

ANNEXE 1

Protection des données à caractère personnel

Table des matières

1 - Description du traitement de données à caractère personnel.....	2
2 - Obligations du titulaire	3
3 - Mesures techniques et organisationnelles de sécurité du traitement	3
4 - Sous-traitance des prestations du Sous-traitant.....	3
5 - Exercice des droits des personnes.....	4
6 - Notification des violations de données à caractère personnel	4
7 - Assistance du Sous-traitant.....	4
8 - Sort des données.....	4
9 - Délégué à la protection des données.....	4
10 - Registre des catégories d'activités de traitement.....	4
11 - Documentation et gestion de la preuve	5
12 - Audit	5
13 - Obligations du Responsable de traitement vis-à-vis du Sous-traitant.....	5

Protection des données à caractère personnel

Conformément à l'article 5.2 du CCAG-PI, chaque partie au contrat 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 contrat. Ces règles sont issues du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 ci-après désigné « le règlement européen sur la protection des données ».

Pour les besoins du présent article, les parties sont dénommées conformément aux définitions énoncées à l'article 4 du règlement (UE) 2016/679 du 27 avril 2016 (ci-après, le « RGPD ») comme suit :

- le titulaire du marché est dénommé le « Sous-traitant » ;
- l'ISAE-SUPAERO est dénommée le « Responsable de traitement ».

Le Sous-traitant déclare être en conformité avec la réglementation en vigueur applicable aux traitements de données à caractère personnel et en particulier au RGPD ainsi qu'aux dispositions de la loi du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés.

Chacune des parties fait son affaire des formalités lui incombant au titre de la réglementation applicable en matière de protection des données à caractère personnel.

1 - Description du traitement de données à caractère personnel

Le titulaire est autorisé à traiter pour le compte de l'acheteur les données à caractère personnel nécessaires pour fournir les prestations objet du contrat.

La Direction des formations et/ou les référents ISAE-SUPAERO adresse à l'organisme de formation : la liste nominative des étudiants, numéro INE, nom, prénom, e-mail, pays et université d'origine, genre.

Cette liste peut être ajustée par ordre de service, selon les conditions visées à l'article 17 du présent CCP.

La nature des opérations réalisées sur les données est :

- Enregistrement de données
- Organisation de données
- Structuration de données
- Adaptation ou modification de données
- Extraction de données
- Consultation de données
- Utilisation de données
- Communication de données (transmission ou toute autre forme de mise à disposition)

Les finalités du traitement sont : l'utilisation pour réaliser la prestation objet du marché. Les données à caractère personnel traitées sont confidentielles.

Les Données courantes sont relatives à l'Etat civil, identité, données d'identification, images. Les Données sensibles ou à caractère hautement personnel sont des données relevant de la prétendue origine raciale ou ethnique. Les catégories de personnes concernées sont les élèves.

La durée du traitement des données est limitée à la période d'exécution du marché notifié et est de 3 ans au maximum.

Le Sous-traitant s'engage à appliquer les durées de conservation des données selon les instructions du Responsable de traitement afin de lui permettre de respecter son obligation d'appliquer une durée de conservation n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées.

2 - Obligations du titulaire

Le Sous-traitant s'engage à :

- traiter les données uniquement pour la ou les seule(s) finalité(s) qui fait/font l'objet de la sous-traitance ;
- ne traiter les données que sur instruction documentée du Responsable de traitement , y compris en ce qui concerne les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, à moins qu'il ne soit tenu d'y procéder en vertu du droit de l'Union ou du droit de l'État membre auquel le Sous-traitant est soumis. Dans ce cas, le Sous-traitant informe le Responsable de traitement de cette obligation juridique avant le traitement, sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public ;
- informer immédiatement le Responsable de traitement si, selon lui, une instruction constitue une violation du règlement européen sur la 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 ;
- garantir la confidentialité, l'intégrité et la disponibilité des données à caractère personnel traitées dans le cadre du présent contrat et pouvoir retracer l'accès à ces données ;
- 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 l'information et la formation nécessaire en matière de protection des données à caractère personnel ;

Le Sous-traitant s'interdit de :

- divulguer, sous quelque forme que ce soit, tout ou partie des données exploitées ;
- prendre copie ou de stocker, quelles qu'en soit la forme et la finalité, tout ou partie des informations ou données contenues sur les supports ou documents qui lui ont été confiés ou recueillies au cours de l'exécution des présentes.

3 - Mesures techniques et organisationnelles de sécurité du traitement

Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le Sous-traitant prend toutes les mesures techniques et organisationnelles requises afin de garantir un niveau de sécurité adapté au risque.

Le Sous-traitant s'engage à maintenir ses moyens au cours de l'exécution des présentes et à défaut, à en informer immédiatement le Responsable de traitement.

4 - Sous-traitance des prestations du Sous-traitant

Le Sous-traitant peut faire appel à un autre sous-traitant (ci-après, « le sous-traitant ultérieur ») pour mener des activités de traitement spécifiques. Dans ce cas, il informe préalablement et par écrit le Responsable de traitement 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 contrat de sous-traitance. Le Responsable de traitement dispose d'un délai maximum de 21 jours à compter de la date de réception de cette information pour présenter ses objections. Cette sous-traitance ne peut être effectuée que si le Responsable de traitement n'a pas émis d'objection pendant le délai convenu.

Le Sous-traitant ultérieur est tenu de respecter les obligations relatives à la protection des données pour le compte et selon les instructions du Responsable de traitement. Il appartient au Sous-traitant initial de s'assurer que le sous-traitant ultérieur 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 RGPD. Si le sous-traitant ultérieur ne remplit pas ses obligations en matière de protection des données, le Sous-traitant initial demeure pleinement responsable devant le Responsable de traitement de l'exécution par l'autre sous-traitant de ses obligations.

5 - Exercice des droits des personnes

Dans toute la mesure du possible, le Sous-traitant aide le Responsable de traitement, par des mesures techniques et organisationnelles appropriées, 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, 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), droit à donner des directives post-mortem sur le sort des données.

Lorsque les personnes concernées exercent auprès du Sous-traitant des demandes d'exercice de droits, le Sous-traitant doit adresser ces demandes dès réception par courrier électronique à l'adresse suivante : marches@isae.fr

6 - Notification des violations de données à caractère personnel

Le Sous-traitant notifie au Responsable de traitement toute violation de données à caractère personnel dès qu'il en a pris connaissance et sans retard indu par mail à l'adresse suivante : dpo@isae-supero.fr.

Cette notification est accompagnée de toute documentation utile afin de permettre au Responsable de traitement, si nécessaire, de notifier cette violation à l'autorité de contrôle compétente dans les 72 heures après la prise de connaissance de la violation.

Lorsque le Responsable de traitement doit gérer une violation de données à caractère personnel qui concerne les traitements réalisés par le Sous-traitant, ce dernier aide le Responsable de traitement à respecter son obligation de notification à l'autorité de contrôle et de communication de la violation à la personne concernée lorsque la violation est susceptible d'engendrer un risque élevé pour ses droits et libertés.

7 - Assistance du Sous-traitant

Le Sous-traitant s'engage selon les moyens et les informations dont il dispose ainsi qu'en fonction de la nature du traitement à fournir au Responsable de traitement toute aide raisonnable qui lui serait nécessaire pour :

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

8 - Sort des données

Au terme de la prestation de services relatifs au traitement de ces données, le Sous-traitant s'engage à supprimer toutes les données à caractère personnel ; les copies existantes seront détruites, à moins que le droit de l'Union ou le droit de l'Etat membre n'exige la conservation des données à caractère personnel.

Une fois les données détruites, le Sous-traitant doit justifier par écrit de la destruction auprès du Responsable de traitement.

9 - Délégué à la protection des données

Le Sous-traitant communique au Responsable de traitement 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

10 - Registre des catégories d'activités de traitement

Le Sous-traitant déclare **tenir par écrit un registre** de toutes les catégories d'activités de traitement effectuées pour le compte du Responsable de traitement 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 RGPD, 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.

11 - Documentation et gestion de la preuve

Le Sous-traitant met à la disposition du Responsable de traitement toutes les informations nécessaires pour démontrer le respect de toutes ses obligations prévues dans les présentes.

Cette documentation sera notamment constituée de tous les éléments permettant de démontrer que les traitements sont effectués conformément à une instruction du Responsable de traitement.

12 - Audit

Le Sous-traitant permettra la réalisation d'audits, y compris des inspections, par le Responsable du traitement ou un autre auditeur qu'il a mandaté.

Le Sous-traitant s'engage à contribuer à la réalisation de ces audits.

Dans le cas où le Sous-traitant ferait l'objet d'une enquête ou d'une demande d'information par l'autorité de contrôle concernant tout traitement effectué pour le compte du Responsable de traitement, le Sous-traitant s'engage à en informer le Responsable de traitement au plus tard dans les 24 heures suivantes à la demande d'information de l'autorité de contrôle et à satisfaire cette enquête ou demande.

13 - Obligations du Responsable de traitement vis-à-vis du Sous-traitant

Le Responsable de traitement s'engage à :

- fournir au Sous-traitant les données nécessaires à la mise en œuvre de ses obligations ;
- documenter par écrit toute instruction concernant le traitement des données par le Sous-traitant ;
- veiller, au préalable et pendant toute la durée du traitement, au respect des obligations prévues par la réglementation applicable en matière de protection des données à caractère personnel de la part du Sous-traitant ;
- superviser le traitement, y compris réaliser les audits et les inspections auprès du Sous-traitant.