**Annexe 1 – CCAP**

**ACCORD DE TRAITEMENT DE DONNEES A CARACTERE PERSONNEL**

**Lot 1 : Mise à disposition d’un système de vote électronique**

Le présent accord a pour objet de définir les conditions dans lesquelles le sous-traitant (titulaire du lot 1) s’engage à effectuer pour le compte du responsable de traitement (Université Sorbonne Nouvelle) les opérations de traitement de données à caractère personnel définies ci-après.

Pour l’application du présent accord, le responsable de traitement, au sens du RGPD, est le pouvoir adjudicateur (l’Université Sorbonne Nouvelle, ci-après, « l’USN ») et le sous-traitant est le titulaire du lot 1 de l’accord-cadre (ci-après, « le titulaire »).

Dans le cadre de leurs relations contractuelles, les parties que sont

Université Sorbonne Nouvelle, 17 rue de la Sorbonne - 75005 Paris, représentée par le responsable de traitement, Monsieur Daniel Mouchard-Zay, Président de l’USN

d’une part, et

***Nom de l’entreprise, Adresse postale - Code postal,* représentée par *fonction du représentant, prénom et nom du représentant***

d’autre part,

s’engagent à respecter la réglementation en vigueur applicable au traitement de données à caractère personnel et, en particulier, le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (ci-après, « le règlement européen sur la protection des données »)

1. **Description du traitement faisant l’objet de la sous-traitance**

* Le sous-traitant est autorisé à traiter pour le compte du responsable de traitement les données à caractère personnel nécessaires pour fournir le ou les services faisant l’objet de l’accord-cadre cité en référence.
* La nature des opérations réalisées sur les données est relative à l’organisation sécurisée d’un vote électronique.

Le détail des opérations est précisé dans le CCTP de l’accord-cadre commun aux deux lots (mise à disposition d’un système de vote électronique et mise en œuvre de l’expertise indépendante du système de vote électronique retenu)

* La ou les finalité(s) du traitement sont : Assurer l’organisation sécurisée du vote électronique dans le cadre des élections mises en œuvre par l’USN liées à l’accord-cadre cité en référence.

Plus précisément, l’organisation des élections universitaires implique :

* + La constitution des listes électorales,
  + La réception des candidatures dans les conditions fixées par la règlementation applicable,
  + L’organisation des scrutins,
  + La mise en œuvre et le scellement d’un système de vote électronique,
  + L’organisation du dépouillement suite aux opérations électorales,
  + L’établissement d’un procès-verbal suite au dépouillement,
  + La proclamation des résultats,
* Les données à caractère personnel traitées sont : les données et informations liées à l’identité et au statut des personnels, vacataires et usagers de l’USN et notamment :
  + Les pièces d’identité pour les personnels candidats,
  + Les informations liées au statut des personnels électeurs de l’USN
  + Les informations liées à la scolarité des étudiants et usagers de l’USN,
  + La date de naissance des électeurs de l’USN ainsi que des candidats.
* Les catégories de personnes concernées sont les personnels et usagers de l’USN.

**II. Durée du contrat**

Le présent accord-cadre est conclu pour une durée de douze (12) mois à compter de sa notification. Il est reconduit trois (3) fois douze (12) mois par tacite reconduction sans que la durée totale ne puisse excéder quatre (4) ans.

**III. Obligations du sous-traitant vis-à-vis du responsable de traitement**

Le sous-traitant s'engage à :

* Traiter les données uniquement pour les seules finalités qui font l’objet de la sous-traitance
* Traiter les données conformément aux instructions documentées du responsable de traitement figurant en annexe du présent contrat. Si le sous-traitant considère qu’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, il en informe immédiatement le responsable de traitement. En outre, si le sous-traitant est tenu de procéder à un transfert de données vers un pays tiers 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 le responsable du traitement de cette obligation juridique avant le traitement, sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public
* Garantir la confidentialité 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 et 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

1. **Sous-traitance**

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 minium de huit (8) 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 du présent contrat 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 règlement européen sur la protection des données. 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.

1. **Droit d’information des personnes concernées**

Le sous-traitant, au moment de la collecte des données, doit fournir aux personnes concernées par les opérations de traitement l’information relative aux traitements de données qu’il réalise. La formulation et le format de l’information doit être convenue avec le responsable de traitement avant la collecte de données.

1. **Exercice des droits des personnes**

Dans la mesure du possible, le sous-traitant doit aider le responsable de traitement 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).

Lorsque les personnes concernées exercent auprès du sous-traitant des demandes d’exercice de leurs droits, le sous-traitant doit adresser ces demandes dès réception par courrier électronique à l’adresse [dpd@sorbonne-nouvelle.fr](mailto:dpd@sorbonne-nouvelle.fr).

1. **Notification des violations de données à caractère personnel**

Le sous-traitant notifie au responsable de traitement toute violation de données à caractère personnel dans un délai maximum de douze (12) heures après en avoir pris connaissance et par le moyen suivant : courriel à l’adresse dpd@sorbonne-nouvelle.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.

Après accord du responsable de traitement, le sous-traitant notifie à l’autorité de contrôle compétente (la CNIL), au nom et pour le compte du responsable de traitement, les violations de données à caractère personnel dans les meilleurs délais et, si possible, soixante-douze (72) heures au plus tard après en avoir pris connaissance, 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 responsable du traitement 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 du responsable de traitement, le sous-traitant communique, au nom et pour le compte du responsable de traitement, 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 le responsable du traitement 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.

1. **Aide du sous-traitant dans le cadre du respect par le responsable de traitement de ses obligations**

Le sous-traitant aide le responsable de traitement pour la réalisation d’analyses d’impact relative à la protection des données. Le sous-traitant aide le responsable de traitement pour la réalisation de la consultation préalable de l’autorité de contrôle.

1. **Mesures de sécurité**

Le sous-traitant s’engage à mettre en œuvre les mesures de sécurité suivantes :

* La pseudonymisation et/ou 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.

1. **Sort des données**

Au terme de la prestation de services relatifs au traitement de ces données, le sous-traitant s’engage à détruire toutes les données à caractère personnel.

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

1. **Délégué à la protection des données (*DPO-DPD*)**

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

1. **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 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, est communiquée, y compris entre autres, selon les besoins :

* 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.

1. **Documentation**

Le sous-traitant met à la disposition du responsable de traitement la documentation nécessaire pour démontrer le respect de toutes ses obligations et pour permettre la réalisation d'audits, y compris des inspections, par le responsable du traitement ou un autre auditeur qu'il a mandaté, et contribuer à ces audits.

**IV. Obligations du responsable de traitement vis-à-vis du sous-traitant**

Le responsable de traitement s’engage à :

* Fournir au sous-traitant les données visées au point I du présent accord ;
* 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 le règlement européen sur la protection des données de la part du sous-traitant ;
* Superviser le traitement, y compris réaliser les audits et les inspections auprès du sous-traitant.

Fait à Paris, le

Signature du représentant de l’entreprise sous-traitante

Signature du responsable de traitement de l’Université Sorbonne Nouvelle

Daniel Mouchard-Zay

Président de l’université