Cahier des Clauses Particulières (CCP)

ANNEXE SUR LE TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL (conformément à l'article 28 du RGPD).

Procédure n° *2020_SU_DA_BAT_CS_SPECTNOELENF*

La présente Annexe a pour objet de décrire les obligations respectives des Parties en matière de données personnelles et fait partie intégrante du CCP.

Préambule : Définitions spécifiques

Données personnelles : désigne toute information se rapportant à une personne physique identifiée ou identifiable ; 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 de téléphone, une adresse email, 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.

Traitement : désigne toute opération ou tout ensemble d'opérations qui est réalisé sur les Données à Caractère Personnel, de manière automatisée ou non, tels que la collecte, l'enregistrement, l'organisation, 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, le verrouillage, l'effacement ou la destruction.

Fichier : désigne tout ensemble structuré de Données personnelles, accessible selon les critères déterminés dans la présente Annexe, que cet ensemble soit centralisé, décentralisé, ou réparti de manière fonctionnelle ou géographique.

Instruction : désigne toute instruction écrite ou par saisie de données, reçue par le titulaire de la part de Sorbonne Université en vertu du contrat et notamment de la présente Annexe, et, le cas échéant, des avenants conclus entre le titulaire et Sorbonne Université et ayant pour objet le traitement de Données personnelles.

Responsable de Traitement : désigne la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement ; dans le cadre du contrat, le Responsable de Traitement est Sorbonne Université.

Sous-traitant : désigne la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des Données personnelles pour le compte du Responsable du Traitement ; dans le cadre du présent contrat, le Sous-traitant est le titulaire. Le terme de sous-traitant est à ne pas confondre avec le terme de sous-traitant au sens de la règlementation de la commande publique.

1. Objet

Les présentes clauses ont pour objet de définir les conditions dans lesquelles le sous-traitant s'engage à effectuer pour le compte du responsable de traitement les opérations de traitement de données à caractère personnel définies ci-après.

2. Durée

Le présent accord entre en vigueur à compter de la notification du présent contrat et jusqu'à sa date de fin.

3. Protection du traitement des Données personnelles

3.1 Réglementation applicable

Dans le cadre du présent contrat, Sorbonne Université et le titulaire s'engagent à respecter leurs obligations, respectivement en leur qualité de Responsable de Traitement et de Sous-traitant telles que prévues :

- à compter du 25 mai 2018, par la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, telle que modifiée le 6 août 2004, le cas échéant mise à jour, ainsi que 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 abrogeant la directive 95/46/CE ;

- en toute hypothèse et, le cas échéant, par les lois locales susceptibles d'affecter et de s'appliquer aux données personnelles en fonction du lieu d'hébergement desdites données personnelles ;

- les textes et décisions émanant d'autorités administratives indépendantes et notamment ceux de la Commission Nationale de l'Informatique et des Libertés (CNIL) ;

- la jurisprudence émanant des tribunaux nationaux et communautaires applicable en matière de données personnelles.

(ci-après la « Réglementation concernant les Données personnelles »).

3.2. Description du traitement faisant l'objet de la sous-traitance :

Dans le cadre du présent contrat, Sorbonne Université confie au titulaire le(s) traitement(s) ayant trait à l'exécution du contrat

3.3. Obligations du sous-traitant vis-à-vis du responsable de traitement et droits des personnes concernées :

Le titulaire s'engage à communiquer à Sorbonne Université, à première demande de ce dernier, des documents relatifs à la politique informatique et libertés en vigueur au sein de sa société pour ce qui relève des informations n'ayant pas vocation à rester confidentielles.

Dans le cas où le titulaire ne disposerait pas d'une politique informatique et libertés, il s'engage à en établir une et à la communiquer à Sorbonne Université au plus tard dans les quinze (15) jours suivant la notification du contrat.

Parallèlement, le titulaire s'engage à mettre en œuvre les programmes de formation et de sensibilisation relatifs à la protection de la vie privée et des données personnelles à destination de ses salariés et sous-traitants au sens de la Loi Informatique et Libertés ayant accès en permanence ou régulièrement aux données personnelles.

Par ailleurs, en application de la Réglementation concernant les données personnelles et dans le cadre du présent contrat, les parties reconnaissent, en ce qui concerne l'ensemble des données personnelles qui sont traitées par le titulaire aux fins de réalisation des prestations, qu'il appartient au ministère seul, de déterminer la manière (incluant les moyens) et les finalités pour lesquelles ces données personnelles seront traitées par le titulaire ; le ministère agit en qualité de Responsable de Traitement ; et le titulaire agit en qualité de Sous-traitant.

Lorsque, dans le cadre du présent contrat, le titulaire est amené à traiter des données personnelles pour le compte du ministère en qualité de sous-traitant, le titulaire s'engage à :

(a) traiter lesdites données personnelles uniquement sur la base d'Instructions du ministère et dans la mesure raisonnablement nécessaire ou appropriée pour l'exécution du présent contrat ;

(b) ne pas divulguer ces données personnelles excepté dans les conditions prévues au présent contrat ou sous réserve du consentement écrit du ministère ;

(c) ne pas vendre, céder, louer ou exploiter commercialement ces données personnelles ;

(d) mettre en place les mesures organisationnelles et techniques indiquées par le ministère à l'article 3.4 ci-après afin d'assurer la protection des données personnelles contre toute destruction accidentelle ou illicite, toute perte fortuite, altération, accès ou divulgation non autorisée ainsi que contre toute forme de traitement illicite ; étant entendu que si ces mesures nécessitent des investissements de la part du titulaire, ces derniers seront pris en charge par Sorbonne Université pour autant que ces investissements ne relèvent pas d'une mise en conformité du titulaire en tant que sous-traitant, à la loi ou règlementation applicable en matière de protection des données personnelles ;

(e) supprimer ou modifier à première demande du ministère, à bref délai et en tout état de cause dans un délai de 15 jours calendaires maximum, les données personnelles identifiées par Sorbonne Université ;

(f) ne pas effectuer d'études statistiques sur les données personnelles ou de traitement sans l'accord préalable du ministère pour chaque type d'étude ;

(g) fournir à première demande un certificat de suppression des données personnelles au ministère ;

(h) notifier immédiatement toute modification ou changement pouvant impacter le traitement des données personnelles ;

(i) respecter la durée de conservation des données personnelles au regard des finalités pour lesquelles elles ont été collectées ou transmises et à supprimer les données personnelles à expiration de la durée de conservation ;

(j) à coopérer avec Sorbonne Université pour envisager les hypothèses dans lesquelles la pseudonymisation et le chiffrement des données personnelles pourrait être appropriée pour l'ensemble des phases ;

(k) à mettre à disposition de Sorbonne Université les informations nécessaires pour démontrer le respect de ses obligations prévues à la présente annexe et pour permettre la réalisation d'audits, y compris des inspections, par le ministère ou un autre auditeur qu'il a mandaté ;

(l) à renvoyer ou à supprimer, dans un délai de 15 jours à compter de la fin du contrat, et selon la préférence de Sorbonne Université, l'intégralité des données personnelles qui lui a été confiée par le ministère, et ce quelle que soit la raison pour laquelle le contrat prend fin. Le cas échéant, le renvoi de toutes les données à caractère personnel s'effectue auprès du responsable de traitement ou auprès du sous-traitant désigné par le responsable de traitement. Le renvoi doit s'accompagner de la destruction de toutes les copies existantes dans les systèmes d'information du titulaire. Une fois détruites, le sous-traitant doit justifier par écrit de la destruction ;

(m) à respecter les droits d'accès, de rectification, d'opposition, de portabilité et de suppression et le droit à la limitation du traitement ainsi que le droit des personnes concernées, de ne pas faire l'objet d'une décision individuelle automatisée y compris le profilage. Dès lors, si une personne dont les données personnelles ont été traitées dans le cadre du présent contrat devait contacter directement le titulaire pour exercer son droit d'accès, de rectification, de portabilité des données, de suppression et/ou d'opposition, ce dernier communiquera à Sorbonne Université dans un délai de trois (3) jours ouvrés, à l'adresse mail qui lui sera communiquée après la notification du contrat, les demandes d'exercice de ces droits qui lui seront parvenues et coopère avec le ministère. Le titulaire ne fera droit à ces demandes que sur instruction écrite de Sorbonne Université à cette fin ;

(n) Le titulaire s'interdit par ailleurs :

- la consultation, le traitement de données personnelles autres que celles concernées par le présent contrat et ce, même si l'accès à ces données est techniquement possible ;

- de prendre copie ou de stocker, quelles qu'en soit la forme et la finalité, tout ou partie des données personnelles qui lui ont été transmises ou qu'il a collectées au cours de l'exécution du contrat en dehors de l'exécution du présent Contrat ;

- de divulguer, sous quelque forme que ce soit, tout ou partie des données personnelles à des tiers, sauf dans le cadre d'instructions formalisées par écrit du ministère .

(o) Délégué à la protection des données (DPO) :

Le titulaire communique à Sorbonne Université, au plus tard au début de la phase 3 « acquisition », le nom et les coordonnées de son DPO, s'il en a désigné un conformément à l'article 37 du RGPD.

3.4. Sécurité des données personnelles

Le titulaire s'engage à assurer la sécurité et la confidentialité des données personnelles qui lui sont communiquées et auxquelles il pourrait avoir accès sur son environnement (Poste de travail par exemple). Les dispositions du présent article 3.4 visent expressément les mesures associées à un accès aux données personnelles sur le ou les systèmes d'information du titulaire.

A ce titre, le titulaire s'engage à mettre en place des mesures de sécurité organisationnelles ainsi que des mesures de sécurité techniques appropriées pour préserver la sécurité et l'intégrité des données personnelles et les protéger contre toute déformation, altération, destruction fortuite ou illicite, endommagement, perte, divulgation ou accès à des tiers non autorisés, telles que décrites dans les sous-paragraphes (a) et (b) ci-dessous.

Le titulaire s'engage à maintenir ces mesures et moyens pour toute la durée du contrat et à défaut, à en informer immédiatement Sorbonne Université.

En tout état de cause, le titulaire s'engage, en cas de changement des moyens visant à assurer la sécurité, l'intégrité et la confidentialité des données personnelles, à les remplacer par des moyens équivalents ou d'une performance supérieure.

(a) Mesures de sécurité organisationnelles

Le titulaire s'engage à mettre en place a minima les mesures de sécurité organisationnelles suivantes :

- présence d'une politique d'habilitations individuelles et de sécurité appropriées pour restreindre l'accès aux données personnelles aux seules personnes qui ont à en connaitre ;

- mise en place d'un engagement de confidentialité visant à ce que les personnes autorisées à traiter les données personnelles soient soumises à une obligation de confidentialité étant entendu que cette obligation peut être prise par le biais du contrat de travail de la personne concernée;

- élaboration de mesures restrictives d'accès aux données personnelles permettant de s'assurer que les personnes habilitées à utiliser le système de traitement de données personnelles ne puissent accéder qu'aux Données personnelles auxquelles elles sont habilitées à accéder conformément à leurs droits d'accès et que, dans le cadre du traitement et de l'utilisation après stockage, les données personnelles ne puissent être lues, copiées, modifiées ou supprimées sans autorisation ;

- mise en place de mesures pour empêcher le transfert des données personnelles à toute personne/entité non autorisée ;

- mise en place de campagnes de sensibilisation des utilisateurs des applications à la sécurité et à la confidentialité des données, notamment au moyen de procédures internes, chartes, engagements de confidentialité, etc. notamment via l'espace d'information et de collaboration que le titulaire aura mis en place conformément au CCAP.

(b) Mesures de sécurité techniques

De manière générale, il est formellement interdit au titulaire de faire transiter des données personnelles sans que le canal de communication de celles-ci soit sécurisé ou sans que les Données personnelles soient chiffrées, étant entendu que le titulaire utilisera exclusivement les moyens mis à la disposition du ministère pour accéder aux données personnelles.

Par ailleurs, le titulaire s'engage à ce que les mesures de sécurité techniques mises en place répondent *a minima* aux exigences suivantes :

- mise en place d'outils permettant de s'assurer que les données personnelles ne peuvent être lues, copiées, modifiées ou supprimées sans autorisation au cours de leur transfert électronique, de leur transport ou de leur stockage, et que les entités destinataires de tout transfert de données personnelles via les installations servant au transfert de données peuvent être identifiées et vérifiées ;

- mise en place de contrôles permettant de s'assurer que les données personnelles sont protégées contre les destructions ou les pertes accidentelles ;

- mise en place de mesures permettant de veiller à ce que les données personnelles fournies par le ministère puissent être traitées distinctement des données personnelles de ses autres clients en utilisant des séparations logiques ;

- mesures sécurisées d'authentification pour l'accès à ses équipements ;

- mesures de sécurisation physique des locaux, du réseau interne, des matériels, des serveurs et des applications ;

- en tout état de cause, assurer les moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ainsi que 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 ;

- engager une procédure visant à tester, à analyser et évaluer régulièrement l'efficacité des mesures techniques et organisationnelles afin d'assurer la sécurité du traitement.

3.5. Transfert de données personnelles en dehors de l'Union Européenne

Les parties reconnaissent que l'exécution des prestations selon les modalités envisagées par le titulaire implique des transferts internationaux de données personnelles. A cet égard, les parties ont convenu de respecter la procédure suivante :

(a) Tout transfert de données personnelles en dehors de l'Union Européenne ne pourra avoir lieu qu'après autorisation écrite du ministère. Toute modification de flux ou de territoire de transfert en dehors de l'Union Européenne requiert également l'autorisation écrite du ministère.

(b) Tout transfert de données personnelles en dehors de l'Union Européenne ne peut avoir lieu que conformément aux dispositions des articles 44, 45 et 46 du RGPD.

3.6. Sous-traitance ultérieure

Dans le cas où Sorbonne Université aurait autorisé par écrit, expressément et préalablement, le titulaire à sous-traiter les prestations objets du présent contrat, le titulaire s'oblige à :

(a) signer un contrat écrit avec son sous-traitant, lequel fera expressément référence aux présentes et mettra à la charge du sous-traitant des obligations identiques à celles contenues à la présente annexe et qui lui incombent ; le titulaire s'engage à communiquer à ses sociétés affiliées l'ensemble de leurs obligations résultant de la présente annexe ;

(b) mettre à la charge de son sous-traitant toutes obligations incombant au Sous-traitant définies dans la présente annexe pour que soient respectées la confidentialité, la sécurité et l'intégrité des données personnelles, et pour que lesdites données personnelles ne puissent être ni cédées ou louées à un tiers à titre gratuit ou non, ni utilisées à d'autres fins que celles définies au contrat ;

(c) le cas échéant, communiquer au ministère une copie du contrat de sous-traitance ainsi signé ou, à défaut, une description des obligations relatives à la protection des données personnelles mises à la charge du sous-traitant, étant entendu que le titulaire est autorisé à retirer du contrat toute information confidentielle n'étant pas en rapport avec les données personnelles ;

(d) informer le ministère de tout projet de modification des dispositions du contrat signé et/ou des obligations relatives à la protection des données personnelles mises à la charge du sous-traitant ;

(e) Le titulaire est et demeure pleinement responsable devant le ministère de l'exécution par ses sous-traitants de leurs obligations en matière de protection des données personnelles ;

(f) En cas de sous-traitance ultérieure, le ministère se réserve le droit de procéder à toutes vérifications qui lui paraitraient utile pour constater le respect par le titulaire des obligations précitées, et notamment au moyen d'audits. Le titulaire s'engage à répondre aux demandes d'audit du ministère, effectuées par lui-même ou par un tiers de confiance qu'il aura sélectionné et missionné à cette fin. Les audits doivent permettre une analyse du respect par le titulaire des termes de la présente annexe et des dispositions applicables en matière de protection des données personnelles, notamment de s'assurer que des mesures de sécurité et de confidentialité adéquates sont mises en œuvre, qu'elles ne peuvent pas être contournées sans que cela ne soit détecté et que, dans une telle hypothèse ou dans toute autre hypothèse de survenance d'une faille de sécurité, une procédure de notification et de traitement est mise en œuvre par le prestataire pour y remédier sans délai ;

(g) Le titulaire tient à jour une liste des sous-traitants auquel il fait appel dans le cadre du contrat qu'il maintient à disposition de Sorbonne Université et lui communique à première demande de ce dernier ;

(h) Le titulaire, en cas de sous-traitance ultérieure autorisée, informera également Sorbonne Université de toute modification prévue concernant l'ajout ou le remplacement de sous-traitants et s'engage à informer et à signer un contrat écrit avec tout nouveau sous-traitant comme indiqué au (a) ci-dessus.

4. Notification d'incidents/faille de sécurité

(a) Un incident de sécurité (ci-après désigné « Incident ») s'entend comme une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée à des tiers de données personnelles transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données.

(b) Le titulaire s'engage à notifier dès qu'il en a connaissance, et dans un délai maximum de 24h à Sorbonne Université (les coordonnées seront communiquées au titulaire dans les meilleurs délais après la notification du contrat), tout incident entraînant accidentellement ou de manière illicite la perte, l'altération, la divulgation ou l'accès non autorisé à des données personnelles faisant l'objet du traitement.

(c) Cette notification doit préciser :

- la nature et, si elles sont connues, les conséquences probables de l'incident,
- les mesures déjà prises par titulaire ou celles qui sont proposées pour y remédier dans la mesure où elles relèvent de sa responsabilité ;
- les personnes auprès desquelles des informations supplémentaires peuvent être obtenues ;
- lorsque cela est possible, une estimation du nombre de personnes susceptibles d'être impactées par l'Incident.

(d) Dès qu'il est informé d'un incident dont il est à l'origine, le titulaire procède à toutes investigations utiles sur les manquements aux règles de protection afin d'y remédier dans un délai aussi rapide que possible et de faire en sorte d'en diminuer l'impact pour les personnes concernées.

(e) Le titulaire s'engage à informer le ministère de ses investigations et ce de manière régulière.

(f) Les parties s'engagent à collaborer activement pour qu'elles soient en mesure de répondre à leurs obligations réglementaires et contractuelles.

(g) Il revient à Sorbonne Université, en tant que responsable du traitement, de notifier cette violation de données personnelles à l'autorité de contrôle compétente ainsi que, le cas échéant, à la personne concernée dans un délai approprié et après en avoir pris connaissance.

5. Coopération avec les autorités de contrôle

En cas de contrôle d'une autorité compétente en relation avec les données personnelles traitées dans le cadre du présent contrat, les parties s'engagent à coopérer entre elles et avec l'autorité de contrôle.

Dans le cas où le contrôle mené ne concerne que les traitements mis en œuvre par le titulaire en tant que responsable du traitement, le titulaire fait son affaire d'un tel contrôle et s'interdit de communiquer ou de faire état des données personnelles de Sorbonne Université.

Dans le cas où le contrôle mené chez le titulaire concerne les traitements mis en œuvre au nom et pour le compte de Sorbonne Université, le titulaire s'engage à en informer immédiatement ce dernier, dans la mesure permise par la loi, et à ne prendre aucun engagement pour lui.

En cas de contrôle d'une autorité compétente à Sorbonne Université portant notamment sur les prestations réalisées par le titulaire, ce dernier s'engage à coopérer avec le ministère et à lui fournir toute information demandée dont il pourrait avoir besoin ou qui s'avèrerait nécessaire.

6. Obligations particulières du sous-traitant

Dans la mesure où 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 abrogeant la directive 95/46/CE (le « Règlement ») est en vigueur à la date de notification du présent Contrat et est applicable à partir du 25 mai 2018, le titulaire s'engage, à revenir vers Sorbonne Université concernant les points clés suivants du Règlement :

- Tenue du registre :

Le titulaire, en tant que sous-traitant de Sorbonne Université, s'engage à tenir un registre de toutes les catégories d'activités de traitement effectuées pour le compte du responsable du traitement, conformément au RGPD et comprenant :

- le nom et les coordonnées du responsable de traitement 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 responsable du traitement ;
- 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 européen 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, y compris entre autres, 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.

- Analyse d'impact (Privacy Impact Assessment – PIA) :

Conformément à l'article 28.3 du RGPD, le titulaire s'engage à collaborer avec Sorbonne Université pour permettre à celui-ci de réaliser toute analyse d'impact conformément à l'article 35 du RGPD, que ce dernier décidera de mener afin d'évaluer la probabilité et la gravité des risques inhérents à un traitement de données personnelles, compte tenu de sa nature, de sa portée, de son contexte, de ses finalités et des sources du risque. Le titulaire assiste le ministère efficacement afin que cette analyse puisse comporter obligatoirement les éléments suivants

- une description systématique des opérations de traitement envisagées et les finalités du traitement, y compris, le cas échéant, l'intérêt légitime poursuivi par le responsable du traitement ;
- une évaluation de la nécessité et de la proportionnalité des opérations de traitement au regard des finalités ;
- une évaluation des risques sur les droits et libertés des personnes concernées et ;

- les mesures envisagées pour faire face aux risques, y compris les garanties, mesures et mécanismes de sécurité visant à assurer la protection des données à caractère personnel et à apporter la preuve du respect du règlement.

- Code de conduite / Certification:

Le titulaire fera ses meilleurs efforts pour appliquer un code de conduite approuvé au titre du RGPD ou pour obtenir une certification.