ANNEXE CONTRACTUELLE
PORTANT DEFINITION ET CONDITIONS DE REALISATION DES OPERATIONS DE TRAITEMENT DE DONNEES A CARACTERE PERSONNEL POUR LE COMPTE DE L'AUTORITE CONTRACTANTE

ANNEXE A INSERER SOUS FORME D'ANNEXE DANS LES CONTRATS DONT L'OBJET PORTE SUR LE TRAITEMENT DE DCP

La présente annexe au contrat a pour objet de définir les conditions dans lesquelles le titulaire du contrat s'engage à effectuer pour le compte de l'autorité contractante les opérations de traitement de données à caractère personnel définies ci-après.

1. Description du traitement de données à caractères personnel

Le titulaire est autorisé à traiter pour le compte de l'autorité contractante, pour la durée du présent contrat, les données à caractère personnel nécessaires à la fourniture de la ou des prestation(s) suivante(s), qui constituent aussi la ou les finalité(s) du traitement au sens du RGPD : ***Préciser l'objet de la prestation et compléter par les objectifs poursuivis par le traitement considéré***

Les personnes concernées par le traitement de leurs données personnelles sont :

☐ Salariés

☐ Candidats à toute procédure nécessaire à l'exécution du présent contrat

☐ Fournisseurs et prestataires

☐ Visiteurs

☐ Prospects

☐ Partenaires

☐ Autre : ***A compléter***

Les catégories de données à traiter sont : ***Cocher les cases pertinentes***

☐ Etat civil, Identité, Données d'identification

☐ Vie personnelle (habitudes de vie, situation familiale, etc.)

Expertise France - - 40, Boulevard de Port Royal - France
SIRET : 808 734 792

☐ Vie professionnelle (CV, adresse mail professionnelle, formation professionnelle, parcours académique, etc.)

☐ Informations d'ordre économique et financier (revenus, situation financière, situation fiscale, etc.)

☐ Données de connexion (adresse IP, journaux de connexion, etc.)

☐ Données de localisation (déplacements, données GPS, GSM, etc.)

☐ Autre : ***A compléter***

Si des catégories de données hautement personnel sont collectées et font également l'objet d'un traitement : ***Cocher les cases pertinentes***

☐ Données relatives aux données bancaires (RIB, données de CB, transactions financières, …)

☐ Données relatives aux difficultés sociales

Si des catégories de données sensibles sont collectées et font également l'objet d'un traitement : ***Cocher les cases pertinentes***

☐ Données révélant l'origine raciale ou ethnique

☐ Données révélant les opinions politiques

☐ Données révélant les convictions religieuses ou philosophiques

☐ Données révélant l'appartenance syndicale

☐ Données génétiques

☐ Données biométriques

☐ Données concernant la santé

☐ Données concernant la vie ou l'orientation sexuelle

☐ Données relatives aux condamnations pénales et aux infractions ou aux mesures de sûreté connexes

2. Obligations du titulaire vis-à-vis de l'acheteur (article 28.3 du RGPD)

Le titulaire du contrat s'engage notamment à :

- traiter les données uniquement pour la ou les seule(s) finalité(s) qui fait/font l'objet du présent contrat;
- traiter les données conformément aux documents du présent contrat. Si le titulaire considère qu'une instruction est donnée en violation à la règlementation en matière de protection des données 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'autorité contractante.

Si le titulaire est tenu de procéder à un transfert de données vers un pays tiers (situé hors de l'Union européenne) ou à une organisation internationale, en vertu du droit de l'Union ou du droit de l'Etat membre auquel il est soumis, il doit informer l'autorité contractante de cette obligation juridique avant le traitement, sauf si le droit concerné interdit une telle information ;

- garantir la confidentialité et la sécurité des données à caractère personnel traitées dans le cadre du présent contrat ;
- veiller à ce que les personnes autorisées à traiter les données à caractère personnel en vertu du présent contrat :
  - s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité ;
  - 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 (privacy by design et privacy by default).

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 l'autorité contractante 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 de contrat.

Afin d'obtenir l'acceptation et l'agrément d'Expertise France, 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 tout autre document équivalent (téléchargeable sur http://www.economie.gouv.fr/daj/formulaires-declaration-candidat).

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

Le titulaire fournit à l'autorité contractante les moyens d'informer les personnes concernées par les opérations de traitement au moment de la collecte des données.

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

Le titulaire prend attache auprès de son interlocuteur au sein d'Expertise France concernant le présent contrat, afin de lui notifier toute violation de données à caractère personnel, sous un délai de 24 heures après avoir pris connaissance de la violation.

Il informe l'autorité contractante par tout moyen permettant de déterminer de façon certaine la date et l'heure de réception de la notification. Cette notification est accompagnée de toute documentation utile afin de permettre à l'autorité contractante, 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) dans un délai raisonnable après en avoir pris connaissance.

Après accord écrit d'Expertise France, le titulaire notifie à l'autorité de contrôle compétente, au nom et pour le compte d'Expertise France, 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 titulaire propose de prendre en accord avec l'autorité contractante 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 pour le titulaire de fournir toutes ces informations en même temps, les informations peuvent être communiquées de manière échelonnée sans retard indu.

6. Aide du titulaire à l'autorité contractante pour le respect de ses obligations

Le titulaire s'engage à collaborer avec l'autorité contractante à la réalisation de la consultation préalable de l'autorité de contrôle.

7. Mesures de sécurité

Le titulaire met en œuvre les moyens, mesures et procédures qui permettent de :

- rendre anonymes (pseudonyme, chiffrement, …) les données à caractère personnel à traiter ;
- garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;
- 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 ;
- tester, analyser et évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

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

Au terme de l'exécution du présent contrat, et selon le choix d'Expertise France, le titulaire ainsi que son (ses) éventuel(s) sous-traitant(s) doivent chacun :

- renvoyer à Expertise France ou au tiers désigné par celui-ci toutes les données à caractère personnel en leur possession ;
- détruire, effacer, supprimer de manière définitive toutes les données à caractère personnel ou leurs copies, sur quelque support que ce soit, en leur possession et être en capacité d'attester de la destruction auprès d'Expertise France.

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

Le titulaire communique à Expertise France, dès la notification du contrat, 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 aux questions relatives à la protection des données.

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 d'Expertise France comprenant :

1. les noms et coordonnées des personnels ou autre représentant d'Expertise France pour le compte duquel il agit, des éventuels sous-traitants et, le cas échéant, du délégué à la protection des données ;
2. les catégories de traitements effectués pour le compte d'Expertise France ;
3. 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 ;
4. dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles répondant à vos obligations en matière de protection des données à caractère personnel.
5.

11. Documentation (article 28.3.h du RGPD)

Le titulaire met à la disposition de l'autorité contractante 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 l'autorité contractante ou un auditeur mandaté par lui, et contribuer à ces audits.

12. Obligations de l'autorité contractante vis-à-vis du titulaire

Expertise France s'engage à :

- Collaborer avec le titulaire afin de fournir de répondre aux obligations relatives à la « Description du traitement de données à caractères personnel » telle qu'elle figure à l'article 1 de la présente annexe ;