**Annexe 1 au CCAPC portant sur la protection des données à caractère personnel**

**PREAMBULE :**

Dans le cadre de ce marché, l’université de Bordeaux et le titulaire du marché s’engagent à respecter la règlementation en vigueur applicable au traitement de données à caractère personnel. A ce titre, la présente annexe vise à encadrer les responsabilités et les obligations des Parties en matière de protection des données à caractère personnel.

Les dispositions suivantesdéfinissent les conditions dans lesquelles le titulaire du marché, dans le cadre de l’exécution de ce marché public, est amené à réaliser des opérations de traitement de données à caractère personnel pour le compte de l’université de Bordeaux.

Dans ce présent marché, l’université de Bordeaux et le titulaire du marché s’engagent à respecter leurs obligations telles que prévues :

* 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 ;
* Par 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, (RGPD) ;
* 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 à caractère personnel.

L’université de Bordeaux et le titulaire du marché respecteront les engagements prévus au sein de la présente annexe et veilleront à ce que leur personnel permanent ou temporaire et le(s) Sous-traitant(s) ultérieur(s) en respectent les dispositions.

IL A ETE CONVENU CE QUI SUIT :

1. **Définitions**

**Données à caractère personnel :** l’ensemble des données directement ou indirectement identifiantes visant une personne physique faisant l’objet d’un traitement dans le cadre du présent marché public.

**Traitement :** opération, ou ensemble d'opérations, portant sur des Données à caractère personnel, quel que soit le procédé ou le support utilisés.

**Responsable du traitement :** personne morale qui détermine les finalités et les moyens d’un traitement, c’est à dire l’objectif et la façon de le réaliser. L’université de Bordeaux, est Responsable du traitement, au sens de l’article 4.7 du RGPD, c’est-à-dire, la personne morale qui détermine les actions à mener et les résultats attendus pour l’exécution de la prestation faisant l’objet du marché public mis en œuvre par le titulaire qui est sous-traitant au sens de l’article 4.8 RPGD.

**Sous-traitant** : la personne morale qui réalise une prestation de service et qui traite les Données à caractère personnel pour le compte du Responsable de traitement. Le titulaire du marché est qualifié de sous-traitant au sens de l’article 4.8 du RGPD. Dans le cadre de ce marché, ***le titulaire*** est un sous-traitant de l’université de Bordeaux.

**Sous-traitant ultérieur** : personne morale, dont le Sous-traitant a fait appel pour mener des activités de traitement spécifiques nécessaires à l’exécution de la prestation visée par ce marché public et attendu par le Responsable de traitement.

1. **Objet de la présente annexe**

La présente annexe a pour objet de régir les règles de traitement des données personnelles dans le cadre du marché n°2025-088 relatif à la mise à disposition, la correction et la délivrance des résultats des tests d’anglais au profit des étudiants de l’université de Bordeaux.

1. **Description des traitements faisant l’objet du marché public**
2. **Licéité des traitements**

Le traitement défini à l’article 1 de la présente annexe a pour base légale le contrat liant l’Université de Bordeaux et le titulaire du marché public, telle que défini par l’article 9 du RGPD.

1. **Finalités**

Le Responsable du traitement détermine sous sa responsabilité les finalités des traitements confiées au Sous-traitant.

Le Sous-traitant est autorisé à traiter pour le compte du Responsable du traitement les Données à caractère personnel nécessaires pour fournir le ou les prestation(s) de service suivante(s), et selon les modalités suivantes :

* ***Hébergement des données à caractère personnel***

Le Sous-traitant stockera les données à caractère personnel qu’il sera amené à traiter dans le cadre de l’exécution du marché public. Il s’engage à ce que le stockage des données se fasse impérativement en France ou au sein de l’Union européenne.

1. **Catégories de Données à caractère personnel**

Dans le cadre de ce marché public, les [Données à caractère personnel](#Données" \o "Toute information concernant les personnes physiques impliquées dans votre projet de recherche et confiée au Sous-traitant. Exemple: nom(s) et prénom(s) des participants, leurs adresses mails, leurs catégories socio-professionnelles, leurs âges...)que le Sous-traitant sera amené à manipuler sont :

* Nom
* Prénom
* Adresse postale
* Adresse mail
* Numéro de téléphone
* Date de naissance
* Numéro de pièce d’identité (CNI/passeport)
* Numéro de visa

Ces données sont dites « sensibles » au sens de l’article 9 du RGPD.

1. **Personnes concernées**

Les catégories de personnes concernées sont :

* Agents de l’université
* Etudiants de l’université

Ces personnes sont considérées comme des personnes dites « vulnérables » selon les lignes directrices du CEPD.

1. **Conservation des Données à caractère personnel**

Les Données à caractères personnelles devront être conservées pendant la durée du marché jusqu’à l’achèvement complet des prestations.

Le Sous-traitant doit notamment garantir le maintien et le suivi des réservations en cours pour tout type de prestations. Il doit fournir une assistance aux utilisateurs jusqu’à l’achèvement complet des prestations.

1. **Propriété des Données à caractère personnel**

Le Responsable du traitement demeure propriétaire des Données à caractère personnel confiées au Sous-traitant pour l’exécution du marché public concerné.

Dès la finalisation de ce marché public, le Sous-traitant mettra en œuvre le processus de restitution et de destruction des Données à caractère personnel établi par l’article 8 de la présente annexe.

1. **Obligations du Sous-traitant**

Le Sous-traitant s’oblige à :

* Traiter les données personnelles uniquement sur la base d'Instructions du Responsable du traitement et de manière raisonnablement nécessaire ou appropriée pour l'exécution du présent marché ;
* Garantir la confidentialité des Données à caractère personnel traitées dans le cadre du marché public ;
* Ne pas divulguer ces Données à caractère personnel, excepté dans les conditions prévues au présent marché ou sous réserve du consentement écrit du Responsable du traitement ;
* Ne pas vendre, céder, louer ou exploiter commercialement les données à caractère personnel traitées dans le cadre du marché public ;
* Supprimer ou modifier dès la première demande du Responsable du traitement, à bref délai et en tout état de cause dans un délai de 15 jours calendaires maximum, les données personnelles identifiées par le Responsable du traitement ;
* Ne pas effectuer d’études statistiques sur les Données à caractère personnel ou de Traitement sans l’accord préalable du Responsable du traitement pour chaque type d’étude ;
* Notifier immédiatement toute modification ou changement pouvant impacter le Traitement des Données à caractère personnel ;
* Respecter la durée de conservation des Données à caractère personnel au regard des finalités pour lesquelles elles ont été collectées ou transmises et supprimer lesdites Données à l’expiration de la durée de conservation ;
* A coopérer avec le Responsable du traitement pour envisager les hypothèses dans lesquelles la pseudonymisation et le chiffrement des données personnelles pourraient être appropriées pour l’ensemble des phases ;
* A mettre à disposition du Responsable du traitement 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 du Responsable du traitement ou un auditeur externe mandaté ;
* Veiller à ce que les personnes autorisées à traiter les Données à caractère personnel en vertu de la présente annexe s’engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité (par exemple, dans le cadre de leur contrat de travail) et reçoivent la formation nécessaire en matière de protection des Données à caractère personnel ;
* Réaliser les Traitements en respectant les principes de pro­portionnalité, de minimalisation et de limitation des Données à caractère personnel, assurant que seules les Données pertinentes, telles que définies par le Responsable du traitement, sont traitées, pour les seules finalités conve­nues et sous le contrôle des seules personnes ayant à en connaître ;
* Prendre en compte, s’agissant des outils, produits, applications ou services, les principes de protection des données dès la conception et de protection des données par défaut ;
* Ne pas transférer les Données à caractère personnel communiquée dans le cadre de ce marché, hors de l’Union Européenne ;

1. **Obligations de sécurité**

Le Sous-traitant s’engage à assurer la sécurité et la confidentialité des Données à caractère personnel qui lui sont communiquées et auxquelles il pourrait avoir accès sur son environnement (Poste de travail par exemple). Les dispositions du présent article visent expressément les mesures associées à un accès aux Données à caractère personnel sur le ou les systèmes d’information du Sous-traitant.

A ce titre, le Sous-traitant 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 à caractère personnel 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 articles ci-dessous.

Le Sous-traitant s’engage à maintenir ces mesures et moyens pour toute la durée du marché et à défaut, à en informer immédiatement le Responsable du traitement.

En tout état de cause, le Sous-traitant s’engage, en cas de changement des moyens visant à assurer la sécurité, l’intégrité et la confidentialité des Données à caractère personnel, à les remplacer par des moyens équivalents ou d’une performance supérieure.

1. **Mesures de sécurité organisationnelles**

Le Sous-traitant 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;
* Elaboration de mesures restrictives d’accès aux Données à caractère personnel permettant de s’assurer que les personnes habilitées à utiliser le système de traitement de données personnelles ne puissent accéder qu'aux Données à caractère personnel 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 à caractère personnel ne puissent être lues, copiées, modifiées ou supprimées sans autorisation ;
* Mise en place de mesures pour empêcher le transfert des Données à caractère personnel à toute personne ou entité non autorisées ;
* Mise en place de campagnes de sensibilisation des utilisateurs des applications à la sécurité et à la confidentialité des Données à caractère personnel, notamment au moyen de procédures internes, chartes, engagements de confidentialité, etc. notamment via l’espace d’information et de collaboration que le Sous-traitant aura mis en place conformément au CCAP.

1. **Mesures de sécurité techniques**

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

Par ailleurs, le Sous-traitant 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 à caractère personnel 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 à caractère personnel sont protégées contre les destructions ou les pertes accidentelles ;
* Mise en place de mesures permettant de veiller à ce que les Données à caractère personnel fournies par le Responsable du traitement puissent être traitées distinctement des Données à caractère personnel 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. Les Parties se transmettent le nom et les coordonnées de leur Délégué à la protection des données à la date de la signature du marché concerné et s’engagent à se notifier toute nouvelle désignation de Délégué à la protection des données.

1. **Obligations du/des Sous-traitant(s) ultérieur(s)**

Dans le cas où le Responsable du traitement aurait autorisé par écrit, expressément et préalablement, le Sous-traitant à sous-traiter les prestations objets du présent marché, le Sous-traitant s’oblige à :

* Signer un contrat écrit avec le Sous-traitant ultérieur, lequel fera expressément référence aux obligations de la présente annexe ;
* Mettre à la charge du Sous-traitant ultérieur toutes obligations incombant au Sous-traitant définies dans la présente annexe pour que soient respectées la confidentialité, la sécurité et l’intégrité des Données à caractère personnel, et pour que lesdites Données à caractère personnel ne puissent être ni cédées ou louées à un tiers à titre gratuit ou non, ni utilisées à d’autres fins que celles définies dans le cadre du présent marché ;
* Le cas échéant, communiquer au Responsable du traitement une copie du contrat de sous-traitance ainsi signé ou, à défaut, une description des obligations relatives à la protection des Donnée à caractère personnel mises à la charge du Sous-traitant ultérieur, étant entendu que le Sous-traitant est autorisé à retirer du contrat toute information confidentielle n’étant pas en rapport avec les Données à caractère personnel ;
* Informer le Responsable du traitement 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 ultérieur;

Le Sous-traitant est et demeure pleinement responsable devant le Responsable du traitement de l’exécution par le Sous-traitant ultérieur de leurs obligations en matière de protection des Données à caractère personnel ;

En cas de sous-traitance ultérieure, le Responsable du traitement se réserve le droit de procéder à toutes vérifications qui lui paraitraient utiles pour constater le respect par le Sous-traitant des obligations précitées, et notamment au moyen d’audits. Le Sous-traitant s’engage à répondre aux demandes d’audit du Responsable du traitement, effectuées par lui-même ou par un auditeur externe mandaté. Les audits doivent permettre une analyse du respect par le Sous-traitant et le Sous-traitant ultérieur des termes de la présente annexe, et 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 Sous-traitant et le Sous-traitant ultérieur pour y remédier sans délai ;

Le Sous-traitant tient à jour une liste des Sous-traitants ultérieurs auquel il fait appel dans le cadre du marché qu’il maintient à disposition du Responsable du traitement et lui communique dès la première demande de ce dernier ;

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

1. **Sort des Données à caractère personnel**

Au terme du présent marché public, ou en cas de résiliation de ce dernier pour tout motif, le Sous-traitant s'engage à détruire les Données à caractère personnel en sa possession ou sous son contrôle sous un délai de 15 jours.

Le renvoi doit s’accompagner, le cas échéant, de la destruction de toutes les copies existantes dans les systèmes d’information du Sous-traitant et des Sous-traitants ultérieurs le cas échéant.

A la demande du Responsable du traitement, toute destruction visée aux alinéas précédents peut donner lieu, de la part du Sous-traitant et des Sous-traitants ultérieurs le cas échéant, à une justification écrite de la destruction.

1. **Personnes concernées par le traitement**

Il appartient au Responsable du traitement de fournir l’information aux personnes concernées par les opérations de traitement au moment de la collecte des Données, et de répondre aux demandes d’exercice de droit. A ce titre, toutes les personnes concernées peuvent exercer leurs droits en s’adressant au Délégué à la protection des données de l’université de Bordeaux via cette adresse mail : [dpo@u-bordeaux.fr](mailto:dpo@u-bordeaux.fr)

Dans la mesure du possible, le Sous-traitant doit aider le Responsable du 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 au Responsable du traitement à l’adresse suivante : [dpo@u-bordeaux.fr](mailto:dpo@u-bordeaux.fr)