Marché d'étude et assistance à maîtrise d'ouvrage dans le cadre d'un projet de densification du site de la direction départementale des territoires (DDT) de la Haute-Saône

CCAP – Annexe 1
Traitement des données à caractère personnel

Préambule :

A) lexique du RGPD

Donnée à caractère personnel (Article 4.1 du RGPD) : toute information identifiant directement ou indirectement une personne physique (ex : nom, no d'immatriculation, no de téléphone, photographie, date de naissance, commune de résidence, empreinte digitale…) ; ou encore « *toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée « personne concernée »*).

Une *« personne physique identifiable* » est 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 ».

« Constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres », article 2 de la Loi 78-17 du 6 janvier 1978 modifiée.

Données sensibles (article 9 du RGPD) : données susceptibles de donner lieu à discrimination (origine raciale ou ethnique, opinions politiques, convictions religieuses ou philosophiques, orientation sexuelle…) ou propres à une personne (données génétiques, biométriques, de santé).

Traitement (article 4.2 du RGPD) : toute opération (automatisée ou non) sur des données à caractère personnel (collecte, enregistrement, organisation, stockage, conservation, adaptation, modification, extraction, utilisation, communication par transmission, rapprochement ou interconnexion…).

Responsable du traitement (« data controller », article 4.7 du RGPD) : personne, service ou organisme (public ou privé : entreprises, administrations, associations…) qui détermine les finalités et les moyens du traitement (ACHETEUR dans les marchés publics)

Sous-traitant (« data processor », article 4.8 du RGPD) : personne, service ou organisme (public ou privé) qui traite des données personnelles pour le compte du responsable de traitement (TITULAIRE dans les marchés publics)

Finalité d'un traitement (article 5 du RGPD) : par exemple, objectif principal d'une application informatique de données personnelles (gestion des recrutements, gestion des clients, enquête de satisfaction, surveillance des locaux, etc.)

B) précisions terminologiques :

☑Le présent marché comporte des traitements de données à caractère personnel.

Pour l'application de ce paragraphe, le responsable de traitement, au sens du RGPD, est le pouvoir adjudicateur et le « sous-traitant » est le titulaire du marché.

La présente clause a pour objet de définir les conditions dans lesquelles le titulaire du marché s'engage à effectuer pour, le compte du pouvoir adjudicateur, les opérations de traitement de données à caractère personnel définies ci-après.

Dans le cadre du présent marché, les parties s'engagent à respecter la réglementation en vigueur applicable au traitement de données à caractère personnel et, notamment le règlement (UE) 2016/679 du Parlement européen et du Conseil 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 abrogeant la directive 95/46/CE (ci-après, *«règlement général sur la protection des données »* RGPD) et la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

1-Description du traitement de données à caractères personnel :

Le titulaire est autorisé à traiter, pour le compte du pouvoir adjudicateur et pour la durée du présent marché, les données à caractère personnel nécessaires pour fournir les prestations faisant l'objet du présent marché

La nature des opérations réalisées sur les données est de contacter les services bénéficiaires du présent accord-cadre en prenant contact avec ses correspondants administratifs en charge du suivi administratif et financier du marché.

Les finalités du traitement sont d'assurer l'exécution des prestations prévues à l'accord-cadre.

Les données à caractère personnel traitées sont le nom, le prénom, l'adresse mail et le numéro de téléphone des correspondants désignés par les services bénéficiaires pour chacun de leur site.

Les catégories de personnes concernées sont des agents des services de l'État et des opérateurs de l'Etat en Bourgogne-Franche-Comté.

2-Obligations du titulaire vis-à-vis du pouvoir adjudicateur (article 28.3 du RGPD) :

Le titulaire du marché public s'engage, notamment, à :

- traiter les données uniquement pour les seules finalités faisant l'objet du présent marché ;
- traiter les données conformément aux instructions documentées par la pouvoir adjudicateur et figurant en annexe à l'acte d'engagement du présent marché ;
- si le titulaire considère qu'une instruction constitue une violation du règlement général 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, il en informe immédiatement le pouvoir adjudicateur ;
- si le titulaire est tenu de procéder à un transfert de données vers un pays tiers (hors de l'Union européenne) ou à une organisation internationale, en vertu du droit de l'Union ou du droit de l'État membre auquel il est soumis, il doit informer le pouvoir adjudicateur de cette obligation juridique avant le traitement, sauf si le droit concerné interdit une telle information ;
- garantir la confidentialité des données à caractère personnel traitées dans le cadre du présent marché ;
- 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 ; que ces personnes reçoivent la formation nécessaire en matière de protection des données à caractère personnel ;
- 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.

3-Sous-traitance des activités de traitement (articles 28.2 et 28.4 du RGPD) :

Lorsque le titulaire fait appel à un sous-traitant pour mener des activités de traitement spécifiques, il informe préalablement et, par écrit, le pouvoir adjudicateur de tout changement envisagé concernant l'ajout ou le remplacement d'autres sous-traitants. Cette information doit indiquer clairement les activités de traitement sous-traitées, l'identité et les coordonnées du sous-traitant et les dates du marché.

Afin d'obtenir l'acceptation et l'agrément du pouvoir adjudicateur, le titulaire doit présenter son sous-traitant par le biais de l'acte spécial de sous-traitance, dont les formalités sont comprises dans le formulaire DC4 ou équivalent (téléchargeable sur http://www.economie.gouv.fr/daj/formulaires-declaration-candidat).

Le sous-traitant est tenu de respecter les obligations du présent marché pour le compte et selon les instructions du pouvoir adjudicateur. Il appartient au titulaire de s'assurer que le sous-traitant 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 général sur la protection des données. Si le sous-traitant ne remplit pas ses obligations en matière de protection des données, le titulaire demeure pleinement responsable devant le pouvoir adjudicateur de l'exécution par le sous-traitant de ses obligations.

4-Droit d'information et exercice des personnes concernées par le traitement (articles 13 à 15 du RGPD) :

Pour l'exécution du présent marché, le pouvoir adjudicateur a choisi de retenir l'option suivante : fournir l'information aux personnes concernées par les opérations de traitement au moment de la collecte des données.

Le titulaire aide le pouvoir adjudicateur à s'acquitter de son 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 à la portabilité des données, droit de ne pas faire l'objet d'une décision individuelle automatisée (y compris le profilage).

5-Notification des violations de données à caractère personnel (article 33 du RGPD) :

Le titulaire notifie au pouvoir adjudicateur toute violation de données à caractère personnel dans un délai d'**un jour ouvré** après en avoir pris connaissance et par le moyen suivant : messagerie électronique à l'adresse suivante : sgar-pfra@bfc.gouv.fr

Cette notification est accompagnée de toute documentation utile afin de permettre au pouvoir adjudicateur, si nécessaire, de notifier cette violation à l'autorité de contrôle compétente (en l'occurrence, à la Commission nationale de l'informatique et des libertés, CNIL) **si possible 72 heures au plus tard** après en avoir pris connaissance.

Après accord écrit du pouvoir adjudicateur, le titulaire notifie à l'autorité de contrôle compétente, au nom et pour le compte du pouvoir adjudicateur, les violations de données à caractère personnel dans un délai maximum de **72 heures** à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques.

La notification 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 auprès duquel des informations supplémentaires peuvent être obtenues ;
- la description des conséquences probables de la violation de données à caractère personnel ;
- la description des mesures prises ou que le pouvoir adjudicateur 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.

Si, et dans la mesure où il n'est pas possible de fournir toutes ces informations en même temps, les informations peuvent être communiquées de manière échelonnée sans retard indu.

Après accord écrit du pouvoir adjudicateur, le titulaire communique, au nom et pour le compte du pouvoir adjudicateur, la violation de données à caractère personnel à la personne concernée dans les meilleurs délais, lorsque cette violation est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique.

La communication à la personne concernée décrit, en des termes clairs et simples, la nature de la violation de données à caractère personnel et 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 auprès duquel des informations supplémentaires peuvent être obtenues ;
- la description des conséquences probables de la violation de données à caractère personnel ;
- la description des mesures prises ou que la pouvoir adjudicateur 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.

6-Aide du titulaire dans le cadre du respect par le pouvoir adjudicateur de ses obligations :

Le titulaire aide le pouvoir adjudicateur à :

- la réalisation d'analyses d'impact relative à la protection des données ;
- à la réalisation de la consultation préalable de l'autorité de contrôle.

7-Mesures de sécurité

Le titulaire met en œuvre les mesures de sécurité suivantes :

- la pseudonymisation et le chiffrement des données à caractère personnel ;
- les moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;
- 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 ou 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.

Le titulaire met en œuvre les mesures de sécurité prévues par les lois et règlements en vigueur dans le domaine de la tierce maintenance applicative.

8-Sort des données (article 28.3.g du RGPD)

Au terme de l'exécution du présent marché, et selon le choix du pouvoir adjudicateur, le titulaire doit détruire toutes les données à caractère personnel.

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

sous-traitant. Une fois détruites, le sous-traitant doit justifier par écrit de la destruction.

9-Délégué à la protection des données (articles 37 à 39 du RGPD) :

Le titulaire communique au pouvoir adjudicateur, dès la notification du marché, le nom et les coordonnées de son délégué à la protection des données, s'il en a désigné un conformément à l'article 37 du règlement européen sur la protection des données, ou, à défaut, l'identité et les coordonnées d'un point de contact dédié à ces questions.

10-Registre des activités de traitement (article 30 du RGPD) :

Le titulaire tient, par écrit, un registre de toutes les activités de traitement effectuées pour le compte du pouvoir adjudicateur, ce registre comprenant :

- le nom et les coordonnées du pouvoir adjudicateur pour le compte duquel il 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 pouvoir adjudicateur ;
- le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale et, dans le cas des transferts visés à l'article 49, paragraphe 1, deuxième alinéa du règlement général sur la protection des données, les documents attestant de l'existence de garanties appropriées ;
- dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles, notamment, selon les besoins :
- la pseudonymisation et le chiffrement des données à caractère personnel ;
- des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;
- des 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 ou 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.

11-Documentation (article 28.3.h du RGPD)

Le titulaire met à la disposition du pouvoir adjudicateur **la documentation nécessaire pour démontrer le respect de toutes ses obligations** et pour permettre, le cas échéant, la réalisation d'audits, y compris des inspections, par le pouvoir adjudicateur ou un auditeur mandaté par lui, et contribuer à ces audits.

12-Obligations du pouvoir adjudicateur vis-à-vis du titulaire

Le pouvoir adjudicateur s'engage à :

- fournir au titulaire les données visées dans la clause relative à la *«Description du traitement de données à caractère personnel»*
- documenter par écrit toute instruction concernant le traitement des données par le titulaire ;
- veiller, au préalable et pendant toute la durée du traitement, au respect des obligations prévues par le RGPD et par la loi Informatique et Libertés de la part du titulaire ;
- superviser le traitement, y compris réaliser les audits et les inspections auprès du titulaire.