|  |  |
| --- | --- |
| GHT | **Centre Hospitalier Régional et Universitaire de Tours**  **Direction des Achats, de la Logistique, des Approvisionnements et de la Transition Ecologique**  37044 Tours Cedex 9  [http://www.CHRU-tours.fr](http://www.chu-tours.fr) |
| **ACCORD DE SOUS-TRAITANCE DES DONNEES**  **PERSONNELLES**  Procédure N° 2025-DALATE-PREST-077  **Formations d'anglais en e-learning à destination des étudiants des écoles du CHRU de Tours**  Période : A compter du 16 juin 2025, ou de la date de notification si postérieure, pour une durée de 12 mois, renouvelable 3 fois 12 mois.  Le présent document comprend 12 pages | |

Entre les soussignés :

Le Centre Hospitalier Régional Universitaire de Tours, Etablissement public de santé, situé au : 2 Boulevard Tonnellé – 37044 Tours Cedex 9,

Représenté par Madame RIVIERE en qualité de Directrice Générale.

D’une part

Et :

<NOM de la société>,

Marché issu de la procédure N°2025-DALATE-PREST-077

Immatriculé au registre du commerce et des sociétés de ……………………………….………………..

Sous le numéro ……………………………….………………..

dont le siège social est situé au

……………………………….………………..

……………………………….………………..

……………………………….………………..

Représenté par ……………………………….………………..

En qualité de ……………………………….………………..

D’autre part

Tables des matières

[1. Préambule 4](#_Toc162949844)

[2. Définitions prévues par l’article 4 RGPD du 27 avril 2016 4](#_Toc162949845)

[3. Objet de la convention et garanties 4](#_Toc162949846)

[4. Description du traitement 5](#_Toc162949847)

[4.1 Objet 5](#_Toc162949848)

[4.2 Durée 5](#_Toc162949849)

[4.3 Nature et finalités 5](#_Toc162949850)

[4.4 Type 5](#_Toc162949851)

[4.5 Catégorie des personnes 5](#_Toc162949852)

[5. Obligations du Responsable de traitement 5](#_Toc162949853)

[6. Obligations du Titulaire 6](#_Toc162949854)

[7. Sécurité 7](#_Toc162949855)

[8. Droit d’information des personnes concernées 7](#_Toc162949856)

[9. Exercice des droits des personnes 7](#_Toc162949857)

[10. Violation de données 7](#_Toc162949858)

[11. Sous-traitance 8](#_Toc162949859)

[12. Registre 8](#_Toc162949860)

[13. Audit et contrôle 8](#_Toc162949861)

[14. Conservation des données 10](#_Toc162949862)

[15. Produit concerné : <Logiciel xxx> 11](#_Toc162949863)

## Préambule

Dans le cadre de l’exécution du Marché, le Titulaire est amené à traiter des données à caractère personnel pour le compte et sur les instructions du Responsable de traitement.

Le RGPD impose ainsi des obligations spécifiques aux sous-traitants (sécurité, confidentialité, documentation de leur activité) dont la responsabilité sera susceptible d’être engagée en cas de manquement dans le cadre d’un service ou d’une prestation. Ces diverses obligations conduisent notamment à prendre en compte la protection des données dès la conception du service ou du produit ainsi que la mise en place de mesures visant à garantir une protection optimale des données. S’ajoute à ces exigences, une obligation de conseil visant à aider le Responsable de traitement dans la mise en œuvre de certaines obligations du RGPD (consultation préalable de l’autorité de contrôle, étude d’impact sur la vie privée…).

## Définitions prévues par l’article 4 RGPD du 27 avril 2016

**« Données à caractère personnel »** : toute information se rapportant à une personne physique identifiée ou identifiable directement ou indirectement

**« Traitement »** : toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, 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, la limitation, l'effacement ou la destruction

**« Responsable detraitement »** : 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

**« Sous-traitant » :** la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du Responsable de traitement

**« Violation de données à caractère personnel »** : une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données.

**« DPD » ou « DPO »** : Délégué à la Protection des Données ou « Data Protection Officer », fonction rendue obligatoire pour toute société, établissement ou institution traitant des données personnelles, par le Règlement Général sur la Protection des Données Personnelles.

## Objet de la convention et garanties

La présente annexe vise à définir les conditions dans lesquelles le Titulaire s’engage à effectuer pour le compte du Responsable de traitement les opérations de traitement de données à caractère personnels définies au point 4.

La présente annexe vise à garantir au Responsable de traitement que le titulaire respecte bien les obligations légales et règlementaires lui incombant au regard notamment de la réglementation sur la protection des données et le respect de ses obligations au titre de la présente annexe et des dispositions du marché. A ce titre, le Titulaire s’engage à fournir une description de la politique qu’il mène en matière de protection de données.

La présente annexe vise à garantir au Responsable de traitement, que le sous-traitant/titulaire présente bien les garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement des données réponde au RGPD et garantisse ainsi la protection des droits des personnes concernées.

La présente annexe fait partie intégrante des Documents d’exécution du Marché tels que définis à l’article 3 du CCAP et fait office de contrat tel que l’exige l’article 28.3 du RGPD.

## Description du traitement

## 4.1 Objet

Le titulaire est autorisé à traiter pour le compte du Responsable de traitement les données à caractère personnels nécessaires pour fournir le service suivant :

**Formations d'anglais en e-learning à destination des étudiants des écoles du CHRU de Tours**

Le Titulaire est responsable distinct de traitement pour les traitements qu’il réalise pour son propre compte et dont les finalités sont décrites à l’article 4.3 ci-dessous.

## 4.2 Durée

Les traitements réalisés par le Titulaire pour le compte du Responsable de traitement sont réalisés pendant toute la durée nécessaire à l’exécution des prestations fournies par le Titulaire au profit du Responsable de traitement.

## 4.3 Nature et finalités

La nature des opérations réalisées sur les données est la collecte, l’extraction, l’enregistrement, l’utilisation, l’organisation, la structuration, la conservation, l’adaptation, l’effacement ou la destruction.

Les traitements ont pour finalité les formations d'anglais en e-learning à destination des étudiants des écoles du CHRU de Tours.

## 4.4 Type

Les données à caractère personnel traitées sont des données relatives à l’identité et aux formations suivies par les étudiants du CHRU de Tours et l’identité des formateurs.

## 4.5 Catégorie des personnes

Les catégories de personnes concernées sont les étudiants et les responsables de formations.

## Obligations du Responsable de traitement

Le Responsable de traitement s’engage à :

* + - Donner accès au Titulaire aux données visées l’article 4 ci-dessus
    - Documenter par écrit les instructions concernant le traitement des données par le Titulaire notamment dans le cadre de la présente annexe et des autres documents d’exécution du Marché
    - Superviser le traitement, y compris réaliser les audits et les inspections auprès du Titulaire
    - à alerter sans délai le Titulaire en cas d’évolution des services demandés, entraînant ou risquant d’entraîner un changement potentiel du statut sous-traitant du Titulaire au regard de la Réglementation
    - reconnaitre que le Titulaire se limite à suivre les instructions documentées du Responsable de traitement, sous réserve d’informer le Responsable de traitement en cas d’instructions données non conformes à la Réglementation. Toute demande du Responsable de traitement excédant ou modifiant les instructions de traitement figurant à l’article 4.3 du présent contrat fera l’objet d’un devis séparé. Toute instruction non documentée par écrit ou non conforme à la Réglementation n’est pas prise en compte.
    - À fournir l’information aux personnes concernées par les opérations de traitement au moment de la collecte des données à caractère personnel.

## Obligations du Titulaire

Le Titulaire s’engage à prendre toutes les mesures utiles et/ou nécessaires au respect par lui-même et par son personnel de ses obligations et notamment à :

* + - 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
    - Ne pas traiter et consulter les données ou fichiers à d’autres fins que l’exécution des prestations objet du présent marché excepté en ce qui concerne les finalités énumérées à l’article 4.3 de la présente Annexe pour lesquelles le Titulaire agit en tant que Responsable distinct de traitement.
    - Ne pas traiter, consulter les données en dehors du cadre des instructions documentées et des autorisations reçues 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 que le titulaire ne soit tenu d’y procéder en vertu d’une disposition impérative résultant du droit communautaire ou du droit de l’Etat membre auquel elle est soumise. Dans ce cas, le Titulaire informe le Responsable de traitement de cette obligation juridique avant le traitement des données, sauf si le droit concerné interdit une telle information pour des motifs importants d’intérêt public.
    - Ne pas insérer dans les fichiers de données étrangères
    - Ne pas divulguer, sous quelque forme que ce soit, tout ou partie des données exploitées
    - Alerter le Responsable de traitement si une ou plusieurs instructions écrites constituent, directement ou indirectement, une violation du RGPD ou de toute réglementation communautaire ou nationale applicable au traitement
    - Notifier immédiatement au Responsable de traitement toute modification ou changement pouvant impacter le traitement des données à caractère personnel
    - Communiquer les coordonnées et le nom du délégué à la protection des données
    - Assister le responsable de traitement pour la réalisation d’analyses d’impact relatives à la protection des données
    - Veiller à ce que les personnes autorisées à traiter les données à caractère personnel en vertu du présent contrat :

o s’engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité,

o reçoivent la formation nécessaire en matière de protection des données à caractère personnel.

## Sécurité

Des mesures spécifiques de sécurité applicable à tous les traitements sont prévues et comprennent si besoin :

* 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 ou de violation des données à caractère personnel
* Une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

Le Titulaire s’engage notamment à maintenir ces mesures de sécurité mises en œuvre tout au long de l’exécution du Marché et à défaut, à en informer le Responsable de traitement.

## Droit d’information des personnes concernées

L’article 7§1 du RGPD prévoit explicitement que dans les cas où le traitement repose sur le consentement, le responsable de traitement est en mesure de démontrer que la personne concernée a donné son consentement au traitement de données à caractère personnel le concernant.

## Exercice des droits des personnes

Le Titulaire (ou 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 Titulaire (ou sous-traitant) des demandes d’exercice de leurs droits, le Titulaire (ou sous-traitant) doit adresser ces demandes au Délégué à la Protection des Donnés dès réception par courrier électronique : [dpo@chu-tours.fr](mailto:dpo@chu-tours.fr)

## Violation de données

Le Titulaire s’engage à notifier au Responsable de traitement , dans les meilleurs délais (< à 48 heures) après en avoir pris connaissance, toute violation de donnée à caractère personnel, soit toute violation de sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l’altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d’une autre manière, ou l’accès non autorisé à de telles données.

Cette notification doit être envoyée au Délégué à la Protection des Données du Responsable de traitement par courrier électronique ([dpo@chu-tours.fr](mailto:dpo@chu-tours.fr)), puis confirmée par lettre recommandée avec accusé de réception. Elle doit préciser la nature et les conséquences de la violation des données ainsi que les mesures prises ou celles proposées pour y remédier. Lorsque cela est possible, une estimation de nombre de personnes et d’enregistrements impactés est donnée.

Le Titulaire s’engage à collaborer activement avec le Responsable de traitement pour qu’il soit en mesure de répondre à ses obligations réglementaires et contractuelles, et ce, sans frais complémentaires à la charge du Responsable de traitement. Il revient uniquement au Responsable de traitement, de notifier cette violation de données à l’autorité de contrôle compétente ainsi que, le cas échéant, aux personnes concernées.

## Sous-traitance

Le Titulaire ne peut sous-traiter tout ou partie des traitements, notamment vers un pays qui n’est pas situé dans l’Union Européenne, qu’après avoir obtenu l’accord préalable, écrit et exprès du Responsable de traitement. L’identité de chaque sous-traitant situé en dehors de l’UE nécessitera une autorisation spécifique du Responsable de traitement.

Le sous-traitant ultérieur est tenu de respecter les obligations du présent contrat pour le compte et selon les instructions du responsable de traitement. Un contrat spécifique sera conclu entre le sous-traitant initial et le sous-traitant ultérieur. 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.

Le Titulaire peut faire appel à un autre sous-traitant 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 60 jours précédant l’utilisation des services de ce sous-traitant.

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 30 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.

## Registre

Le titulaire s’engage à tenir un registre de toutes les catégories d’activités de traitements effectuées pour le compte du Responsable de traitement, conformément aux dispositions de la réglementation sur la protection de données. Le Titulaire donnera au Responsable de traitement accès à une copie de ce registre sur demande pour les seuls traitements qui le concernent.

Le registre comprend notamment:

* Le nom et les coordonnées du Responsable de traitement pour le compte duquel il agit, des éventuels sous-traitants et le cas échéant le Délégué à la Protection des Données.
* Les catégories de traitements effectués pour le compte du Responsable de 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.
* Une description générale des mesures de sécurité techniques et organisationnelles mises en œuvre par le Titulaire conformément aux dispositions de l’article 7 ci- dessus.

## Audit et contrôle

## 

A la demande du Responsable de traitement, le Titulaire devra établir une attestation ou transmettre toute information utile pour démontrer que les règles prévues par la présente annexe et le Marché, et de manière générale ses obligations en matière de données à caractère personnel ont bien été respectées.

Il est donné la possibilité au responsable de traitement d’effectuer des audits :

1° sur la sécurité et plus particulièrement sur les applications mises en production sur la Plateforme.

2° sur la conformité du Titulaire à ses obligations issues de la règlementation relative à la protection des données à caractère personnel (notamment vis-à-vis du RGPD et de la Loi Informatique et Libertés) en tant que sous-traitant du responsable de traitement (conformément à l’article 4.1. de la présente Accord sur la protection des données à caractère personnel).

L’audit doit permettre notamment de s’assurer que les mesures de sécurité et de confidentialité mises en place ne peuvent être contournées sans que cela ne soit détecté et notifié.

Tout audit doit être validé par le Titulaire. Le Titulaire ne pourra refuser un tel audit que pour motif légitime.

Le Responsable de traitement s’engage alors à prévenir le Titulaire de tout audit sur site ou à distance, dans le respect d’un préavis d’un (1) mois, par l’envoi d’une lettre recommandée avec accusé de réception précisant le périmètre de l’audit, la durée de l’audit, le nom et les références des personnes en charge de l’audit. Le responsable de traitement s’engage à ne pas nommer d’auditeur appartenant à une société directement ou indirectement concurrente du Titulaire. En cas de faille de sécurité avérée concernant les Données personnelles, l’audit pourra néanmoins être réalisé par le CHU de Tours dans le respect d’un préavis de quarante-huit (48) heures. Le Titulaire peut refuser l’auditeur nommé par le Client : en cas de refus, le Titulaire devra le notifier dans un délai de quinze (15) jours calendaires suivant la notification d’audit faite par le Responsable de traitement. A défaut d’accord sur la personne de l’auditeur, le Titulaire pourra proposer un cabinet externe. Le Responsable de traitement ne pourra pas réaliser plus d’un audit du Prestataire sur une période glissante de 12 mois, sauf accord de ce dernier.

Si les éléments que le Responsable de traitement souhaite auditer conformément au présent article ont fait l’objet d’un précédent audit par un prestataire indépendant ou toute autorité compétente, le Prestataire peut lui fournir les résultats de ces précédents audits sur ces éléments. Le Responsable de traitement accepte alors que ces résultats feront foi, de sorte qu’il ne sera plus nécessaire de procéder à l’audit demandé.

En aucun cas, quel que soit le type d’audit envisagé, le Responsable de traitement ne tentera de porter atteinte ou ne portera atteinte aux performances, à la sécurité et à la confidentialité des infrastructures du Titulaire ou des autres clients du Titulaire. Tout manquement à cette obligation relèvera de la seule et unique responsabilité du Responsable de traitement qui en supportera seul toutes les conséquences dommageables et garantira le Titulaire contre celles-ci. Tout audit des services et tout audit impliquant la communication de documents du Titulaire ou une visite des locaux du Titulaire devra également être réalisé dans le respect des politiques de sécurité et de confidentialité du Titulaire. En aucun cas le Responsable de traitement ne pourra tenter d’accéder à d’autres données hébergées par le Titulaire que les Données des utilisateurs qui sont à sa charge, notamment dans le cas d’un audit de sécurité nécessitant des tests d’intrusion. Il est rappelé au Client qu’un tel accès ou tentative d’accès aux données d’autrui est puni pénalement.

Ces audits seront à la charge exclusive du responsable de traitement et le temps qui y serait consacré par les collaborateurs du Titulaire sera facturé au tarif en vigueur au moment des audits.

Le rapport d’audit sera adressé gratuitement et dans les plus brefs délais au Titulaire par l’auditeur afin que le Titulaire puisse formuler toute observation ou objection dans un délai de quinze (15) jours calendaires à partir de la date de réception par le Titulaire dudit rapport. Ce rapport est confidentiel et strictement réservé au Titulaire et au responsable de traitement.

## Conservation des données

Au terme de la prestation, et sauf disposition impérative contraire résultant du droit communautaire ou du droit d’un Etat membre de l’Union européenne applicable aux traitements objets des présentes, le Titulaire s’engage à restituer au Responsable de traitement ou à tout sous-traitant désigné par le Responsable de traitement , dans le cadre de la phase de réversibilité, l’ensemble des Données à caractère personnel qui lui ont été confiées en qualité de sous-traitant.

Le Titulaire s’engage ensuite à détruire l’ensemble des Données à caractère personnel traitées par le Titulaire en qualité de sous-traitant, ainsi que tous les fichiers manuels ou informatisés stockant les Données à caractère personnel collectées, sans en garder de copie, après s’être assuré auprès du Responsable de traitement que ce dernier dispose bien de ces informations et accord formel, écrit et exprès du Responsable de traitement.

Dans l’hypothèse où le droit communautaire ou le droit d’un Etat membre exigerait la conservation des Données à caractère personnel, le Titulaire informera le Responsable de traitement de cette obligation.

Le Titulaire s’engage à fournir à première demande un certificat de suppression des Données à caractère personnel.

1. **Produit concerné : <Logiciel xxx>**

**15.1 Type de données personnelles devant faire l'objet d'un traitement**

|  |  |
| --- | --- |
|  | Etat civil, identité, données d'identification, images… |
|  | Vie personnelle (habitudes de vie, situation familiale, etc.) |
|  | Informations d'ordre économique et financier |
|  | Données de connexion (adresse IP, logs, etc.) |
|  | Données de localisation (déplacements, données GPS, GSM, etc.) |
|  | Données de Santé |
|  | Numéro d'identification national unique (NIR pour la France) |
|  | Données génétiques |
|  | Données biométriques (Identification d'une personne de manière unique) |

**15.2 Durée et finalités du traitement**

|  |  |
| --- | --- |
|  | Gestion administrative |
|  | Gestion des notes des étudiants |
|  | Gestion des parcours de formation |
|  | Flux de données |
|  | Gestion des rendez-vous |
|  | Comptabilité / Facturation |
|  | Gestion administrative de l'établissement de formation |
|  | Durée de conservation : Selon les lois et règlements en vigueur |
|  | .................... |
|  | ....................... |

**15.3 Nature des opérations réalisées sur les données personnelles**

Création, Collecte, Modification, Consultation, Conservation, Diffusion, Destruction, Archivage.

**15.4 Catégories de personnes concernées**

|  |  |
| --- | --- |
| X | Etudiants |
| X | Formateurs et responsables de formations |
|  | Utilisateurs Administratifs |
|  | Prestataires de maintenances |

**15.5 Transfert hors UE**

|  |  |
| --- | --- |
|  | Transfert hors UE (Oui / Non) |

|  |  |
| --- | --- |
|  | Sous-traitants ulterieurs hors UE (Si applicable) |
|  |  |
|  |  |
|  |  |

**15.6 Mesures techniques et organisationnelles**

|  |  |
| --- | --- |
| **Catégories** | **Description** |
| Mesures permettant de garantir la confidentialité des données |  |
| Mesures permettant de garantir l’intégrité des données |  |
| Mesures permettant de garantir la disponibilité des données |  |