engage à coopérer avec l'Autorité juridique à lui fournir les informations dont cette dernière pourrait avoir besoin ou qui s'avéreraient nécessaires.