



**PROCEDURE
N°2025-03**

**ACCORD-CADRE DE
PRESTATIONS DE SERVICES EN
TRANSPORT EXPRESS**

**ANNEXE N°1 AU CAHIER DES CLAUSES
PARTICULIERES (CCP)**

**CONFIDENTIALITE, PROTECTION DES DONNEES
ET MESURES DE SECURITE**

Table des matières

ARTICLE 1 – OBLIGATION DE CONFIDENTIALITE	3
ARTICLE 2 – PROTECTION DES DONNEES A CARACTERE PERSONNEL.....	4
2.1 Information des personnes.....	6
2.2 Traitement des demandes d'accès aux données personnelles	6
2.3 Sécurité des données	6
2.4 Localisation du traitement des données.....	6
2.5 Obligations liées à la sous-traitance de prestations par le Titulaire de l'accord-cadre 7	
2.6 Audit.....	7
2.7 Pénalités associées.....	8
ARTICLE 3 – MESURE DE SECURITE	8
3.1 Mesures de sécurité particulières.....	8
3.2 Autorisations d'accès des personnels du Titulaire et de ses sous-traitants	9
3.4 Mesures de portée générale	10
ARTICLE 4 – DISPOSITIONS GENERALES SUR LA PROTECTION DES DONNEES ..	11
4.1 Hébergement des données	11
4.2 Échange d'informations.....	12
4.3 Pénalité pour non-respect des règles de sécurité et de protection des informations confidentielles n'impliquant pas des données à caractère personnel	12
4.3 Plan d'assurance sécurité.....	12

ARTICLE 1 – OBLIGATION DE CONFIDENTIALITE

Sans préjudice des informations ou supports classifiés, les informations ou supports portant la mention diffusion restreinte ou des informations ou supports sensibles au sens des instructions interministérielles n°901¹ et 1300², toutes les informations et données et tous les renseignements, documents et objets, quelle qu'en soit la forme ou la nature, écrits ou oraux, qui seraient communiqués au Titulaire et à l'ensemble de ses intervenants dans le cadre de l'exécution de l'accord-cadre devront être considérés comme strictement confidentiels au sens de l'article 5.1 du CCAG-FCS.

Le Titulaire s'engage et engage ses personnels à ne faire aucune divulgation, sous quelle que forme que ce soit, sans autorisation du CNRS, de tout élément connu dans le cadre du présent accord-cadre, en dehors des communications strictement indispensables à l'exécution du présent contrat.

Le Titulaire s'oblige à aviser immédiatement le CNRS de tout projet de modification relatif à une éventuelle restructuration industrielle et de tout audit de son entreprise de nature à remettre en cause les conditions d'exécution de l'accord-cadre.

Les documents et livrables, quel que soit leur format, qui sont réalisés à l'occasion de l'accord-cadre sont propriété exclusive du CNRS.

Responsable vis-à-vis du CNRS, le Titulaire doit observer le secret professionnel et s'interdit tout conflit d'intérêt.

Le Titulaire, en raison du secret professionnel auquel il est tenu, doit :

- N'accepter que de témoigner de ce qu'il peut savoir sur ses clients ou affaires professionnelles que dans les cas prévus par la loi ;
- Refuser de donner communication des actes et dossiers de ses clients à toute autre personne qu'aux parties elles-mêmes, leurs ayants droit ou leurs mandataires, ou toute personne autorisée par la loi ou par décision judiciaire d'une juridiction française ou européenne, sur justification de leur identité et de leur qualité.

Le secret professionnel n'est pas opposable aux personnes légalement habilitées à effectuer des enquêtes judiciaires, administratives ou douanières, ni aux juridictions françaises ou européennes.

Le Titulaire doit informer ses sous-traitants des obligations de confidentialité qui s'imposent à lui pour l'exécution des contrats, en s'assurant du respect de ces obligations par ses sous-traitants.

¹ ¹ Instruction ministérielle relative à la protection des systèmes d'informations sensibles n°901/SGDSN/ANSSI (NOR : PRMD1503279J)

² ² Instruction ministérielle n°1300 sur la protection du secret de la défense nationale

Par dérogation à l'article 41.2 du CCAG-FCS, le non-respect de ces dispositions entraîne la résiliation immédiate de l'Accord-cadre sans préavis, ni indemnité.

L'open data :

Dans le cadre d'une démarche Open data, conformément à la loi n° 78-753 du 17 juillet 1978 codifiée dans le code des relations entre le public et l'administration, ainsi que dans la perspective de l'application de la directive 2013/37/UE du 26 juin 2013 modifiant la directive du 2003/98/CE concernant la réutilisation des informations du secteur public, le Titulaire de l'accord-cadre fournit au CNRS, dans des standards ouverts (c'est-à-dire selon l'article 4 de la LCEN du 21 juin 2004³ « *tout protocole de communication, d'interconnexion ou d'échange et tout format de données interopérable et dont les spécifications techniques sont publiques et sans restriction d'accès ni de mise en œuvre* ») tels que les formats de type .CSV, .ODS, .XML, .KML, .SHP, les données et bases de données collectées ou produites à l'occasion de l'exécution du présent accord-cadre. Il autorise par ailleurs le CNRS, ou un tiers désigné par celui-ci, à extraire et exploiter librement tout ou partie de ces données et bases de données notamment en vue de la mise à disposition à titre gratuit des informations publiques à des fins de réutilisation à titre gratuit ou onéreux.

Sont expressément exclues de cette démarche les données personnelles ainsi que celles sur lesquelles des tiers détiennent des droits de propriété intellectuelle.

L'accès à ces données pourra se faire notamment sous une licence de réutilisation publique, qui précise les droits et obligations rattachés aux données, conformément au décret n°2017-638 du 27 avril 2017 relatif aux licences de réutilisation à titre gratuit des informations publiques et aux modalités de leur homologation.

ARTICLE 2 – PROTECTION DES DONNEES A CARACTERE PERSONNEL

Pour la protection des données personnelles, les parties s'engagent à respecter les dispositions du règlement européen 2016/279 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données et de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée.

Le Titulaire est amené à traiter ou accéder à des données à caractère personnel (DCP) dans le cadre de la réalisation des prestations.

Conformément aux dispositions du RGPD, le CNRS contracte en qualité de responsable de traitement et le Titulaire intervient en qualité de sous-traitant de traitement des prestations de services de transport express.

La finalité du traitement porte sur : les prestations de services de transport express.

Les personnes concernées sont : l'expéditeur, le destinataire, le payeur et le demandeur de la prestation.

³ Loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique

La nature des données personnelles concernées sont notamment :

- Des données d'identification : nom, prénom, coordonnées, informations de contacts (mail, téléphone) ;
- Des données liées à l'activité professionnelle : structures de rattachement, établissements employeur, adresses postales.
- Des données liées la vie personnelle : téléphone mobile personnel, adresse personnelle.

Les Parties assurent et préservent la sécurité, la confidentialité, l'intégrité, la disponibilité et la résilience, dans le périmètre relevant de leurs attributions :

- Des systèmes de traitement ;
- Des données personnelles ;
- Des documents contenus.

Le CNRS, en tant que responsable de traitement inscrit les traitements de données personnelles concernés dans le cadre du présent accord-cadre dans le registre des traitements de données tenu par le/la Délégué(e) à la Protection des Données.

Le Titulaire tient registre des traitements de DCP 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).

Si le Titulaire considère qu'une instruction constitue une violation ou non-conformité au RGPD, il en informe immédiatement le CNRS.

Le Titulaire communique au CNRS le nom et les coordonnées de son/sa délégué(e) à la protection des données.

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

En leur qualité de sous-traitant et responsable de traitement, le Titulaire et le CNRS examinent et mettent en œuvre les demandes d'exercice des droits des personnes concernant l'accès, l'opposition, la rectification, l'effacement, le retrait du consentement et la portabilité de leurs données dans les conditions prévues par la réglementation.

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.

Le Titulaire 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.

2.1 Information des personnes

Le CNRS procède, au moment de la collecte des données, à l'information des personnes concernées en leur indiquant l'identité du responsable de traitement, les finalités poursuivies par le traitement et les droits dont elles disposent au sens du RGPD.

2.2 Traitement des demandes d'accès aux données personnelles

Le Titulaire intervient dans le processus d'information des personnes et de demandes d'accès aux données personnelles. Il s'engage à coopérer avec le CNRS, par des mesures techniques et organisationnelles appropriées, dans toute la mesure du possible, à permettre l'exercice, par les personnes concernées, de leurs droits d'accès, d'opposition, de rectification ou de suppression prévus par la réglementation.

2.3 Sécurité des données

Le Titulaire s'engage à mettre en œuvre les mesures techniques et organisationnelles pour assurer la sécurité du traitement et atténuer les éventuelles conséquences négatives d'une faille de sécurité.

Le Titulaire s'engage à communiquer au CNRS dans les meilleurs délais, et si possible 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.

Cette notification est accompagnée de toute documentation utile afin de permettre au CNRS, 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 34 du RGPD.

Il lui fournit notamment toute information relative à la nature de la violation notamment :

- Le nombre de personnes concernées,
- Les catégories et le nombre d'enregistrements de données à caractère personnel concernés,
- Les conséquences probables de la violation,
- Ainsi que les 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 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.

2.4 Localisation du traitement des données

En principe, le traitement des données ne peut être localisé en dehors de l'Union européenne.

Toutefois, conformément à l'article 45 du RGPD, tout transfert de données hors de l'Union européenne nécessaire pour la prestation peut être réalisé si la Commission européenne, par

voie de décision, constate que le pays tiers, un territoire ou un ou plusieurs secteurs déterminés dans ce pays tiers, ou l'organisation internationale en question assure un niveau de protection adéquat. En l'absence de décision, un tel transfert peut être réalisé moyennant des garanties appropriés, conformément à l'article 46 du RGPD.

2.5 Obligations liées à la sous-traitance de prestations par le Titulaire de l'accord-cadre

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-cadre. 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.

2.6 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 Titulaire 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 de l'accord-cadre 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 CNRS 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.

2.7 Pénalités associées

En cas de non-respect de ses engagements tels que décrits dans le cadre de réponse technique du Titulaire, ce dernier encourt une pénalité forfaitaire de 1 000 euros HT par manquement constaté, par trimestre et dans la limite de cinq manquements par trimestre.

En cas de constatation de plusieurs faits générateurs, les pénalités ainsi établies sont appliquées de façon cumulative.

ARTICLE 3 – MESURE DE SECURITE

3.1 Mesures de sécurité particulières

En complément de l'article 5.3 du CCAG-FCS, il est précisé que lorsque les prestations sont à exécuter dans un lieu où des mesures de sécurité particulières s'appliquent, ou concernent des informations considérées comme sensibles au titre des différents documents constitutifs de l'accord-cadre, le Titulaire, ses personnels et ses éventuels sous-traitants sont tenus de se conformer aux dispositions édictées ci-après et à la réglementation applicable en la matière.

Le Titulaire ne peut prétendre ni à prolongation du délai d'exécution, ni à indemnité, ni à supplément de prix, par dérogation à l'article 5.3 du CCAG-FCS.

La réglementation sur la protection du potentiel scientifique et technique de la nation (PPST) introduite par les dispositions des articles R.413-1 et suivants du code pénal, du décret n°2011-1425 du 2 novembre 2011 et du décret n°2024-430 du 14 mai 2024 (applicable à compter du

1er janvier 2025) prévoit des dispositions de contrôle de l'accès physique ou virtuel aux Zones à Régime Restrictif (ZRR).

À ce titre, le Titulaire, ses personnels et ses sous-traitants peuvent être soumis aux procédures correspondantes d'autorisations préalables d'accès lorsque l'exécution des prestations est susceptible de concerner les informations relevant d'une ZRR.

3.2 Autorisations d'accès des personnels du Titulaire et de ses sous-traitants

Si la protection des intérêts essentiels du CNRS l'exige, le CNRS peut soumettre l'accès physique ou virtuel à certaines informations, données ou à certains composants sensibles des systèmes et applications du CNRS à l'agrément préalable des personnels du Titulaire et des sous-traitants éventuels y ayant accès, par le Fonctionnaire de Sécurité et de Défense (FSD) du CNRS.

Afin de permettre au CNRS d'effectuer les vérifications nécessaires, le Titulaire s'engage à remplir un formulaire de renseignements comprenant *a minima* les informations suivantes concernant les personnes dont il sollicite l'agrément :

- le patronyme et les prénoms de son personnel ;
- une photocopie lisible et recto-verso d'un titre d'identité dont la nature varie selon la situation individuelle du personnel visé :
 - carte nationale d'identité (CNI) ou passeport en cours de validité pour les ressortissants français et communautaires ;
 - titre de séjour en cours de validité avec une autorisation de travail valable ou carte de résident pour les étrangers extracommunautaires ;
- adresse actuelle du personnel si celle-ci diffère de celle portée sur le titre d'identité fourni.

Par ailleurs, le CNRS se réserve le droit de solliciter toute autre information qu'il juge nécessaire à l'évaluation du risque en considération du niveau de sensibilité des informations ou données concernées, en rapport direct avec la prestation ou l'intervention demandée au titre de l'exécution des prestations objet de l'accord-cadre (exécuté par marchés subséquents/bons de commande).

Les informations demandées au Titulaire ne sont pas utilisées à d'autres fins que celles décrites dans le présent article, et ne sont pas conservées par le CNRS une fois connue la décision prise par le FSD pour le CNRS, d'agréer ou non la personne physique intervenant pour réaliser la prestation demandée au titre de l'accord-cadre (exécuté par marchés subséquents/bons de commande).

A l'issue de la procédure interne d'agrément, le CNRS peut refuser au demandeur, sans indiquer le motif, l'accès aux équipements, installations et données concernés par l'objet du présent accord-cadre. Seule la décision d'agrément ou de refus d'agrément prise sur la base des renseignements fournis par le Titulaire est conservée par le CNRS. Conformément à la réglementation, le refus d'autorisation d'accès n'est pas motivé.

Le refus d'agrément notifié par le CNRS vaut interdiction pour le demandeur d'accéder aux équipements, installations et données concernés par l'objet du présent accord-cadre. Le CNRS peut retirer son agrément à tout moment sans avoir à énoncer ses motifs, le Titulaire doit alors proposer immédiatement un personnel remplaçant, de niveau et compétences équivalents, qui fera l'objet de la procédure d'agrément décrite au présent article.

Le maintien dans les équipes du Titulaire d'un personnel dont l'agrément a été refusé selon la procédure décrite ci-dessus expose le Titulaire et la personne physique concernée à des poursuites pénales.

Le bénéficiaire d'une autorisation d'accès à une ZRR délivrée dans les conditions prévues à l'article R. 413-5-1 du code pénal est tenu d'informer le CNRS de tout changement de situation susceptible d'affecter l'appréciation portée sur son droit d'accès (*à compter du 1^{er} janvier 2025*).

Précisions relatives aux sous-traitants du Titulaire :

Dès lors que l'exécution des prestations de l'accord-cadre a lieu dans une ZRR, les sous-traitants du Titulaire sont soumis aux dispositions générales relatives à la sous-traitance au sens des articles R2193-1 à R2193-9 du code de la commande publique et aux mesures de sécurité particulières visées aux articles 1.1 et 1.2 ci-dessus au titre de la PPST (dont la procédure d'agrément préalable).

Au titre de la PPST, le CNRS se réserve le droit de refuser l'accès physique ou virtuel du sous-traitant du Titulaire à la ZRR sans avoir à se justifier d'une quelconque manière ou de l'autoriser après vérification et agrément préalable suivant la procédure prévue à l'article *Mesures de sécurité particulières* du présent document.

Le Titulaire informe ses sous-traitants de leur soumission aux obligations prévues à cet article et reste responsable du respect de celles-ci envers le CNRS.

Le Titulaire s'engage à insérer dans les documents contractuels régissant ses rapports avec son sous-traitant, l'obligation pour celui-ci de respecter l'ensemble des règles issues de la PPST et de protection de la sécurité des données et systèmes d'information auxquelles le Titulaire est lui-même soumis aux termes du présent accord-cadre.

Toute sous-traitance non-autorisée préalablement par le CNRS autorise celui-ci à résilier, sans indemnité, l'accord-cadre (ou ses bons de commande), pour faute du Titulaire et à ses frais et risques.

3.4 Mesures de portée générale

L'exécution de l'accord-cadre peut conduire le Titulaire et certains de ses personnels à avoir connaissance d'informations sensibles qui, sans être couvertes par le secret de défense, ne doivent pas être rendues publiques.

Le Titulaire s'engage à informer ces personnels de l'ensemble des obligations auxquelles ils sont soumis au titre du présent accord-cadre.

Lorsque la PPST l'exige, le Titulaire de l'accord-cadre et ses personnels doivent se conformer à la procédure interne en vigueur au CNRS, en particulier les dispositions spécifiques applicables aux ZRR détaillées en annexe du règlement intérieur (RI) de l'unité concernée par l'exécution des prestations. Le RI de l'unité est transmis au Titulaire lors de la notification de l'accord-cadre. En cas de modification du RI, le CNRS notifie la version modifiée au Titulaire.

Le Titulaire s'engage à transmettre ce RI d'unité à ses éventuels sous-traitants et s'assure du respect de ses dispositions.

Les personnels du Titulaire ainsi que ses sous-traitants participant à l'exécution des prestations du présent accord-cadre (exécuté par bons de commande) ne doivent en aucune façon accéder à des informations classifiées.

Ils doivent se conformer strictement aux règles de protection des données sensibles qu'ils pourraient avoir à connaître au titre de l'exécution de l'accord-cadre, ainsi qu'au RI de l'unité, aux règles de sécurité et de contrôle en vigueur au CNRS.

Les personnels du Titulaire et ses sous-traitants ne doivent accéder qu'aux seuls locaux et installations concernés et nécessaires pour l'exécution du présent accord-cadre.

L'exécution de l'accord-cadre peut conduire le Titulaire, ses personnels et ses sous-traitants à avoir connaissance des données sensibles qui, sans être couvertes par le secret de défense, ne doivent pas être rendues publiques.

Le Titulaire s'engage et engage ses personnels et ses sous-traitants à ne faire aucune divulgation, sous quelque forme que ce soit, sans autorisation du CNRS, de tout élément connu dans le cadre de l'accord-cadre, en dehors des communications strictement indispensables à l'exécution du présent contrat.

Le non-respect par le Titulaire, ses personnels ou ses sous-traitants des prescriptions de sécurité prévues au titre du présent accord-cadre peut entraîner la résiliation du contrat pour faute du Titulaire, sans indemnité.

L'émission, la reproduction et l'acheminement des documents protégés sont conformes aux règlements en vigueur. Les documents protégés de toutes natures et de tous types ayant servi à la réalisation et à l'exécution du présent accord-cadre sont restitués au CNRS au terme du contrat, sans délai.

Aucune donnée ne peut être partagée ou communiquée par le Titulaire, ses personnels ou ses sous-traitants à un tiers au contrat sans le consentement exprès et préalable du CNRS propriétaire des données.

Les obligations définies ci-dessus doivent continuer à s'appliquer pendant les 10 ans qui suivent la date d'expiration de l'accord-cadre.

ARTICLE 4 – DISPOSITIONS GENERALES SUR LA PROTECTION DES DONNEES

4.1 Hébergement des données

Les systèmes d'information du Titulaire qui traitent les données confiées par le CNRS doivent être considérés comme relevant de l'instruction interministérielle 901 (DR), pouvant comporter des informations à régime restrictif (IRR) et à ce titre :

- **Le Titulaire utilise pour le traitement des données du CNRS des outils et services hébergés de préférence en France** (ou à défaut en Union Européenne), dont les exploitants sont exclusivement sur le même territoire. Une attention particulière est portée sur la souveraineté des outils et services utilisés pour les prestations.
Le Titulaire est sous juridiction FR ou à défaut UE.

L'ensemble des outils et services utilisés par le soumissionnaire est tel que précisé dans le cadre de réponse technique (outils collaboratifs, plateformes d'échange, outils d'analyse, etc.).

4.2 Échange d'informations

Les échanges d'informations seront réalisés de manière à garantir strictement la confidentialité des données en transit et au repos.

Toute donnée sensible sera notamment échangée en utilisant des moyens de communication chiffrés à l'état de l'art, y compris lorsque ces échanges se réalisent par courrier électronique (ce mode étant déconseillé au profit de l'utilisation de plateformes d'échange souveraines et sécurisées, pouvant être fournies au besoin par le CNRS).

4.3 Pénalité pour non-respect des règles de sécurité et de protection des informations confidentielles n'impliquant pas des données à caractère personnel

En cas de non-respect de ses engagements tels que décrits dans le cadre de réponse technique du Titulaire, ce dernier encourt une pénalité forfaitaire de 1 000 euros HT par manquement constaté, par trimestre et dans la limite de cinq manquements par trimestre.

En cas de constatation de plusieurs faits générateurs, les pénalités ainsi établies sont appliquées de façon cumulative.

4.3 Plan d'assurance sécurité

Le Titulaire rédige et maintient un Plan d'Assurance Sécurité (PAS) ayant notamment pour objectif de couvrir les risques liés à l'exécution des prestations portant sur les données confiées par le CNRS. A ce stade, ces risques portent principalement sur la rupture de confidentialité des données, les sources de menace à considérer pouvant être externes (étatique, concurrence, hackers agissant pour leur compte ou le compte de tiers à motivation pécuniaire ou idéologique) ou internes (malveillance ou maladresse d'exploitants, consultants, sous-traitants ou toute personne ayant accès aux données).

Le Titulaire a initialisé le PAS selon le modèle ci-après qu'il a joint à sa réponse à l'appel d'offres. Le PAS doit être mis à jour en cas de modifications.

Il fournit également sur demande du CNRS :

- La Politique de Sécurité des Systèmes d'Information (PSSI) en vigueur dans son entreprise,
- La politique de protection des données personnelles appliquée dans son entreprise, Les nom et contacts du RSSI de sa structure.

Le PAS doit respecter les exigences suivantes :

Titre 1	PSSI du Titulaire et déclinaison (Plan d'Assurance Sécurité) PAS
1.1	Pendant toute la durée de l'accord-cadre, le Titulaire doit formaliser, maintenir à jour, appliquer et contrôler la mise en œuvre de la Politique de Sécurité des

	Systèmes d'Information (PSSI) pour le périmètre placé sous sa responsabilité (notamment par le Plan d'Assurance Sécurité (PAS) et les normes adéquates).
1.2	Le Titulaire décline sa PSSI par la matérialisation d'un Plan d'Assurance Sécurité (PAS) opérationnel et des annexes en découlant.
1.3	Le Titulaire doit prendre toutes les mesures nécessaires pour diminuer la vraisemblance de chacun des risques identifiés par le CNRS.
1.4	Concernant les infrastructures hébergeant le système d'information traitant des données liées à l'accord cadre (commercial, support, , ...), le Titulaire présente les éléments suivants pour chaque brique fonctionnelle : <ul style="list-style-type: none"> - Maître d'œuvre (opérateur, hébergeur) ; - Société de droit ... (sous quelle juridiction étatique ?) ; - La localisation géographique du ou des centre(s) d'hébergements actifs ou passifs (plan de reprise d'activité).
Titre 2	Organisation de la Sécurité des Systèmes d'Information (SSI)
2.1	Nomination d'un RSSI
2.1.1	Le Titulaire doit nommer un RSSI en charge du périmètre applicatif et technique du présent accord cadre.
2.2	Formalisation des responsabilités SSI
2.2.1	L'organisation mise en place par le Titulaire doit inclure une partie dédiée à la SSI, qui définit notamment :
2.2.2	<ul style="list-style-type: none"> • Les responsabilités internes et à l'égard des Tiers ;
2.2.3	<ul style="list-style-type: none"> • Les modalités de coordination avec les autorités externes ;
2.2.4	<ul style="list-style-type: none"> • Les modalités d'application des mesures de protection.
2.2.5	Les procédures d'application des mesures sont portées à la connaissance de toutes les parties prenantes et les intervenants concernés.
2.3	Séparation des rôles
2.3.1	L'organisation des responsabilités SSI chez le Titulaire doit être réalisée de manière à assurer une séparation des fonctions (opérationnelles et prescripteurs) afin d'éviter les conflits d'intérêt.
2.4	Contact avec les autorités
2.4.1	Le Titulaire doit se rendre disponible lors des sollicitations éventuelles des autorités (l'ANSSI, CNIL, FSD, etc).
2.4.2	Le Titulaire informe des modalités de ces échanges.
2.5	Politique de sécurité pour les relations avec les Tiers (sous-traitants)
2.5.1	Le Titulaire doit inclure et formaliser une politique spécifique relative aux relations avec les Tiers dans le cadre des contrats sous-jacents, l'appliquer et contrôler sa mise en œuvre. Cette PSSI doit être revue annuellement.
2.6	Intégration de la sécurité dans les contrats avec les Tiers (sous-traitants)

2.6.1	Le Titulaire doit également intégrer les aspects relatifs à la sécurité, notamment en matière de confidentialité, dans les contrats passés avec les Tiers dans le cadre des contrats sous-jacents.
Titre 3	Gestion des Incidents
3.1	<p>Délais de notification maximums à compter de la constatation de l'incident auprès du CNRS et des autorités de contrôle :</p> <p>72h par le responsable de traitement pour ceux impactant les données à caractère personnel</p> <p>Incident bloquant : 4h</p> <p>Incident majeur : 1 à 2 jours</p> <p>Le Titulaire doit définir et implémenter des procédures et éventuellement des outils lui permettant de détecter les incidents de sécurité, de prévenir (notification) immédiatement, de les traiter de manière appropriée et de capitaliser les retours d'expérience en coordination avec le CNRS.</p> <p>Une fois l'incident clos le Titulaire fournit un rapport d'incident au CNRS indiquant les modalités du traitement.</p>
3.2	Le Titulaire met en place un numéro d'urgence, permettant aux équipes SSI du CNRS, de déclarer un incident de sécurité bloquant ou majeur qu'elles auraient détecté elles-mêmes ou qui aurait été porté à leur connaissance par un tiers.
Titre 4	Contrôle et conformité
4.1	Conformité à la législation sur la protection des informations personnelles
4.1.1	Le Titulaire s'engage à s'assurer de sa conformité à la réglementation sur la protection des données personnelles (Règlement européen sur la protection des données et Loi informatique et liberté, modifié). Le Titulaire fournit la copie de sa politique de protection des données ainsi que la copie de son registre des traitements de données personnelles. Il fournit également les noms et coordonnées du/de la délégué/e à la protection des données qui le conseille.
4.2	4.2 Audits de conformité avec les standards et politiques de sécurité
4.2.1	Le Titulaire doit mener lui-même ou en s'appuyant sur des Tiers spécialisés parmi la liste des Prestataires d'audit de la sécurité des systèmes d'information (PASSI) de l'ANSSI, des audits de conformité avec les standards, la PSSI de l'entreprise et le Plan d'Assurance Sécurité en vigueur.
4.2.2	Le Titulaire transmet sur demande les résultats des audits et les Plans d'Actions associés au CNRS dans un délai raisonnable.
4.3	Délai de traitement d'une vulnérabilité
4.3.1	<p>Lors de la découverte d'un code d'exploitation connu (https://www.cisa.gov/known-exploited-vulnerabilities-catalog), le Titulaire s'engage sur un délai maximum de résolution en rapport avec les délais de traitement exigés ci-dessous.</p> <p>Selon le niveau de gravité de la vulnérabilité de l'exploit (CVSS V3), si le Titulaire estime ce délai trop faible, il notifie ce fait au CNRS en expliquant les raisons et en faisant une contre-proposition.</p>

	<p>Les délais de traitement exigés en fonction du niveau de gravité de la vulnérabilité sont les suivants :</p> <p>Vulnérabilité critique score CVSS ≥ 9) : traitée (correctif ou contournement) en 8h ouvrées</p> <p>Vulnérabilité majeure (score $9 > \text{CVSS} \geq 7$) : traitée (correctif ou contournement) en 2 jours</p> <p>Vulnérabilité moyenne (score $7 > \text{CVSS} \geq 4$) : traitée (correctif ou contournement) en 4 jours</p> <p>Vulnérabilité mineure : traitée (correctif ou contournement) en best effort</p> <p>Le titulaire doit respecter les exigences du décret n° 2024-421 du 10 mai 2024 pris pour l'application des articles L. 2321-2-1 à L. 2321-4-1 du code de la défense et des articles L. 33-14 et L. 36-14 du code des postes et des communications électroniques.</p>
--	---