



ANNEXE 1.1 RGPD

INSTRUCTIONS DOCUMENTEES

AC 26-18 Relatif à la tierce maintenance applicative et évolutive de la solution de gestion des ressources humaines Siham (HR Access FPE) des établissements d'enseignement supérieur et de recherche



TABLE DES MATIERES

1.1 Tierce Maintenance applicative	3
1.2 Assistance à l'exploitation d'application de l'offre SI Amue	4
1.3 Expertise, AMOA ou formation	5
1.4 Intégration.....	6
1.5 Gestion des données relationnelles appartenant aux intervenants Amue et nécessaires aux échanges entre l'Amue et le sous-traitant dans le cadre des prestations.....	7
1.6 Gestion des données relationnelles appartenant aux intervenants-collaborateurs du sous-traitant et nécessaires aux échanges entre l'Amue et le sous-traitant dans le cadre des prestations.....	8



1.1 TIERCE MAINTENANCE APPLICATIVE

- Pour les besoins de bases de formation ou de tests de masse (tests de performance sur données issues des établissements), le sous-traitant n'est pas autorisé à récupérer les données réelles des bases de production en dépit même d'une « convention de confidentialité » entre l'Amue, le sous-traitant et les établissements exploitant l'application maintenue.
- Au besoin, le sous-traitant devra fournir aux établissements souhaitant coopérer à la réalisation des tests de masse ou à la constitution de bases de formation, un outil d'anonymisation adapté pouvant être appliqué en toute autonomie par ces établissements eux-mêmes sur leurs propres données avant de les transmettre au sous-traitant via l'Amue sous forme déjà anonymisée.
- Les mécanismes d'anonymisation proposés par le sous-traitant devront être correctement explicités et préalablement évaluables par l'Amue.
- Les mises à jour de la base (ou des bases) de formation ou de tests seront à réaliser par ré-applications successives de l'outil d'anonymisation sur les nouvelles données réelles de l'établissement.
- Le sous-traitant prévoira lorsque nécessaire la mise à jour de l'outil d'anonymisation lui-même en cas de changement de structure, ou en cas de tout autre possible impact de versions évolutives du produit de l'offre SI Amue sur cet outil
- Le sous-traitant s'engage à appliquer le principe de protection des données dès la conception (**Privacy by Design**) conformément aux attendus de l'article 25 et du considérant 78 du RGPD de manière à garantir qu'aucune déficience attachée à la conception même de l'application maintenue ne puisse, lors de son exploitation, rendre impossible la vérification des points de contrôle de l'analyse d'impact sur la vie privée (PIA) exigée par le RGPD (concernant à la fois les mesures de nature dite « juridique » et, le cas échéant, la gestion des risques). Les différents points de contrôle sont mentionnés dans l'annexe n° 1.2.



1.2 Assistance à l'exploitation d'application de l'offre SI Amue

Aucun traitement de données à caractère personnel n'est en principe autorisé.

- Les données à caractère personnel doivent avoir été préalablement anonymisées par le responsable de traitement avant d'être déposées sur DADM ou transmis au sous-traitant.
- L'accès aux environnements de production renfermant des données à caractère personnel est et doit être interdit au personnel du sous-traitant.
- Les interventions d'assistance à l'exploitation nécessitant exceptionnellement un accès à l'environnement de production en dysfonctionnement doivent être effectuées avec un membre de l'équipe du responsable de traitement disposant des droits nécessaires et appeler à effectuer les manipulations préconisées par le sous-traitant (jamais d'accès direct par le sous-traitant).

Cas des données réelles en exploitation consultées sur site par le sous-traitant ou transmis au sous-traitant

- En cas d'urgence exceptionnelle et s'il n'est pas possible de procéder sans connaissance de données à caractère personnel réelles, le traitement par le sous-traitant desdites données ne doit s'effectuer qu'avec l'unique finalité de résoudre le dysfonctionnement fonctionnel de l'application en exploitation. Et ses données doivent être immédiatement détruites dès l'atteinte de cette finalité.
- Les clauses de confidentialité professionnelle auxquelles sont soumis les personnels du sous-traitant susceptibles de prendre connaissance de données à caractère personnel pendant leur mission doivent être telles qu'elles interdisent non seulement la diffusion à un tiers par quelque moyen que ce soit mais aussi l'enregistrement même temporaire de données réelles appartenant au responsable de traitement sur dispositif de stockage individuel.



1.3 Expertise, AMOA ou formation

- Les interventions d'expertise ou d'AMOA nécessitant exceptionnellement un accès à l'environnement de production doivent être effectuées avec un membre de l'équipe du responsable de traitement disposant des droits nécessaires et devant effectuer les opérations recommandées par le sous-traitant (jamais d'accès direct par le sous-traitant).
- Les environnements de formation sont exclusivement alimentés au moyen de données de tests ou de données anonymisées.
- L'accès aux environnements de production renfermant des données à caractère personnel est et doit être interdit au personnel du sous-traitant



1.4 Intégration

- Aucun traitement de données à caractère personnel n'est autorisé.
- En phase de cadrage et d'analyse, les éléments conçus ou à concevoir tels que les éditions, les exemples de cas, les structures de fichiers, les user stories etc. doivent être construites et illustrées avec des données anonymisées ou masquées
- Les phases de recette sont à exécuter sur des « jeux d'essais » de nihilo ou des données anonymisées (et non des données réelles).
- L'accès aux environnements de production renfermant des données à caractère personnel est et doit être interdit au personnel du sous-traitant.
- Le sous-traitant n'est en aucun cas autorisé à enregistrer des données à caractère personnel réelles appartenant au responsable de traitement.
- Dans le cas où des reprises de données sont commandées au sous-traitant, les travaux effectués dans ce cadre doivent être réalisés sur des serveurs appartenant au (futur) responsable de traitement qui en assure la sécurité y compris les sauvegardes logiques et physiques. Le sous-traitant n'est autorisé à effectuer ces travaux sur ses propres dispositifs de stockage.



1.5 Gestion des données relationnelles appartenant aux intervenants Amue et nécessaires aux échanges entre l'Amue et le sous-traitant dans le cadre des prestations

- Cette gestion fait l'objet de la fiche de registre attachée conforme au modèle de la CNIL décrivant les données dites relationnelles indispensables à l'organisation des activités entre les deux Parties et collectées et traitées par le sous-traitant à des fins de communication entre les équipes.



1.6 Gestion des données relationnelles appartenant aux intervenants-collaborateurs du sous-traitant et nécessaires aux échanges entre l'Amue et le sous-traitant dans le cadre des prestations

- Cette gestion fait l'objet de la fiche de registre attachée conforme au modèle de la CNIL décrivant les données dites relationnelles indispensables à l'organisation des activités entre les deux Parties et collectées et traitées par l'Amue à des fins de communication entre les équipes.