CONDITIONS D'APPLICATION DU REGLEMENT EUROPEEN DE PROTECTION DES DONNEES PERSONNELLES (RGPD)

A EDF

(Extrait des CGA/CPA)

GESTION DES DONNEES A CARACTERE PERSONNEL

Chacune des Parties s'engage au respect des obligations légales et réglementaires lui incombant au titre de « la législation relative à la protection des données à caractère personnel », en particulier la loi « Informatique et libertés » n°78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés et le règlement (UE) n° 2016/679 du 27 avril 2016 du Parlement européen et du Conseil 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 (ci-après le « RGPD»)..

Chacune des Parties veille à assurer la sécurité et la confidentialité des données conformément à ce qu'elles auront définies en annexe du CCTP et/ou dans le Plan d'Assurance Qualité et Sécurité. (ci-après « PAQS »).

Nota : Le Titulaire est qualifié de « Sous-Traitant » au sens de la législation européenne relative à la protection des données à caractère personnel, lorsqu'il effectue, pour le compte et sur instructions documentées de l'Entreprise (agissant en qualité de Responsable de Traitement), des Traitements de Données à Caractère Personnel au titre du Marché (par exemple, consultation de fichiers contenant des données à caractère personnel, opérations de maintenance permettant d'accéder d'une quelconque manière à des données à caractère personnel détenues par l'Entreprise, hébergement de données …). Par la suite, dans les présentes CPA, le terme « sous-traitant ultérieur » est employé uniquement pour désigner la personne physique ou morale à qui le Titulaire a confié l'exécution d'une partie du marché par un contrat d'entreprise. Si le Titulaire détermine les finalités et moyens du Traitement, il sera considéré alors comme le Responsable dudit Traitement.

DEFINITIONS :

Donnée(s) à Caractère Personnel : est toute information se rapportant à une personne physique identifiée ou identifiable au sens de la législation relative à la Protection des Données Personnelles (ci-après dénommée «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.

Pays Tiers : pays hors U.E. reconnus par la Commission européenne comme n'assurant pas un niveau de protection suffisant des Données à Caractère Personnel au sens de la Législation de Protection des Données à Caractère Personnel.
Responsable de Traitement : désigne toute personne physique ou morale, l'autorité publique, le service ou un autre organisme, qui seul ou conjointement avec d'autres, détermine les finalités et moyens du ou des Traitements.
Traitement : désigne 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.

1. FORMALITES PREALABLES AU DEMARRAGE DES PRESTATIONS

Chacune des Parties, lorsqu'elle est qualifiée de Responsable du Traitement, fait son affaire des formalités préalables lui incombant au titre de la législation relative à la protection des Données à Caractère Personnel.

Toutefois, le Titulaire assistera l'Entreprise dans la réalisation de ses formalités préalables relatives au Traitement de données qui lui est confié :

- Préalablement au Traitement des Données à Caractère Personnel, une analyse d'impact relative à la protection des données sera menée par l'Entreprise. Le Titulaire s'engage à fournir à l'Entreprise toute information nécessaire pour la réalisation de cette analyse, à apporter toute l'assistance nécessaire et à l'alerter sur les risques engendrés par le traitement des données ou par la finalité du Traitement. Cette analyse sera annexée au PAQS.
- Le Titulaire apportera son aide à l'Entreprise pour toute consultation préalable de la CNIL ou de toute autre autorité de contrôle, lorsque celle-ci est requise.

2. OBLIGATIONS DU TITULAIRE

Le Titulaire s'engage à prendre toutes les mesures nécessaires au respect par lui-même, par son personnel et par ses éventuels sous-traitants ultérieurs autorisés dans l'exécution du Marché, des obligations énoncées au Marché et notamment à :

i. traiter ou consulter les données uniquement pour la (ou les) seule(s) finalité(s) objet du présent Marché ; en particulier, le Titulaire s'interdit de consulter ou de traiter les données autres que celles nécessaires à l'exécution du Marché, même si l'accès à ces données est techniquement possible ;

ii. traiter les données uniquement et conformément aux instructions documentées de l'Entreprise, figurant au présent Marché, ainsi qu'aux modifications apportées à ces instructions en cours d'exécution. Si le Titulaire considère qu'une instruction constitue une violation de la législation relative à la protection des Données à Caractère Personnel, il en informe dès que possible l'Entreprise et à la condition que le Titulaire explique la teneur de la violation, il se réserve le droit de ne pas exécuter cette instruction tant que sa légalité n'est pas assurée. En outre, si le Titulaire est tenu de procéder à un transfert de données vers un Pays Tiers ou une organisation internationale, en vertu de dispositions législatives ou

réglementaires auxquelles il est soumis, il doit informer l'Entreprise de cette obligation juridique ;

iii. mettre en œuvre les mesures techniques et organisationnelles appropriées afin d'assurer la sécurité des données, telles que décrites dans les instructions documentées et communiquées par l'Entreprise dans le cadre du présent Marché et/ou dans le PAQS.

Les mesures techniques et organisationnelles garantissant un niveau de sécurité adapté concerneront, à titre d'exemple :

- la pseudonymisation et le chiffrement des Données à Caractère Personnel,

- la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement,

- toute mesure permettant d'empêcher toute utilisation hors des finalités retenues notamment détournée, malveillante ou frauduleuse des données et des fichiers objet du traitement,

- des moyens permettant de rétablir la disponibilité des Données à Caractère Personnel et à l'accès à celles-ci dans des délais appropriés en cas d'incident physique et technique,

- une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du Traitement.

Ces mesures techniques et organisationnelles sont détaillées dans le CCTP et complétées dans le Plan Assurance Qualité et Sécurité propre à ce marché.

iv. assurer la confidentialité des Données à Caractère Personnel traitées dans le cadre du présent Marché ; et à cet égard, ne pas divulguer à des tiers non préalablement autorisés, sous quelque forme que ce soit, tout ou partie des données exploitées ;

v. veiller à ce que les personnes autorisées à traiter les Données à Caractère Personnel en vertu du présent Marché s'engagent à :

- respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité et,

- reçoivent la formation nécessaire en matière de protection des Données à Caractère Personnel ;

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

vii. ne pas, sans autorisation de l'Entreprise, insérer dans les traitements des données étrangères à celles confiées par l'Entreprise, ni réaliser de copie ou de stockage des données autres que ceux autorisés au titre du Marché, ni louer ou vendre des données confiées par l'Entreprise ;

viii. restituer au terme du Marché pour quelque cause que ce soit, les données à l'Entreprise sur un support fidèle et tangible convenu entre les Parties. Le renvoi doit s'accompagner de la destruction de toutes les copies existantes dans les systèmes d'information du Titulaire et le Titulaire doit justifier par écrit de leur destruction ;

ix. mettre à la disposition de l'Entreprise toutes les informations pour démontrer le respect des obligations prévues pour le Traitement des Données à Caractère Personnel et pour permettre la réalisation d'audits, y compris des inspections, par l'Entreprise ou un autre auditeur qu'il a mandaté, et contribuer à ces audits ;

x. notifier par courriel à l'Entreprise toute violation de Données à Caractère Personnel au plus tôt et dans un délai maximum de 72 heures après en avoir pris connaissance et par écrit à l'interlocuteur technique désigné au présent Marché. Cette notification est accompagnée de toute documentation utile permettant à l'Entreprise, si nécessaire, de notifier cette violation à l'autorité de contrôle compétente. La notification à l'Entreprise contient au moins :

- la description de la nature de la violation de Données à Caractère Personnel y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de Données à Caractère Personnel concernés ;

- le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact chez le Titulaire auprès duquel des informations supplémentaires peuvent être obtenues ;

- dans la mesure des informations en sa connaissance dans ce délai de 72 heures, la description des conséquences probables de la violation de Données à Caractère Personnel ;

- dans la mesure des informations en sa connaissance dans ce délai de 72 heures, la description des mesures prises ou que le Titulaire propose de prendre pour remédier à la violation de Données à Caractère Personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

S'il n'est pas possible de fournir toutes les informations en même temps, le Titulaire s'engage à notifier à l'Entreprise toute information complémentaire relative à la violation de manière échelonnée, sans autre retard indu, et à collaborer avec l'Entreprise en vue de la résolution de la violation.

En outre, le Titulaire s'engage également à :

- fournir aux personnes concernées par les opérations de traitement, au moment de la collecte des données, l'information relative aux traitements de données qu'il réalise dans la formulation et le format convenu avec l'Entreprise ;

- aider l'Entreprise sur les volets techniques et/ou organisationnels à s'acquitter de son obligation de donner suite aux demandes d'exercice des droits des personnes concernées sur leurs données : 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. Dans l'hypothèse où les demandes des personnes concernées seraient exercées directement auprès du Titulaire, ce dernier peut être amené à y répondre et il en informera alors l'Entreprise ;

- communiquer à l'Entreprise le nom et les coordonnées de son délégué à la protection des données, s'il en a désigné un. A défaut, il communique à l'Entreprise le nom et les coordonnées de son Référent chargé de la protection des Données à Caractère Personnel ;

- tenir par écrit un registre de toutes les catégories d'activités de traitement effectuées pour le compte de l'Entreprise, comprenant toutes les mentions conformes aux exigences de la législation relative à la protection des Données à Caractère Personnel.

3. OBLIGATIONS DE L'ENTREPRISE VIS-A-VIS DU TITULAIRE

En tant que responsable du traitement, l'Entreprise s'engage notamment à :

i. fournir au Titulaire un descriptif du traitement de Données à Caractère Personnel pour l'exécution du présent Marché. Ce descriptif comporte notamment :

a. la nature des opérations réalisées sur les données

b. la (ou les) finalité(s) du Traitement

c. les Données à Caractère Personnel traitées

d. les catégories de personnes concernées.

ii. documenter par écrit toute instruction concernant le traitement des données par le Titulaire;

iii. veiller, au préalable et pendant toute la durée du traitement, au respect des obligations prévues par la législation relative à la protection des Données à Caractère Personnel de la part du Titulaire ;

iv. superviser le traitement, y compris réaliser des audits et des inspections auprès du Titulaire.

L'ensemble de ces éléments ainsi que les instructions destinées à permettre au Titulaire de respecter ses engagements au titre du RGPD seront définis dans l'annexe au CCTP prévue à cet effet et/ou dans le PAQS.

4. TRANSFERTS DES DONNEES A CARACTERE PERSONNEL VERS UN PAYS TIERS

Le Titulaire ne peut transférer des Données à Caractère Personnel que vers les Pays Tiers ou les Organisations Internationales dont la Commission européenne a constaté par voie de décision que le pays tiers ou l'Organisation Internationale en question assure un niveau de protection adéquat. Toutefois, le Titulaire peut transférer des Données à Caractère Personnel vers un Pays Tiers ne bénéficiant pas d'une décision de la Commission constatant que le Pays Tiers en question assure un niveau de protection adéquat et ce, sans autorisation particulière d'une autorité de contrôle depuis le 25 mai 2018, lorsque le Titulaire apporte les garanties appropriées à la protection des Données à Caractère Personnel et notamment, lorsque le Titulaire apporte la preuve du respect de règles d'entreprises contraignantes (« Binding Corporate Rules » ou « BCR ») prévues par la législation sur la protection des Données à Caractère Personnel ou lorsqu'il encadre les transferts par des clauses contractuelles types de la Commission européenne.

Dans tous les cas, le Titulaire ne peut transférer des Données à Caractère Personnel vers un Pays Tiers ou une Organisation Internationale sans l'accord préalable et écrit de l'Entreprise.

5. SOUS-TRAITANTS DU TITULAIRE

Le Titulaire peut faire appel à un sous-traitant pour mener des activités de Traitement de Données à Caractère Personnel spécifiques. Dans ce cas, il informe, préalablement et par écrit, l'Entreprise de tout changement envisagé concernant l'ajout ou le remplacement de tout sous-traitant. Cette information doit indiquer clairement les activités de Traitement sous-traitées, les mesures techniques et organisationnelles prévues, l'identité et les coordonnées du sous-traitant et les dates du contrat de sous-traitance.

Avant la sous-traitance envisagée, le Titulaire doit obtenir l'autorisation écrite, préalable et spécifique de l'Entreprise.

Le respect de la clause « Gestion des Données à Caractère Personnel » constitue une obligation pour laquelle le Titulaire doit veiller à faire figurer des engagements a minima équivalents à ceux énoncés au dit article dans les contrats qu'il conclut avec ses sous-traitants.

Le Titulaire s'engage à ce que le sous-traitant respecte les obligations du présent Marché. Il appartient au Titulaire de s'assurer que tout sous-traitant présente les mêmes garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles définies au présent Marché. Si le sous-traitant ne remplit pas ses obligations en matière de protection des Données à Caractère Personnel, le Titulaire demeure pleinement responsable devant l'Entreprise de l'exécution par son sous-traitant de ses obligations.