**ANNEXE RGPD AU CAHIER DES CLAUSES ADMINISTRATIVES ET TECHNIQUES PARTICULIERES (CCATP) MARCHE N°**

Intitulé de la consultation :Fourniture, gestion et livraison de titres restaurant pour les agents de l’EPD LE CHARMEYRAN

REGLES APPLICABLES AU TRAITEMENT DES DONNEES A CARACTERE PERSONNEL

1. Obligations fixées par les lois et règlements applicables en matière de protection des données personnelles
   1. Généralités

Le Titulaire est informé de ce qu'il doit se conformer aux lois et règlements applicables en matière de protection des données personnelles, notamment au 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 et à la libre circulation de ces données » (Règlement Général sur la Protection des Données, noté ci-après « RGPD »), lequel est applicable de plein droit depuis le 25 mai 2018 et notamment son article 28.

Constitue une donnée à caractère personnel (article 4.1 du RGPD) « toute information se rapportant à une personne physique identifiée ou identifiable (dénommée dans le RGPD « personne concernée ») ; est réputée être une « personne physique identifiable » une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale ».

Un traitement est, quant à lui, « toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction » (article 4.2 du RGPD).

Le Titulaire est ainsi positionné en tant que « sous-traitant » de l’EPD LE CHARMEYRAN au sens du RGPD. A ce titre, il est donc autorisé à traiter, pour le compte de l’EPD LE CHARMEYRAN (le « responsable du traitement), des données à caractère personnel nécessaires pour principalement le ou les service(s) suivant(s) :

* + L’hébergement de la solution,
  + Son intégration au sein de la collectivité,
  + Maintenir une assistance,
  + Faire intervenir un autre sous-traitant pour escalader des anomalies.

Dans ce cadre, le Titulaire devra garantir qu’il remplit les obligations du RGPD et notamment son article 28. Ainsi, il s’engage à :

* + Traiter les données uniquement pour la ou les seule(s) finalité(s) qui fait/font l’objet de la sous-traitance,
  + Traiter les données sur instructions l’EPD LE CHARMEYRAN par demande d’assistance écrite ou par téléphone consignée dans notre outil de gestion ou par une prestation contractualisée,
  + Informer l’EPD LE CHARMEYRAN en cas d’interventions ou escalade d’une de ses demandes pour correction par un autre sous-traitant,
  + Veiller à ce que les personnes autorisées à traiter les données à caractère personnel en vertu du présent marché en respectent la confidentialité et ont reçu la formation nécessaire en matière de protection des données à caractère personnel,
  + Gérer des habilitations personnelles par utilisateur et administrateur,
  + Journaliser conformément à la réglementation en vigueur,
  + Mener une politique d’archivage au sein de la solution proposée.

Le Titulaire est réputé avoir produit dans son offre l’ensemble des mesures prises et planifiées pour la conformité au RGPD notamment sur les aspects ci-dessus.

* 1. Durée de conservation des données

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.

La loi dispose que ces données soient « conservées sous une forme permettant l’identification des personnes concernées pendant une durée qui n’excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées » (article 6 al.5 de la loi n°78-17 du 6 janvier 1978 relative à l’informatique, aux fichiers et aux libertés modifiée et article 5.1 e) du RGPD).

Les systèmes doivent donc prévoir la suppression, l’archivage, ou encore l’anonymisation de ces données, lorsque leur durée de conservation est atteinte.

* 1. Protection des données à caractère personnel

Chaque partie au marché est tenue au respect des règles relatives à la protection des données à caractère personnel, auxquelles elle a accès pour les besoins de l'exécution du marché.

En cas d'évolution de la législation sur la protection des données à caractère personnel en cours d'exécution du marché, les modifications éventuelles demandées par l’acheteur, afin de se conformer aux règles nouvelles, donnent lieu à la signature d'une modification du marché par les parties.

* 1. Demande d’accès aux données à caractère personnel

D’une manière générale, en conformité aux articles 28 et 29 du RGPD, le Titulaire s’engage à ne traiter les données du responsable de traitement que sur instruction de ce dernier et s’interdit donc toute utilisation de données à caractère personnel sans son consentement préalable.

En cas d’accord de l’acheteur pour un transfert de données à caractère personnel, il sera demandé au Titulaire, après usage des données transférées, de détruire toutes les informations (bases de données, fichiers…) transmises par l’acheteur ainsi que tous les fichiers créés, après validation du service fait.

1. Exigence de sécurité des données personnelles
   1. Localisation des données (uniquement si hébergement externe)

Les lieux d’hébergement des données doivent satisfaire aux exigences de sécurité de la Collectivité et aux dispositions du RGPD.

Le Titulaire doit communiquer la liste de tous les lieux de stockage de données (site d’hébergement principal, sites secondaires, sites de réplication, sites de secours...). Il veillera également à ce que la séparation logique des données par rapport à celles d'autres clients soit garantie.

Si la faisabilité technique de cette exigence peut s’avérer délicate dans le cadre d’architectures distribuées, il peut être demandé au prestataire d’être en mesure de localiser, à postériori, et non en permanence, le lieu de stockage des données, en particulier suite à un incident.

Le Titulaire est réputé avoir précisé dans son offre la localisation des données selon la classification suivante : France, pays membre(s) de l’Union Européenne (en précisant le(s)quel(s)) ou Hors Union Européenne (en précisant le(s)quel(s)).

* 1. Réponse à une demande de droit d’accès conformément aux articles 12 et 15 du RGPD (uniquement si hébergement externe)

Le Titulaire s'engage à fournir au responsable de traitement, au maximum sous 15 jours calendaires à compter de la réception de sa demande, les données personnelles relatives à une personne concernée ayant présenté une demande de droit d'accès auprès du responsable de traitement.

Le non-respect de ce délai de transmission des données expose le Titulaire à des pénalités dont les modalités sont indiquées dans le Cahier des Clauses Administratives Particulières (CCAP).

* 1. Notification des violations de données personnelles conformément à l’article 33-2 du RGPD (uniquement si hébergement externe)

Si le Titulaire considère qu’une instruction émise par l’EPD LE CHARMEYRAN constitue une violation du RGPD ou de toute autre disposition du droit de l’Union ou du droit des Etats membres relative à la protection des données, il en informe immédiatement l’EPD LE CHARMEYRAN.

Le Titulaire devra notifier à la collectivité toute violation de données au maximum sous 24h après en avoir pris connaissance, conformément à l’article 33-2 du RGPD. Il devra également lui fournir la planification des mesures techniques correctives de mise en sécurité qui seront mises en œuvre.

Une violation de données est par définition « toute violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données ».

* 1. Mesures de vérification et audits de conformité conformément à l’article 28-3 h du RGPD (uniquement si hébergement externe)

Dans ce cadre et conformément à l’article 28-3 h) du RGPD, le Titulaire, le cas échéant le(s) sous-traitant(s), « met(tent) à disposition toutes les informations nécessaires pour démontrer le respect des obligations prévues à l’article 28 ».

* 1. Sanctions encourues en cas de non-respect

Il est aussi rappelé au Titulaire que la violation des dispositions du RGPD l’expose :

- aux sanctions pénales prévues aux articles 226-16 à 226-24 du Code pénal (conformément au chapitre VIII de la loi n°78-17 du 6 janvier 1978 relative à l’informatique, aux fichiers et aux libertés modifiée) ;

- aux sanctions prévues à l’article 83 du RGPD (allant jusqu’à 20 millions d’euros d’amende ou jusqu’à 4% du chiffre d’affaires annuel mondial total de l’exercice précédent)

* 1. Obligation de confidentialité

Chacune des parties s'engage à respecter le principe général du secret des affaires et à ne pas divulguer à des tiers (sauf autorisation expresse), à titre onéreux ou gratuit, et sous quelque forme que ce soit, les informations reçues de l'autre partie ou de tiers intervenant (AMO) ou obtenues à l'occasion de l'exécution du présent marché, et qui concerneraient, sans que cette liste soit limitative, ses activités, sa politique, sa stratégie, ses plans de gestion ou d'organisation, ses applications informatiques, sauf autorisation écrite et préalable de l'autre partie désignant le (ou les) bénéficiaire(s) de l'information ainsi que son contenu.

Par ailleurs, chacune des parties s'engage à ne pas divulguer à des tiers non expressément autorisés les concepts, savoir-faire et techniques révélés à l'occasion de l'exécution du marché. Cet engagement ne saurait toutefois empêcher les parties d'utiliser la partie résiduelle de ces concepts, savoir-faire et techniques dans quelque but que ce soit. L'expression « partie résiduelle » désigne les éléments restés présents à l'esprit des personnes ayant eu accès aux concepts, savoir-faire ou techniques.

Pour toute communication d'Informations confidentielles faite par l'une des parties à l'autre :

* + Lorsqu’elle prendra la forme d'un document écrit, le document devra être revêtu de façon visible d'un avertissement de confidentialité,
  + Lorsqu’elle sera faite sous forme orale, elle devra être reprise dans un document écrit devant être revêtu de façon visible d’un avertissement de confidentialité dans lequel sera spécifiée la nature des informations annoncées comme confidentielles lors de leur communication.

Toutefois, les programmes, données et fichiers remis par l’acheteur au Titulaire ou générés au cours des traitements exécutés par le Titulaire ainsi que leur mise à jour constitueront des informations confidentielles, qu'ils soient ou non revêtus d'un avertissement de confidentialité. Il en est de même pour les informations visées au premier paragraphe du présent article.

Le Titulaire garantit que l'ensemble des membres de son personnel, ses éventuels fournisseurs et/ou sous-traitants et/ou cotraitants sont soumis à un engagement de confidentialité compatible avec le présent article.

La partie réceptrice ne pourra transmettre les informations confidentielles de l'autre partie qu'aux seuls membres de son personnel ou de ses cotraitants, fournisseurs, sous-traitants qui ont besoin d'en avoir connaissance pour l'exécution de leurs obligations contractuelles.

Chacune des parties, afin de respecter ses engagements vis-à-vis de l'autre partie, s'engage à prendre toutes précautions nécessaires et, si besoin, à faire signer des engagements de confidentialité afin que les membres de son personnel, appelés à avoir connaissance d'Informations confidentielles de l'autre partie ou des autres titulaires échangées conformément aux dispositions des présentes, les gardes confidentielles.

Les dispositions visées aux deux paragraphes ci-dessus s'appliquent également aux éventuels fournisseurs, cotraitants et sous-traitants du Titulaire.

En conséquence, les parties s'engagent et se portent fort pour leur personnel, à respecter ces informations confidentielles et à ne pas les révéler ou laisser à disposition de tiers, sans avoir obtenu l'accord préalable et écrit de l'autre partie sauf sur injonction d'un Tribunal ou d'une administration.

Toutefois, chaque partie pourra communiquer, sous la plus stricte confidentialité, le présent marché et les documents y afférents :

* + Pour le Titulaire : à son courtier d'assurances, à ses commissaires aux comptes, aux organismes fiscaux et sociaux en cas de contrôle et à sa maison mère, ses conseils,
  + Pour l’acheteur : aux organismes de contrôle concernés, à des experts.

L'obligation de confidentialité ne s'applique pas aux informations connues de la partie réceptrice préalablement à leur communication (à charge pour la partie invoquant cette connaissance préalable d'en apporter la preuve), à celles obtenues de tiers par des moyens légitimes et sans l'obligation de secret, à celles développées indépendamment ou encore à celles rendues publiques par la partie qui les a communiquées.

Les parties s'engagent à respecter les obligations résultant du présent article pendant toute la durée du présent marché ainsi que pendant une durée de cinq ans suivant leur expiration.

Par ailleurs, les parties conviennent que la constatation par l’acheteur du non-respect par le Titulaire des dispositions du présent article présume la faute de ce dernier et permet à l’acheteur d’avoir la faculté de mettre en œuvre les dispositions du CCAP relatif aux modalités de résiliation du marché.