Annexe

à la convention relative aux modalités d'organisation concernant la plateforme de services numériques mutualisés pour la lecture publique (bibliothèques/réseaux de bibliothèques)

PROTECTION DES DONNEES ET OBLIGATIONS

CONFIDENTIALITE, SECURITE, PROTECTION DES DONNÉES

Dans le cadre de leurs relations contractuelles, les parties sont soumises aux dispositions de l'article 226-21 et suivants du Code Pénal et s'engagent à respecter la réglementation en vigueur applicable au traitement de données à caractère personnel et, en particulier, le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 en vigueur (ci-après dans le texte, « *le règlement européen ou RGPD*»).

Chaque partie à la convention est tenue au respect des règles relatives à la protection des données nominatives, auxquelles elle a accès pour ses besoins de gestion, notamment les grands principes posés de protection des données personnelles depuis la collecte jusqu'à l'épuration et les moyens de sécurité adaptés aux risques.

Sont désignées « parties » ci-après dans le texte le Département, l'ADIT63, les membres adhérents de l'ADIT63, la société PROGILONE en tant que titulaire de l'accord cadre n°18.222.

1. Finalité du traitement de données personnelles

La finalité principale du traitement (objet de l'accord cadre) porte sur la mise en œuvre d'une plateforme de services numériques mutualisés à l'usage de la médiathèque départementale du Puy-de-Dôme et autres bibliothèques/médiathèques partenaires adhérentes sur le territoire départemental.

La solution de gestion informatisée SYRTIS de la société PROGILONE a été retenue à l'accord cadre pour l'implantation de cette plateforme incluant toutes les prestations de paramétrage, configuration, intégration des données, et un hébergement en mode SAAS des données de l'application.

Le traitement a pour objet principal la mise en place d'une plateforme de services numériques mutualisés (réseau de bibliothèques/médiathèques partenaires) pour la gestion de leur fonds documentaire matériel et immatériel et de leurs usagers, pour leur portail web et les divers services numériques proposés (envoi de news letter, diffusion sélective d'actualités, inscriptions à des animations, consultation de son compte d'abonné etc.) et la production de statistiques à usage interne pour le suivi d'activité ou pour établir le rapport annuel obligatoire destiné au Ministère de la Culture.

La plateforme de services mutualisés permet également un pilotage centralisé de la solution applicative pour les bibliothèques/médiathèques partenaires, pour faciliter et optimiser leur accès au fonds documentaire matériel et immatériel (fonds propre à chaque partenaire ou fonds commun départemental), la gestion des bases de données (fonds documentaires, utilisateurs, emprunts individuels, création et gestion de comptes en ligne…).La plateforme proposera également au public un inventaire en ligne des lieux de lecture publique du département.

Les accès à la plateforme de services mutualisés seront configurés pour permettre une confidentialité entre les partenaires et leurs usagers.

Les données à caractère personnel collectées auprès des usagers des bibliothèques/médiathèques pour procéder à leur adhésion sur site (formulaire papier) ou en ligne (formulaire en ligne) pour la création d'un compte utilisateur sont de nature usuelle pour gérer une inscription :

- Usagers : nom, prénom, sexe, adresse, date de naissance, CSP, bibliothèque de rattachement principal.
- Pour les mineurs : représentant légal, autorisation du représentant légal et accord pour l'accès au portail web et à la Médiathèque Numérique du Puy-de-Dôme.
- Facultatif : Téléphones, adresses de messageries électroniques.

D'autres données à caractère personnel peuvent être également collectées auprès de professionnels : (qualification, situation professionnelle) pour la gestion des contacts (agents des bibliothèques/médiathèques partenaires…).

2. Statut des parties à la convention d'adhésion

Le statut des parties à la présente convention ainsi que leurs obligations en matière de protection des données personnelles résultent d'une part du règlement général sur la protection des données 2016/679 du Parlement Européen et du Conseil du 27 avril 2016 et de la nature de leur position respective pour la mise en œuvre du traitement d'autre part.

Dans ce contexte, au sens RGPD qui prévoit diverses obligations en fonction du statut, il est précisé que :

- Le Département du Puy-de-Dôme, l'ADIT63 pour le compte de ses adhérents, membres du groupement de commandes, sont stipulés co-traitants au traitement, co-responsables dans sa mise en œuvre sur le périmètre qui les concerne, contractualisé par l'accord cadre 18 .222.

A ce titre, les membres adhérents de l'ADIT63 (bibliothèques/médiathèques partenaires) intégrant le dispositif relèvent de ce même statut et sont stipulés co-responsables dans la mise en œuvre sur le périmètre qui les concerne.

- La société PROGILONE, détentrice des droits éditeur sur la solution de gestion constituée d'une plateforme de services mutualisés, titulaire de l'accord cadre n°18.222, relève du statut de sous-traitant.

3. Obligations des parties

Chacune des parties s'engage à mettre en œuvre les moyens organisationnels et techniques appropriés pour garantir, chacun pour ce qui le concerne et sous son entière responsabilité, l'accessibilité, la confidentialité, l'intégrité et la sécurité des données personnelles.

Le Département, l'ADIT63 et les membres adhérents de l'ADIT63 demeurent propriétaires des données qu'ils renseignent dans l'applicatif.

1°) obligations des membres du groupement de commandes (Département/ADIT63) : les obligations relevant du responsable du traitement (co-responsabilité) ont été fixées au marché initial, à savoir donner des instructions au titulaire PROGILONE sur les mises en conformité à prévoir en terme de configuration de la solution applicative pour respecter l'information des

personnes, sensibiliser les personnels, respecter la confidentialité des données, s'assurer de leur archivage, destruction, sécurité.

Les membres du groupement de commandes s'engagent à proposer aux membres adhérents de l'ADIT63 une solution applicative à jour des mises en conformité. Aucune demande d'adaptation de paramétrage, de configuration…dérogeant à ces mises en conformité ne pourra être acceptée.

Le Département et l'ADIT 63 consulteront s'il y a lieu leur délégué à la protection des données pour toute question relative à la mise en application de la réglementation européenne dans le traitement, objet de la présente convention.

Les sécurités proposées tant sur le socle technique qu'en terme de paramétrage de l'application par PROGILONE ont été validées par les membres du groupement de commandes préalablement à la signature de l'accord cadre. Toute nouvelle adhésion d'un partenaire donnera lieu à vérification/validation des sécurités lors de l'intégration technique.

2°) obligations des membres adhérents de l'ADIT63 (Bibliothèques/médiathèques accédant au réseau) du fait de leur statut de co-responsable.

Chaque membre adhérant à la plateforme de services mutualisés s'engage à :

- consigner le traitement sur son propre registre des traitements

- mettre en place une rubrique « mentions légales » sur sa page d'accès via la plateforme de services, accessible par le public, sur laquelle seront précisées toutes les informations et coordonnées obligatoires relatives au site internet.

- informer ses usagers par tous moyens sur leurs droits d'accès, les modalités d'exercice de ce droit, par tous moyens cumulés (mentions légales, affiches, formulaires papier ou en ligne, oralement si nécessaire...), l'objet du traitement de données personnelles et la diffusion éventuelle de ces données à des tiers.

- ne pas utiliser les informations personnelles traitées pour d'autres finalités (autre objet) que celles pour lesquelles elles ont été collectées, ni les divulguer à autrui sans consentement explicite des personnes.

- prendre toute mesure organisationnelle assurant la confidentialité des données personnelles de ses usagers : ne prendre et ne diffuser aucune copie des documents, supports d'informations, éditions, statistiques sans précautions d'usage et de confidentialité et ne les utiliser que pour répondre aux besoins de son activité.

- se préoccuper en s'informant auprès des membres du groupement, de la confidentialité, l'intégrité des données personnelles hébergées sur les serveurs du titulaire, la disponibilité et la résilience constante des systèmes et des services de traitement (gestion des habilitations et droits d'accès…), de l'organisation de tests sur leurs données et des mesures de sécurité technique proposées sur la plateforme et sur les serveurs du titulaire PROGILONE.

- se préoccuper auprès des membres du groupement des procédures prévues de relevés d'événements (traçabilité…), d'audit d'une faille de sécurité avec notification à l'autorité de contrôle

- sensibiliser/former ses personnels de ses propres obligations sur la protection des données à caractère personnel

- respecter les règles d'archivage des données au titre du code du patrimoine, à épurer les données de ses usagers, les en informer suivant des règles de conservation imposées soit par la plateforme de services mutualisés soit le cas échéant suivant ses propres critères pertinents de conservation.

- demander au terme de la convention, des éventuels contrats d'abonnement Saas et supports ultérieurs, la restitution de ses données assortie de la destruction de toutes les copies existantes dans le SI du prestataire PROGILONE, du Département et de l'ADIT63 s'il y a lieu. Le renvoi conforme des données, validé par le membre adhérent, donnera lieu à un PV attestant de cette destruction.

Chaque membre adhérent engage seul sa responsabilité pleine et entière en cas de non-respect, de son fait, des dispositions de la règlementation européenne. Il pourra être alerté le cas échéant sur tout manquement détecté à ses obligations RGPD, par les membres du groupement ou le titulaire PROGILONE, en conformité avec la règlementation européenne.

Les sécurités proposées par le sous-traitant PROGILONE sur le socle commun, technique et/ou applicatif, sont réputées acceptées par chaque membre adhérent. Des suggestions, améliorations de sécurité pourront être demandées sous réserve de validation par les membres du groupement de commandes et faisabilité technique.

3°) Obligations du sous-traitant : PROGILONE est amené à héberger et traiter sur instruction du groupement de commandes, des données personnelles émanant des usagers des membres du groupement (Département, ADIT63 et membres adhérents de l'ADIT63), conformément aux clauses contractuelles de l'accord cadre n°18.222.

A l'identique des autres parties, PROGILONE est soumis aux clauses du RGPD et de l'article 226-21 et suivants du code pénal pour le traitement des informations et données personnelles qui lui sont confiées et pour lesquelles il s'est engagé à apporter des garanties de conformité, de confidentialité, de sécurité.

Dans la mesure où PROGILONE héberge selon ses propres moyens sa solution applicative (plateforme de services mutualisés), complétée des données renseignées par les parties (Département, ADIT63, membres adhérents de l'ADIT63), il garantit à l'ensemble des cocontractants à sa solution applicative qu'il a procédé aux obligations lui incombant au titre de la loi informatique et liberté et du RGPD, ceci en rappel de ses obligations fixées à l'accord cadre n°18.222 *(cf. en annexe1 -extrait pour information -clauses CCAP de l'accord cadre n° 18.222 « confidentialité, protection des données »)*

« *Extrait pour information :* clauses du CCAP de l'accord cadre n° 18.222 relatives à la confidentialité et aux obligations du titulaire PROGILONE en matière de protection des données»

Extrait :

…..

15.3 – Confidentialité

Les parties qui, à l'occasion de l'exécution de l'accord-cadre, ont connaissance d'informations ou reçoivent communication de documents ou d'éléments de toute nature, signalés comme présentant un caractère confidentiel et relatifs, notamment, aux moyens à mettre en oeuvre pour son exécution, au fonctionnement des services, sont tenus de prendre toutes mesures nécessaires, afin d'éviter que ces informations, documents ou éléments ne soient divulgués à un tiers qui n'a pas à en connaître, sur la durée de l'accord-cadre et même au-delà.

Une partie ne peut demander la confidentialité d'informations, de documents ou d'éléments qu'elle a elle-même rendus publics. Ne sont pas couverts par cette obligation de confidentialité les informations, documents ou éléments déjà accessibles au public, au moment où ils sont portés à la connaissance des parties à l'accord-cadre.

Le titulaire doit informer ses sous-traitants des obligations de confidentialité et des mesures de sécurité qui s'imposent à lui pour l'exécution de l'accord-cadre. Il doit s'assurer du respect de ces obligations par ses sous-traitants.

15.4 – Protection des données à caractère personnel

Les présentes clauses ont pour objet de définir les conditions dans lesquelles le titulaire s'engage à effectuer pour le compte du groupement de commandes les opérations de traitement de données à caractère personnel ou à participer à ces opérations.

Les parties s'engagent à respecter la réglementation en vigueur applicable au traitement de données à caractère personnel et, en particulier, le règlement (UE) 2016/679 du Parlement européen **applicable à compter du 25 mai 2018** (ci-après libellé « le règlement européen sur la protection des données » ou « RGPD»).

Pour l'exécution du présent accord-cadre, les membres du groupement de commandes mettent à la disposition du titulaire les informations nécessaires suivantes : fiche du registre et annexe, documentations utilisateurs, procédures, notes, et tout autre document utile. Les données contenues dans ces supports et documents sont strictement couvertes par le secret professionnel (article 226-13 du code pénal).

15.4.1 Sous-traitance du titulaire de l'accord-cadre (au sens RGPD)

Le titulaire est autorisé à connaître, à accéder et traiter, pour le compte des membres du groupement de commandes, les données à caractère personnel nécessaires à la mise en place des services décrits au cahier des clauses techniques particulières ayant pour finalité principale la mise en oeuvre d'une plateforme de services numériques en mode SaaS permettant notamment :

- la gestion de la plateforme par les agents publics, la consultation via internet de fonds documentaires par les usagers et leur gestion de compte (tout public : abonnés de la médiathèque départementale et autres médiathèque/bibliothèque du réseau), ainsi que des services d'hébergement externalisé des données et d'assistance technique.

Le titulaire peut faire appel à un autre sous-traitant (sous-traitant ultérieur) pour mener des activités de traitement spécifiques (expertise, accompagnement technique…). Dans ce cas, il informe préalablement et par écrit le représentant de chaque membre du groupement de commandes de tout changement envisagé (ajout ou remplacement par d'autres sous-traitants). Celui-ci dispose d'un délai minium de 1 mois à compter de la date de réception de cette information pour présenter ses objections et lui faire connaître ou non son acceptation du sous-traitant.

Le sous-traitant ultérieur est tenu de respecter les obligations du présent contrat pour le compte et selon les instructions des membres du groupement de commandes. Il appartient au titulaire de s'assurer que le sous-traitant ultérieur présente les mêmes garanties suffisantes quant à la mise en oeuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du règlement européen sur la protection des données.

Si le sous-traitant ultérieur ne remplit pas ses obligations en matière de protection des données, le titulaire demeure pleinement responsable devant les membres du groupement de commandes du non-respect desdites obligations par son sous-traitant.

15.4.2 Protection et utilisation des données à caractère personnel

Le titulaire s'engage à :

☐ Traiter les données uniquement pour les seules finalités définies par l'accord-cadre et s'interdit tout autre usage à son initiative.

☐ Traiter les données conformément à ses engagements et autres termes de son offre notifiée par le groupement de commandes notamment sur la partie hébergement de données sur le territoire national.

☐ Garantir la confidentialité des données à caractère personnel traitées dans le cadre du présent accord-cadre étendue à ses propres intervenants, ses sous-traitants ultérieurs et en veillant à :

- ne prendre aucune copie des documents et supports d'informations confiés, à l'exception de celles nécessaires pour les besoins de l'exécution de sa prestation, objet du présent accord-cadre ;

- ne pas utiliser les documents et informations traités à des fins autres que celles spécifiées au présent accord-cadre ;

- ne pas divulguer ces documents ou informations à d'autres personnes, qu'il s'agisse de personnes privées ou publiques, physiques ou morales ;

- prendre toutes mesures permettant d'éviter toute utilisation détournée ou frauduleuse des fichiers de données en cours d'exécution de l'accord-cadre ;

- prendre des mesures de protection identiques lors des essais et tests prévus au présent accord-cadre pour la mise en place des services.

- sensibiliser/former ses intervenants, les sous-traitants en matière de protection des données à caractère personnel préalablement à l'exécution des prestations

☐ Prendre en compte dans les déploiements de sa solution technique (fonctionnalités et outils proposés), les grands principes posés par le règlement européen sur la protection des données personnelles ceci dès la conception ou recueil de la donnée jusqu'à son épuration.

☐ Conseiller et accompagner les membres du groupement sur ces dispositions

☐ Fournir une solution technique permettant de répondre à l'exigence de transparence (ex : zone d'affichage d'information des personnes, le texte publié étant du ressort des membres du groupement,

désabonnement sur les comptes utilisateurs, champs obligatoires/facultatifs sur les formulaires en ligne, consentement…

☐ Accompagner, dans la mesure du possible, les membres du groupement de commandes dans la mise en place de dispositifs leur permettant de s'acquitter de l' obligation de donner suite aux demandes d'exercice des droits des personnes concernées: droit d'accès, de rectification, d'effacement et d'opposition, droit à la limitation du traitement, droit de ne pas faire l'objet à son insu d'une décision individuelle automatisée (incluant le profilage).

☐ Notifier des violations de données à caractère personnel dès constat ou au maximum sous 24 heures après en avoir pris connaissance, par courrier électronique aux adresses qui lui seront communiquées lors de la réunion de lancement de projet. Cette notification est accompagnée de toute documentation utile afin de permettre au membre du groupement de commandes, si nécessaire, de notifier cette violation à l'autorité de contrôle compétente.

☐ Mettre en oeuvre les mesures de sécurité techniques et organisationnelles garantissant un niveau de sécurité adapté au risque, y compris entre autres :

- Les moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constante des systèmes et des services de traitement (gestion des habilitations et droits d'accès…)

- Les moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique et technique

- Les moyens de purge automatique et sélective des données d'une base active à l'issue d'une certaine durée

- Une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement (traçabilité…)

- L'accompagnement (assistance/conseils) des membres du groupement sur les mises en conformité techniques appropriées lors de l'exécution des prestations.

☐ Restituer, épurer les données au terme des prestations de l'accord-cadre et des éventuels contrats d'abonnement Saas et supports ultérieurs. A la demande des membres du groupement il s'engage à restituer toutes les données à caractère personnel aux membres du groupement. Le renvoi doit s'accompagner de la destruction de toutes les copies existantes dans les systèmes d'information du titulaire et de ses éventuels sous-traitants. Une justification écrite lui sera demandée de cette destruction.

☐ Tenir un registre des catégories d'activités du traitement : Le titulaire déclare tenir par écrit un registre de toutes les catégories d'activités du traitement effectuées pour le compte de chaque membre du groupement de commandes portant les informations suivantes :

- le nom et les coordonnées du responsable du traitement pour le compte duquel il agit, des éventuels sous-traitants et, le cas échéant, du délégué à la protection des données de l'entreprise;
- les catégories de traitements effectués pour le compte de chaque membre du groupement de commandes ;
- dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles.

☐ Mettre à disposition la documentation nécessaire pour démontrer le respect de toutes ses obligations et pour permettre la réalisation d'audits par les représentants des membres du groupement de commandes ou un autre auditeur mandaté par eux, et contribuer à ces audits.

Chaque partie à l'accord-cadre est tenue au respect des règles relatives à la protection des données nominatives, auxquelles elle a accès pour les besoins de l'exécution de l'accord-cadre.

En cas d'évolution de la législation sur la protection des données à caractère personnel en cours d'exécution de l'accord-cadre, les modifications éventuelles, demandées par les membres du groupement de commandes afin de se conformer aux règles nouvelles, donneront lieu à la signature d'un avenant à l'accord-cadre.