

Droits et obligations des PARTIES en cas de traitement de données à caractère personnel

La réalisation des prestations de service de contrôle légal et de certification légale des comptes individuels et consolidés pour le CNRS nécessite la mise en œuvre d'un traitement de données à caractère personnel dont les modalités sont définies par la présente annexe.

Il est convenu que le CNRS est responsable du traitement visant la certification de ses comptes et le titulaire du marché détient, au sens de l'article 4 du RGPD, la qualité responsable de traitement distinct pour la finalité du traitement portant sur la réalisation de la prestation.

1 TRAITEMENTS CONCERNES

Dans le cadre de l'exécution du marché, le CNRS fournit au titulaire pour la réalisation de la prestation des données à caractère personnel qui concernent les personnels rémunérés par le CNRS, les agents dans les structures de recherche et de service rattachées au CNRS et toute personne ayant un lien avec les activités du CNRS.

Les catégories de données personnelles peuvent être :

- Des données d'identification
- Des données liées à la vie professionnelle des personnes
- Des données financières
- Des données de localisation
- Des données dites sensibles au sens du RGPD (données de santé)
- Des données de connexion

Les destinataires sont les personnels du titulaire du marché affectés à la réalisation des prestations de contrôle légal des comptes.

Les données transmises au titulaire seront conservées par le titulaire le temps de la réalisation de la prestation, puis seront supprimées. Le titulaire fournit au CNRS un certificat de destruction des données au plus tard six mois après la fin de la prestation.

2 ENGAGEMENTS DES PARTIES

Chaque PARTIE assure un traitement loyal et licite des données à caractère personnel.

Elle effectue les formalités prévues par la réglementation et qui lui incombent.

Elle s'engage à ne pas utiliser les informations, par quelque moyen ou finalité que ce soit, pour son propre compte ou pour le compte d'un tiers, à des fins professionnelles ou privées, autres que celles définies à l'art. 1 de la présente annexe.

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.

La Partie qui reçoit une information confidentielle d'une des autres Parties s'engage à ce que les informations confidentielles émanant de la Partie qui les divulgue :

- soient gardées strictement confidentielles et soient traitées avec le même degré de protection qu'elle accorde à ses propres informations confidentielles ;

- ne soient communiquées qu'aux seuls membres de son personnel ou sous-traitants, eux-mêmes soumis à confidentialité contractuellement ou statutairement ayant à les connaître et ne soient utilisées que pour les finalités définies pour les prestations.

Le titulaire veille à ne divulguer aucune donnée à des tiers non autorisés, et s'il en a l'obligation légale, il informe au préalable le CNRS.

Le titulaire s'engage à faire respecter ces obligations par ses salariés, ses préposés et ses sous-traitants.

Les PARTIES coopèrent entre elles et avec l'autorité de contrôle compétente, en lien avec la ou le délégué.e à la protection des données (DPD) qu'elles ont désigné.e.

3 HEBERGEMENT DES DONNEES

Les données sont hébergées dans un pays de l'union européenne. Les lieux d'hébergement des données du CNRS satisfont aux exigences de sécurité du donneur d'ordres (CNRS) et aux dispositions de la réglementation sur la protection des données en vigueur. En outre, la qualification SecNumCloud est nécessaire pour l'hébergement des données.

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.

4 SECURITE DES DONNEES

4. 1 : Obligations générales

Chaque PARTIE s'engage, s'agissant des outils, produits, applications ou services, à prendre en compte les principes de protection des données dès la conception et de protection des données par défaut.

Les PARTIES mettent en œuvre des mesures de sécurité adéquates afin de protéger les données à caractère personnel contre une destruction fortuite ou illicite, une perte fortuite, une altération, une divulgation ou un accès non autorisé, notamment lorsque le traitement suppose la transmission de données par réseau, et contre toute autre forme illicite de traitement et assurent un niveau de sécurité adapté aux risques liés au traitement et à la nature des données à protéger, eu égard au niveau technologique et au coût de mise en œuvre.

Les PARTIES s'engagent également à mettre en place une procédure visant à tester, analyser et évaluer régulièrement l'efficacité des mesures techniques et organisationnelles qu'elles ont mises en place pour assurer la sécurité des traitements.

Lorsqu'un type de traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement s'engage à effectuer, avant le traitement et en lien avec le sous-traitant le cas échéant, une analyse d'impact des opérations de traitement envisagées sur la protection des données à caractère personnel.

4.2 : Modalités techniques

Afin de garantir un niveau de sécurité adapté aux risques identifiés pour les données à caractère personnel dont elles assurent le traitement, les PARTIES s'engagent à mettre en œuvre les mesures techniques et organisationnelles suivantes :

- ✦ Les mesures de sécurisation physique des matériels et des locaux ainsi que les dispositions prises pour la sauvegarde des fichiers :
 - L'accès du personnel aux serveurs est limité aux personnes autorisées à intervenir sur ces derniers ;
 - Les serveurs sont localisés dans une salle fermant à clef et avec code d'accès dans un immeuble lui-même accessible par contrôle d'accès par badge, dans la mesure du possible
 - Les fichiers sont sauvegardés quotidiennement de façon redondante sur plusieurs serveurs de sauvegarde ;
- ✦ Les modalités d'accès aux données, en particulier la gestion des habilitations, les mesures d'identification et d'authentification, les procédures :
 - Les fichiers sont exclusivement accessibles aux personnes autorisées devant utiliser ces fichiers dans le cadre de leur mission;
 - Les fichiers sont accessibles avec un mot de passe personnel et un identifiant personnel ce qui permet d'en contrôler les accès ;
- ✦ Les mesures de sécurité devant être mises en œuvre pour les transmissions de données :
 - Les fichiers sont transmis par système de cryptage des données transmises qui ne peuvent être décodées que par le destinataire.

Le CNRS respecte la politique de sécurité des systèmes d'information de l'Etat (PSSIE) et est soumis à la politique générale des systèmes d'information du CNRS. Il a défini une PGSI opérationnelle conformément aux dispositions du RGS et du RGI, laquelle est revue périodiquement en fonction de la réglementation et des menaces informatiques.

Le titulaire respecte la PSSI du CNRS et toute disposition de sécurité demandée par le CNRS

Les mesures spécifiques de sécurité pour le traitement défini par l'article 1 de la présente annexe sont précisée dans le Plan d'Assurance Sécurité régulièrement mis à jour par le titulaire et le CNRS.

4.3 : Procédure en cas de violation de données

Le titulaire s'engage à notifier au CNRS toute violation de données à caractère personnel dans un délai maximum de 24h après en avoir pris connaissance et par tout moyen approprié.

Cette notification est accompagnée de toute documentation utile afin de permettre au responsable du traitement, s'il l'estime nécessaire en fonction de la gravité, de notifier cette violation à l'autorité de contrôle compétente et aux personnes concernées conformément aux art. 33 et 24 du RGPD.

Elle comprend notamment la nature et l'origine de la violation de données, les catégories de données concernées, une estimation du nombre de personnes affectées, et la description des conséquences possibles et envisageables de la violation de données.

Le titulaire s'engage à prendre ou à proposer au CNRS dans les plus brefs délais toute mesure nécessaire pour identifier l'origine, la nature, l'étendue et les conséquences de la violation de données, remédier à celles-ci et limiter ou supprimer les conséquences préjudiciables.

5 INFORMATION ET DROITS 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.

L'autre PARTIE s'engage à apporter son aide et communique toute information dont il aurait besoin pour s'acquitter de ces obligations.

6 SOUS-TRAITANCE

Le Titulaire ne peut sous-traiter l'exécution des prestations à une autre société ni procéder à une cession de l'accord-cadre sans l'accord écrit préalable du CNRS et dans le respect de la réglementation applicable.

Dans ce cas, le sous-traitant du Titulaire est tenu de respecter les obligations imposées par le présent accord. Il appartient au Titulaire de s'assurer que son sous-traitant présente les mêmes garanties quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences des dispositions en vigueur.

Le Titulaire demeure pleinement responsable devant le CNRS des éventuels manquements de son sous-traitant ou de ses acteurs clé en matière de protection des données. Il s'assure en particulier que :

- Son ou ses sous-traitants respectent 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.
- Son ou ses sous-traitants et le ou les acteurs clé assurent et préservent, en ce qui concerne les éléments sous leur responsabilité, la sécurité, la confidentialité, l'intégrité, la disponibilité et la résilience des systèmes de traitement et des données contenues.

En cas de changement de sous-traitance ou d'acteur clé ayant un impact sur les données à caractère personnel et sur le niveau d'engagement du Titulaire au titre du présent accord, ce dernier s'engage à mettre en place la procédure idoine de notification et d'acceptation par le CNRS.

En cas de manquement à ces dispositions, la responsabilité du Titulaire pourra être engagée conformément à l'article 41 du CCAG-FCS.

7 AUDIT

Le CNRS 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 titulaire 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 titulaire 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 titulaire ne pourra pas excéder un jour.

Le CNRS 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 titulaire 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 apparaître 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.

8 RESPONSABILITE

Chaque PARTIE demeure responsable des dommages qui lui seraient imputables et qui seraient imputables au sous-traitant auquel elle a recours le cas échéant concernant la protection des données à caractère personnel faisant l'objet d'un traitement dans le cadre de l'exécution du CONTRAT.

En cas de manquement par une PARTIE, l'autre PARTIE pourra mettre fin au CONTRAT dans les conditions prévues.