

En application du règlement européen du 25 mai 2018, le RGPD responsabilise l'ensemble des acteurs traitant des données à caractère personnel (responsable de traitement et sous-traitant), qu'ils soient ou non établis au sein de l'Union Européenne. Pour plus d'informations : articles 4.7 et 4.8 du règlement général sur la protection des données, articles 28.1, 28.3 et 28.10, article 30.2.

Annexe au cahier des clauses administratives particulières N°2026F002

Clauses relatives à la protection des données personnelles

I. Objet

Les présentes clauses ont pour objet de définir les conditions dans lesquelles le titulaire du présent marché (dénommé ci-après « sous-traitant »), s'engage à effectuer pour le compte de l'UP (dénommée ci-après « responsable de traitement ») les opérations de traitement de données à caractère personnel définies ci-après.

Dans le cadre de leurs relations contractuelles, les parties 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 RGPD) applicable à compter du 25 mai 2018 et la loi du 6 janvier 1978.

II. Traitements 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 dans le cadre des missions qui lui sont confiées par le présent marché.

Les finalités principales des traitements sont :

- L'organisation par voie dématérialisée d'opérations électorales relatives à des consultations ou au renouvellement des instances de l'université de Poitiers, ce qui implique :
 - Constituer les listes électorales des agents, des personnels et des usagers concernés
 - Constituer, le cas échéant, les listes des candidats
 - Constituer les bureaux de vote
 - Voter électroniquement
- Le fonctionnement à distance des instances de l'université de Poitiers, ce qui implique :
 - Constituer les listes de leurs membres
 - Voter électroniquement

La nature des opérations réalisées sur les données est 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, la limitation, l'effacement ou la destruction.

Les catégories de personnes concernées par les traitements sont :

- Dans le cadre des opérations électorales de renouvellement des instances de l'université :
 - Agents publics et tous les personnels en activité pendant l'opération électorale dans le service ou la composante concerné par le renouvellement d'une instance, qu'ils soient inscrits d'office sur la liste électorale, non électeurs ou devant faire une demande d'inscription, notamment des :
 - Enseignants-chercheurs, enseignants et chercheurs

- Personnels BIATSS
 - Usagers inscrits de l'établissement pendant l'opération électorale dans le laboratoire ou la composante concernée
- Dans le cadre des délibérations à distances des instances :
- Membres des instances disposant d'une voix délibérative :
 - Internes à l'établissement élus lors des scrutins ou désignés par nomination
 - Externes siégeant au sein des instances de l'université.

Les données à caractère personnel traitées par le sous-traitant sont :

- Dans le cadre des opérations électorales de renouvellement des instances de l'université :
 - Pour la constitution des listes électorales :
 - Pour les agents et personnels concernés :
 - Données extraites de SIHAM (ou toute nouvelle base de données de gestion RH) pour vérification :
 - Identité :
 - Nom usuel / Nom patronymique
 - Prénom
 - Date de naissance
 - Sexe
 - Adresse électronique
 - Identification comme personnel :
 - Numéro SIHAM
 - Données administratives :
 - Affectation
 - Corps
 - Position administrative
 - Situation contractuelle
 - Situation d'hébergement
 - Situation absences pour cause de CLD
 - Données utilisées pour les listes d'émargement :
 - Identité :
 - Nom usuel / Nom patronymique
 - Prénom
 - Collège
 - Composante/Service
 - Pour les étudiants concernés :
 - Données extraites de APOGEE (ou toute nouvelle base de données de gestion des inscriptions) :
 - Identité :
 - Nom usuel / Nom patronymique
 - Prénom
 - Date de naissance
 - Sexe
 - Adresse électronique
 - Identification comme étudiant :
 - Numéro étudiant
 - Composante/Laboratoire
 - Etape d'inscription
 - Données utilisées pour les listes de vérification et d'émargement :
 - Identité :
 - Nom usuel
 - Prénom
 - Collège
 - Composante/Laboratoire
- Pour la constitution des listes de candidatures :
 - Le formulaire de déclaration individuelle ;
 - Une photocopie des pièces justifiant l'identité et la qualité du candidat (pièce d'identité, carte professionnelle, carte d'étudiant, autre)
- Pour la constitution des bureaux de vote :
 - Données extraites des arrêtés électoraux :
 - Nom

- Prénom,
- Coordonnées professionnelles pour joindre la personne (adresse électronique et numéro de téléphone)
- Pour le vote :
 - Envoi d'un identifiant généré aléatoirement par le système de vote
 - Connexion couplée à une information non triviale
 - Réception d'un code à usage unique au moment de la première connexion au système de vote
- Dans le cadre des délibérations à distances des instances :
 - Données extraites des procès-verbaux ou d'arrêtés :
 - Identité des membres des instances :
 - Nom usuel / Nom patronymique
 - Prénom
 - Sexe
 - Qualité donnant voix délibérative
 - Extraite en interne (SIHAM, APOGEE, etc.) ou communiquée par les extérieurs ou leur institution :
 - Adresse électronique institutionnelle ou personnelle

Afin d'assurer la mise en œuvre du service objet du présent marché, l'UP met à la disposition du sous-traitant les informations :

Les personnes suivantes sont susceptibles d'accéder à ces données personnelles :

- Pour l'organisation par voie dématérialisée d'opérations électorales relatives à des consultations ou au renouvellement des instances de l'université de Poitiers :
 - Président de l'université,
 - Cellule d'assistance technique, composée de personnel du prestataire du système de vote et d'agents de l'université, dont du personnel dûment habilité par les arrêtés électoraux des services suivants :
 - Direction générale des services,
 - Direction des affaires juridiques et des archives,
 - Direction des ressources humaines,
 - Direction formation et réussite étudiante,
 - Délégué à la protection des données,
 - I-médias,
 - Composante/service concerné par l'opération électorale
 - Centre d'appel, composé de personnel du prestataire du système de vote et éventuellement d'agents de l'université,
 - Expert indépendant chargé d'auditer le système de vote ;
 - Bureau de vote, chargé de veiller au bon déroulement des opérations électorales,
 - Commission de recours des opérations électorales et juridictions administratives compétentes en cas de recours
- Pour le fonctionnement à distance des instances de l'université de Poitiers :
 - Président de l'université,
 - Directeur général des services et son adjoint,
 - Agent comptable,
 - Président et, éventuellement, bureau de l'instance concernée,
 - Cellule d'assistance technique, composée de personnel du prestataire du système de vote et d'agents de l'université, dont du personnel d'appui au fonctionnement de l'instance concernée.

Obligations du sous-traitant vis-à-vis de l'UP

Le sous-traitant s'engage à :

III.1- traiter les données uniquement pour la ou les seule(s) finalité(s) qui fait/ont l'objet de la sous-traitance,

III.2- traiter les données conformément aux instructions documentées du responsable de traitement.
Si le sous-traitant considère qu'une instruction constitue une violation du RGPD 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.

III-3- garantir la confidentialité des données à caractère personnel traitées dans le cadre du présent marché,

III-4 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 la formation nécessaire en matière de protection des données à caractère personnel,

III-5- 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.

III-6- respecter les règles suivantes en cas de 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 a obligation de le notifier à l'UP et d'apporter toutes les preuves de la conformité du sous-traitant ultérieur au RGPD. Cette notification doit également 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 sous-traitant informe préalablement et par écrit l'UP 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, les dates du contrat de sous-traitance et apporter toutes les preuves de la conformité du sous-traitant ultérieur au RGPD.

La sous-traitance ultérieure ne peut être effectuée qu'après accord de l'UP.

Le sous-traitant ultérieur est tenu de respecter les obligations du présent marché pour le compte et selon les instructions de l'UP. 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 l'UP de l'exécution par l'autre sous-traitant de ses obligations.

III-7- aider l'UP à respecter ses obligations relatives à la protection des données à caractère personnel :

Le sous-traitant aide l'UP pour la réalisation d'analyses d'impact relatives à la protection des données.

Le sous-traitant aide l'UP pour la réalisation de la consultation préalable de l'autorité de contrôle.

III-8- mettre en œuvre les mesures de sécurité garantissant un niveau de sécurité adapté au risque :

Le candidat décrira précisément dans son mémoire technique les mesures techniques et organisationnelles garantissant un niveau de sécurité adapté au risque y compris, entre autres :

- la pseudonymisation et le chiffrement des données à caractère personnel (*décrire ces mesures*),
- les moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement (*décrire ces mesures*),
- 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 (*décrire ces mesures*),
- une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement (*décrire ces mesures*). »

Le sous-traitant s'engage à mettre en œuvre les mesures de sécurité prévues conformément à la réglementation en vigueur.

III-9- mettre à la disposition de l'UP la documentation nécessaire pour démontrer le respect de toutes ses obligations et pour permettre la réalisation d'audits, y compris des inspections, par l'UP ou un autre auditeur qu'il a mandaté, et contribuer à ces audits.

III. Droit d'information des personnes concernées

Il appartient à l'UP de fournir l'information aux personnes concernées par les opérations de traitement au moment de la collecte des données.

IV. Exercice des droits des personnes

Le sous-traitant doit répondre, au nom et pour le compte de l'UP et dans les délais prévus par le règlement européen sur la protection des données aux demandes des personnes concernées en cas d'exercice de leurs droits (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)), s'agissant des données faisant l'objet de la sous-traitance prévue dans le présent marché.

V. Notification des violations de données à caractère personnel

Le sous-traitant notifie à l'UP par courrier électronique (dpo@univ-poitiers.fr) toute violation de données à caractère personnel dans un délai maximum de 72 heures après en avoir pris connaissance. Le sous-traitant s'assure de la réception de cette notification par tous les moyens nécessaires. 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.

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 sous-traitant 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 de l'UP, le sous-traitant communique, au nom et pour le compte de l'UP, 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.

VII - Sort des données

Au terme de la prestation de service, le sous-traitant s'engage à détruire toutes les données à caractère personnel à l'expiration des voies et délais de recours contre les élections ou les délibérations concernées.

VIII - Délégué à la protection des données

Le sous-traitant communique à l'UP 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. Pour l'université de Poitiers, l'adresse de contact est dpo@univ-poitiers.fr

IX - 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.

X - Obligations du responsable de traitement vis-à-vis du sous-traitant

L'UP s'engage à :

- Fournir au sous-traitant les données visées au II des présentes clauses,
- 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 RGPD de la part du sous-traitant,
- Superviser le traitement, y compris réaliser les audits et les inspections auprès du sous-traitant.