Protection des données à caractère personnel (DCP)

Dans le cadre de réalisation de la prestation, des traitements de données à caractère personnel sont réalisés.

Les traitements effectués doivent être conformes au règlement n°2016/679 du 27 avril 2016 relatif la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (RGPD), à la loi n°78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés et aux textes pris pour son application.

Les traitements sont également réalisés en conformité avec toute délibération et recommandation de la Commission nationale de l'informatique et des libertés (CNIL).

Le CNRS est responsable des traitements et le titulaire du marché est sous-traitant au sens de la règlementation sur la protection des données.

Les traitements portés par le responsable de traitement ont pour finalités :

- la vente de formations : de l'inscription au paiement et la délivrance des certificats de formation
- l'organisation des formations : échanges avec les responsables pédagogiques et les intervenants (gestion des déplacements, des rémunérations).

Les traitements de données opérés par le sous-traitant ont pour objectif la fourniture d'un ERP dédié à la formation professionnelle, l'hébergement des données et la maintenance en conditions opérationnelles.

La nature des données personnelles concerne :

► pour les apprenants :

- Des données d'identification : Nom, prénom, civilité, date et lieu de naissance
- Des données liées à la vie professionnelle : fonction, établissement finançant la formation, intitulé et dates de la formation, coordonnées mail et téléphone,
- Identifiants de connexion à l'application pour les inscriptions, les évaluations : logs de connexion, adresses IP

► pour les responsables scientifiques et pédagogiques des formations :

- Des données d'identification : Nom, prénom, civilité, lieu de naissance
- Des données liées à la vie professionnelle : fonction, nom du laboratoire, institut, adresse professionnelle, intitulé de la formation, coordonnées mail et téléphone,
- Identifiants de connexion à l'application : logs de connexion, adresses IP

► pour les intervenants :

- Des données d'identification : Nom, prénom, civilité, date et lieu de naissance, nationalité
- Des données liées à la vie personnelle : adresse postale personnelle,
- Des données liées à la vie professionnelle : fonction, employeur, identifiants CNRS (matricule), intitulé de la formation, coordonnées mail et téléphone,
- Identifiants de connexion à l'application pour la gestion de l'intervention : logs de connexion, adresses IP

Les obligations des parties

Chaque Partie s'engage à respecter l'ensemble des exigences liées à la protection des données personnelles conformément aux dispositions de la loi n°78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés et du règlement européen n°2016/679 sur la protection des données personnelles.

Les Parties assurent et préservent la sécurité, la confidentialité, l'intégrité, la disponibilité et la résilience des systèmes de traitement et des données personnelles et documents contenus dans le périmètre relevant de leurs attributions.

Le CNRS, en tant que responsable de traitement, inscrit le traitement de données personnelles dans le registre des traitements de données tenu par la Déléguée à la Protection des Données du CNRS.

Conformément aux dispositions de l'article 28 du RGPD et de l'article 60 de la loi Informatique et libertés, le sous-traitant s'engage à :

- traiter les données uniquement dans le cadre de la prestation ;
- traiter les données conformément aux dispositions de la prestation et à toute autre instruction du responsable du traitement. Dans l'hypothèse où le sous-traitant estimerait qu'une instruction documentée du responsable du traitement dans le cadre de la prestation pourrait être considérée comme illicite au regard du RGPD ou de la loi Informatique et libertés, il s'engage à en informer immédiatement le responsable du traitement, étant précisé que celui-ci sera seul juge de la validité des instructions données et que cette information ne saurait en aucun cas suspendre la bonne exécution de la prestation par le sous-traitant.

  Le titulaire tient un registre des traitements des données qu'il opère pour le compte du CNRS. Ce registre peut être consulté à tout moment par le CNRS, ou par l'autorité de régulation compétente (Commission nationale de l'informatique et des libertés – CNIL).

Les Parties se communiquent le nom et les coordonnées de leur délégué à la protection des données respectivement désigné.

Les Parties s'engagent à coopérer avec les autorités de protection des données compétentes, notamment en cas de demande d'information ou de contrôle.

Chaque Partie demeure responsable des dommages qui lui seraient imputables concernant la protection des Données à caractère personnel faisant l'objet d'un traitement dans le cadre de l'exécution des Prestations (ex : fuite ou perte de données, intrusion informatique, etc.).

Le titulaire s'engage à mettre en œuvre une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement et atténuer les éventuelles conséquences négatives d'une faille de sécurité.

Il met à la disposition du CNRS toutes les informations nécessaires pour démontrer le respect des obligations prévues au présent article et pour permettre la réalisation d'audits par le CNRS ou tout auditeur dûment mandaté par lui.

Recours à des sous-traitants

Le titulaire est informé que s'il a lui-même recours à des sous-traitants, les dispositions qui lui sont applicables le sont automatiquement à ces sous-traitants, et qu'il fait son affaire de leur information et de la contractualisation écrite de ces obligations. Le CNRS demande communication de ces engagements lors de la phase de consultation et est à tout moment autorisé à vérifier, conformément à la clause d'audit, la réalité de cet engagement.

Le titulaire s'engage à notifier et obtenir l'accord expresse du CNRS de toute modification ou recours à un sous-traitant/hébergeur. En toute hypothèse, le traitement des Données par le sous-traitant ou par l'hébergeur doit respecter les dispositions applicables en matière de protection des données personnelles.

Il appartient au titulaire de s'assurer qu'ils présentent les mêmes garanties quant à la mise en œuvre des mesures techniques et organisationnelles appropriées ainsi que les mesures de sécurité, de manière à ce que le traitement réponde aux exigences des dispositions en vigueur.

Confidentialité

Les données transmises, collectées, exploitées par le titulaire sont, pour partie des données à caractère personnel dont la sensibilité est forte au sens de la règlementation sur la protection des données personnelles.

Le titulaire veille à ce que les personnels autorisés à traiter les données à caractère personnel s'engagent à en respecter la confidentialité ou soient soumis à une obligation légale appropriée de confidentialité et reçoivent la formation nécessaire en matière de protection des données à caractère personnel.

Analyse d'impact sur la vie privée

Le titulaire collabore avec le CNRS pour la réalisation des analyses d'impact sur la vie privée, s'il y a lieu.

L'information et le droit des personnes

Il est convenu que le CNRS est seul tenu de l'obligation de fournir aux personnes dont les données sont traitées l'ensemble des informations requises par les articles 13 et 14 du RGPD.

Par ailleurs, il est tenu du traitement des demandes des personnes concernées par ces traitements dans le cadre de l'exercice de leurs droits conformément aux articles 15 et suivants du RGPD. Le titulaire du marché s'engage à apporter son aide et communique toute information dont le CNRS aurait besoin pour s'acquitter de ces obligations.

La sécurité des données, l'hébergement des données

(i) Conformément au présent CCTP, aux analyses de risques, le titulaire s'oblige à prendre toutes précautions utiles afin de préserver la sécurité des Données et Documents et de les protéger contre toute destruction accidentelle ou illicite, perte, altération, diffusion et de garantir un niveau de sécurité adapté pour que les Données ne soient déformées, endommagées ou communiquées à des personnes non autorisées et d'éviter toute utilisation détournée ou frauduleuse.

(ii) Le sous-traitant s'engage à mettre en œuvre une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement et atténuer les éventuelles conséquences négatives d'une faille de sécurité.

(iii) Il met à la disposition du CNRS toutes les informations nécessaires pour démontrer le respect des obligations prévues au présent article et pour permettre la réalisation d'audits par le CNRS ou tout auditeur dûment mandaté par lui.

L'organisation de la sécurité des systèmes d'information du titulaire pour le projet est décrite dans le Plan d'Assurance Sécurité (PAS).

Le sous-traitant met notamment en œuvre les mesures ci-dessous :

Protection du système d'information

Le sous-traitant se conformera aux exigences du Cahier des Clauses Simplifiées de Cybersécurité (CCSC) préconisées par la Direction de l'État (DAE).

Localisation des informations

Les lieux d'hébergement des données du CNRS, dont les journaux, les jeux d'essai pour les environnements de développement (liste non-exhaustive), satisfont aux exigences de sécurité du donneur d'ordres (CNRS) et aux dispositions de la loi informatique et libertés en vigueur.
Tout transfert de données en dehors des Etats de l'UE est soumis à avis, et autorisation préalable du CNRS, après avis de son Délégué à la Protection des Données.
Le sous-traitant communique la liste de tous les lieux de stockage de données (site d'hébergement principal, site(s) de secours, etc.). Si la faisabilité technique de cette exigence s'avère délicate dans le cadre d'architectures distribuées, il est demandé au sous-traitant d'être en mesure de localiser, a posteriori, et non en permanence, le lieu de stockage des données, en particulier suite à un incident.

Durées de conservation des données, archivage, destruction

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

Le renvoi doit s'accompagner de la destruction de toutes les copies existantes dans les systèmes d'information du sous-traitant, au plus tard six mois après la fin de la prestation. Une fois détruites, le sous-traitant doit justifier par écrit de la destruction.

Traitement des incidents impactant les données à caractère personnel

Le sous-traitant s'engage à communiquer au CNRS dans les meilleurs délais, et sous 48 heures au plus tard après en avoir pris connaissance, la survenance de toute faille de sécurité ayant des conséquences directes sur le traitement des données personnelles ou sur le fonctionnement du système de traitement. Il lui fournit notamment toute information relative à la nature de la violation, au nombre de personnes concernées, aux catégories et au nombre d'enregistrements de données à caractère personnel concernés, ainsi qu'aux conséquences probables de la violation, aux mesures prises pour y remédier et atténuer les éventuelles conséquences négatives. Il conserve en outre tout document relatif à la violation de données, ses effets et les mesures prises pour y remédier.

Le sous-traitant intervient dans le processus de gestion des incidents de sécurité liés à l'application ; son aide est requise pour :

- Evaluer l'impact d'un incident de sécurité sur les DCP (*par exemple* : divulgation de données, modification non autorisée des données, suppression de données…) en nombre d'utilisateurs et en quantité de données exposées ;
- Fournir les correctifs nécessaires à la résolution de l'incident.

Le CNRS peut demander tout complément d'information pour lui permettre d'apprécier la portée de l'incident, afin d'apprécier la nécessité d'informer l'autorité de régulation et/ou les personnes concernées dans les cas prévus par la réglementation.

Le niveau de priorité accordé aux incidents de sécurité impactant les DCP est automatiquement le niveau le plus élevé.

Audit

Le responsable du traitement dispose du droit de faire procéder à ses frais, par ses services ou tout tiers de son choix, à un audit du sous-traitant en vue de vérifier le respect par ce dernier de ses obligations au titre de la présente annexe.

L'audit devra être effectué de manière à préserver les informations confidentielles détenues par les PARTIES et à garantir le respect du secret professionnel.

Le sous-traitant s'engage à permettre et à faciliter la réalisation de ces audits, notamment par la mise à disposition du personnel et de toute la documentation nécessaire et utile à la bonne mise en œuvre des opérations d'audit.

L'audit pourra avoir lieu maximum une fois pendant toute la durée du CONTRAT et à tout moment (i) en cas de suspicion de violation du RGPD ou de la loi Informatique ou libertés ou (ii) pour faire vérifier la mise en place des actions correctives demandées par l'autre PARTIE.

L'audit ne pourra être mis en œuvre qu'à des horaires d'ouverture des bureaux normaux et sous réserve d'un préavis de 10 jours ouvrés, adressé par écrit au sous-traitant et comprenant la désignation des personnes ou entités missionnées par le responsable du traitement pour y procéder. La présence de l'auditeur dans les locaux du sous-traitant ne pourra pas excéder un jour.

Le responsable du traitement s'engage à ce que l'auditeur présente des garanties de confidentialité suffisantes au regard de la nature des informations auxquelles il pourrait accéder dans le cadre de l'audit.

Le sous-traitant pourra s'opposer à la désignation d'un auditeur tiers spécifique si, pour des raisons objectives tenant à sa situation, la réalisation de l'audit par cet auditeur tiers pourrait manifestement lui causer un préjudice direct.

En aucun cas, l'exercice de la faculté de s'opposer à cet audit ne saurait avoir pour objet ou pour effet d'empêcher toute réalisation de l'audit visé par le présent article.

Une copie du rapport d'audit sera remise à chaque PARTIE. Toute recommandation formulée dans le cadre de l'audit sera examinée et les points critiques seront corrigés.

Dans le cas où le rapport d'audit ferait apparaitre une irrégularité, la PARTIE concernée s'engage, dans le cadre d'un plan d'action, à mettre en œuvre à ses frais les mesures correctives nécessaires pour y remédier dans un délai raisonnable à compter de la remise du rapport.