**Marché public de services**



|  |
| --- |
| **CLAUSES RGPD**  **(Règlement Général sur la Protection des Données)** |

**- ANNEXE n°3 du CCTP -**

**OBJET :**

***«*Fourniture de prestations de développement, qualification, diffusion et formation, des applications nationales pour les Missions Nationales de la DSI² de la région académique Occitanie *»***

**Référence consultation : DSI2\_BDMN\_2501**

**Sommaire**

[**Précisions terminologiques** 3](#_Toc194418104)

[Donnée à caractère personnel 3](#_Toc194418105)

[Traitement 3](#_Toc194418106)

[Fichier 3](#_Toc194418107)

[**Objet et durée** 3](#_Toc194418108)

[**Description du traitement objet du présent accord-cadre** 4](#_Toc194418109)

[**Obligations du titulaire vis-à-vis du Rectorat (article 28.3 du RGPD)** 8](#_Toc194418110)

[**Délégué à la protection des données (articles 37 à 39 du RGPD)** 9](#_Toc194418111)

[**Tenue du registre des activités de traitement (article 30 du RGPD)** 9](#_Toc194418112)

[**Sécurité des données à caractère personnel** 9](#_Toc194418113)

[Mesures de sécurité organisationnelles 10](#_Toc194418114)

[Mesures de sécurité techniques 10](#_Toc194418115)

[**Sous-traitance des activités de traitement (articles 28.2 et 28.4 du RGPD)** 10](#_Toc194418116)

[**Exercice du droit des personnes concernées (articles 13 à 15 du RGPD)** 11](#_Toc194418117)

[**Notification des violations de données à caractère personnel (article 33 du RGPD)** 11](#_Toc194418118)

[**Aide du titulaire dans le cadre du respect par le Rectorat de ses obligations** 12](#_Toc194418119)

[Analyse d’impact 12](#_Toc194418120)

[Coopération avec les autorités de contrôle 12](#_Toc194418121)

[**Transfert de données à caractère personnel en dehors de l’Union Européenne** 13](#_Toc194418122)

[**Obligations du Rectorat vis-à-vis du titulaire** 13](#_Toc194418123)

# **Précisions terminologiques**

Pour l'application du présent article, au sens du règlement (UE) 2016/679 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 abrogeant la directive 95/46/CE (ci-après, « règlement général sur la protection des données » ou RGPD) :

* Le **responsable du traitement** est l'**acheteur,** ici le **Rectorat de Montpellier**
* Le **sous-traitant** est le **titulaire** du marché.
* L’éventuel **sous-traitant du sous-traitant** est le **sous-traitant**.

## Donnée à caractère personnel

Toute information se rapportant à une personne physique identifiée ou identifiable.

Une personne physique peut être identifiée :

* Directement (Exemples : nom, prénom)
* Indirectement par référence à un identifiant (Exemples : numéro client, numéro de téléphone, donnée biométrique, plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale, mais aussi la voix ou l’image).

L’identification peut être réalisée :

* A partir d’une seule donnée (Exemples : numéro de sécurité sociale, ADN)
* A partir d’un croisement de données (Exemples : femme vivant à telle adresse, née tel jour et abonnée à tel magazine).

## Traitement

Toute opération (ou tout ensemble d’opérations) qui est réalisée(é) sur les données à caractère personnel, de manière automatisée ou non, telle(tel) que la collecte, l’enregistrement, l’organisation, 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, le rapprochement ou l’interconnexion, le verrouillage, l’effacement ou la destruction.

## Fichier

Tout ensemble structuré de données à caractère personnel, accessible selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique.

# **Objet et durée**

Les présentes clauses ont pour objet de définir les conditions dans lesquelles le titulaire de l’accord-cadre s'engage à effectuer pour le compte du Rectorat les opérations de traitement de données à caractère personnel définies ci-après.

Dans le cadre du présent accord-cadre, 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 applicable depuis le 25 mai 2018, le RGPD.

Le présent accord entre en vigueur à compter de la date de notification du présent accord-cadre et jusqu’à sa date de fin.

# **Description du traitement objet du présent accord-cadre**

Le titulaire est autorisé à traiter pour le compte du Rectorat, pour la durée du présent accord-cadre, les données à caractère personnel nécessaires pour fournir les prestations du présent accord-cadre.

La nature des opérations réalisées sur les données, les finalités du traitement, les types de données à caractère personnel, ainsi que les catégories de personnes concernées sont décrits dans le tableau ci-dessous.

**Lot 1 et 2 (Domaines Climat Scolaire, Référentiel et Pilotage)**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Objet** | **Finalité** | **Durée** | **Type de données   à caractère personnel** | **Catégories de personnes concernées** | **Rôle du titulaire** |
| Tableaux de Bord des missions Nationales (TBN) | Suivi du consommé des équipes  Gestion du PEM  Outil de suivi financier | Toute la durée de l’accord-cadre | login, nom, prénom, mail professionnel, service/division de rattachement | Agents DNE (administration centrale + académies) | Proposer le service conformément à ses engagements |
| RAMSESE/RODHE | Répertoires - Académique et Ministériel Sur les Etablissements du Système Educatif (RAMSESE)  - des Organismes de Détachement Hors Education (RODHE) | Toute la durée de l’accord-cadre | nom, prénom  mail pro et téléphone  login, nom, prénom, mail professionnel | chef d'établissements ou directeur d'écoles, superviseurs académique, ministère et hors éduc (exemple agriculture, défense)  Compte utilisateurs | Proposer le service conformément à ses engagements |
| ORELIE | Annuaire des internats | Toute la durée de l’accord-cadre | nom, prénom, mail professionnel  login, nom, prénom, mail professionnel | Chef d’établissements  Comptes utilisateurs | Proposer le service conformément à ses engagements |
| EFCI | Echange de fichier comptable par internet | Toute la durée de l’accord-cadre | Pas de traitement de données nominative | N/A | Proposer le service conformément à ses engagements |
| DEMACT | outil de rédaction des actes administratifs dans les établissements scolaires d'enseignement secondaire. | Toute la durée de l’accord-cadre | nom, prénom, mail professionnel  login, nom, prénom, mail professionnel | Personnel administratif des établissements | Proposer le service conformément à ses engagements |
| ELCS | outil permettant de produire des statistiques du climat scolaire dans les écoles, les collèges et les lycées. | Toute la durée de l’accord-cadre | Pas de traitement de données nominative |  | Proposer le service conformément à ses engagements |
| FAITS ETABLISSEMENTS | outils de déclaration de faits graves dans les établissements d’enseignements | Toute la durée de l’accord-cadre | nom, prénom, mail professionnel  login, nom, prénom, mail professionnel | CMVA  Recteur  IEN  Chefs établissements | Proposer le service conformément à ses engagements. |
| Planex | outil de gestion du portefeuille de reporting des projets de la Direction du numérique pour l’Education (DNE). | Toute la durée de l’accord-cadre | nom, prénom, mail professionnel  login, nom, prénom, mail professionnel | DNE | Proposer le service conformément à ses engagements |

**Lot 3 : Domaine PAIE** **en EPLE (Oper@)**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Objet** | **Finalité** | **Durée** | **Type de données   à caractère personnel** | **Catégories de personnes concernées** | **Rôle du titulaire** |
| OPÉR@ PAIE et DSN | Permettre le pilotage d’un cycle de paie et de DSN par le personnel administratif en charge dans le cadre de la rémunération d’agents en EPLE | Toute la durée de l’accord-cadre | **Données relatives à l’identité :**  Numéro de sécurité sociale  Prénom/NOM  Sexe  Date et lieu de naissance  Coordonnées bancaire IBAN  **Données relatives à la situation professionnelle :**  Téléphone  Mail  Lieu de travail  Numéro d’identification interne  Date d’entrée dans l’administration  Nature de contrat de travail/emploi occupé  Ancienneté  **Données relatives à la situation personnelle :**  Téléphone  Mail  Situation familiale  Situation matrimoniale  Enfants à charge  ----------  Régime et base de calcul de la rémunération, éléments déterminant l'attribution d'un complément de rémunération, congés et absences donnant lieu à retenues déductibles ou indemnisables, ainsi que toute retenue légalement opérée par l'employeur, frais professionnels, taux de prélèvement à la source,  Données transmises via la Déclaration sociale nominative, listées et détaillées dans le cahier technique de la norme NEODeS | Chefs d’établissement  Agents comptables  Gestionnaires de paie  Agents payés en EPLE | Proposer le service conformément à ses engagements |

**Lot 4 : Domaine Gestion Financière et Comptable** **en EPLE (GFC/Op@le)**

* GFC

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Objet** | **Finalité** | **Durée** | **Type de données   à caractère personnel** | **Catégories de personnes concernées** | **Rôle du titulaire** |
| GFC Fournisseurs | Permettre le paiement des fournisseurs dans les modules de comptabilité budgétaire et de comptabilité générale de GFC, application installée en "local" dans chaque EPLE: soit par mandatement, soit par ordre de paiement. | Toute la durée de l’accord-cadre | Raison sociale de la structure  Contact: Prénom/NOM  Adresse postale  Téléphone/fax  Adresse électronique  Coordonnées bancaires: IBAN/BIC  Dirigeant ou responsable: Prénom/NOM | Fournisseurs | Proposer le service conformément à ses engagements |
| GFC Elèves et débiteurs | Dans le module de comptabilité générale, fonction de gestion des dettes et créances des élèves envers l'établissement: - encaissement des créances d'hébergement et des créances voyages, notamment par le Prélèvement automatique SEPA, - règlement des bourses nationales et aides aux élèves | Toute la durée de l’accord-cadre | Données collectées par le module BEE de l'application SIECLE, des rubriques "Elèves" et "Responsable":  - identité de l'élève NOM ( de famille et d'usage) et Prénom,  - identité du/des responsables: NOM ( de famille et d'usage) et Prénom,  - adresse postale,  - adresse électronique,  - coordonnées bancaires: IBAN/BIC  - lien avec l'élève,  - nombre d'enfants à charge,  - pour les enfants scolarisés dans l'établissement: NOM/Prénom/Division | Elèves et responsables des élèves | Proposer le service conformément à ses engagements |

* Op@le : les traitements sont identifiés en détail dans le document ci-joint :



|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Objet** | **Finalité** | **Durée** | **Type de données   à caractère personnel** | **Catégories de personnes concernées** | **Rôle du titulaire** |
| OP@LE | Permettre la gestion budgétaire et comptable des EPLE (Lycées, collèges) par le personnel administratif en charge. | Toute la durée de l’accord-cadre | Contacts professionnels ou personnels, Prénom/NOM, Mail professionnel  N°INE  Classe/Régime  Qualité de boursier  Période de scolarisation  Statut mineur/majeur/etc  Identité des responsables légaux et financiers  Tiers de subrogation le cas échéant pour le règlement d’une créance  Qualité vis-à-vis du tiers élèves  Types de concession  Allocation  Consommations de fluides  Signature  Arrêté de cautionnement, Prestation de serment  Dénomination commerciale/bancaire, adresse  Société d'affacturage attachée au tiers (mêmes renseignements)  Type de transaction, Transactions opérées : recettes, types de recettes, Droit à recette, Droit à déduction, mode de règlement le cas échéant, versements, droits à versements, Droit à transaction, Situation du débiteur justifiant la remise gracieuse ou ANV | Ordonnateur  Agent comptable  Régisseur  Adjoint gestionnaire  Mandataire  Prestataires privés  Collectivités publiques  Responsable légaux élèves  Personnels de l’établissement  Personnels employés par l’établissement  Personnels payés par l’établissement mutualisateur de paye  Tout personnel logé  Élèves mineurs (dont émancipés) et majeurs  Personnes physiques | Proposer le service conformément à ses engagements |

# **Obligations du titulaire vis-à-vis du Rectorat (article 28.3 du RGPD)**

Le titulaire s’engage à communiquer au Rectorat, à la première demande de ce dernier, les documents relatifs à la politique informatique et libertés en vigueur au sein de sa société, pour ce qui relève des informations n’ayant pas vocation à rester confidentielles.

Dans le cas où le titulaire ne disposerait pas d’une politique informatique et libertés, il s’engage à en établir une et à la communiquer au Rectorat au plus tard dans les quinze jours suivant la notification de l’accord-cadre, sous peine de se voir appliquer des pénalités (dont les modalités sont précisées à l’article 7 du CCAP).

Par ailleurs, en application de la Réglementation concernant les données à caractère personnel et dans le cadre du présent accord-cadre, les parties reconnaissent, en ce qui concerne l'ensemble des données à caractère personnel qui sont traitées par le titulaire aux fins de réalisation des prestations, qu’il appartient au Rectorat seul, de déterminer la manière (incluant les moyens) et les finalités pour lesquelles ces données à caractère personnel seront traitées par le titulaire.

Dans le cadre de cet accord-cadre, le titulaire est amené à traiter des données à caractère personnel pour le compte du Rectorat. Il s’engage à :

* Traiter les données à caractère personnel pour les seules finalités qui font l’objet du présent accord-cadre.
* Traiter les dites données à caractère personnel uniquement sur la base des instructions documentées du Rectorat et dans la mesure raisonnablement nécessaire ou appropriée pour l’exécution du présent accord-cadre.

Si le titulaire considère qu’une instruction est donnée en violation du RGPD ou de toute autre disposition du droit de l’Union Européenne ou du droit des Etats membres relative à la protection des données, il en informe immédiatement le Rectorat.

* Garantir la confidentialité des données à caractère personnel traitées dans le cadre du présent accord-cadre.
* Veiller à ce que les personnes autorisées à traiter les données à caractère personnel en vertu du présent accord-cadre :
  + 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.
* Ne pas vendre, céder, louer ou exploiter commercialement ces données à caractère personnel.
* Prendre en compte, s'agissant de ses outils, produits, applications ou services, les principes de protection des données dès la conception et par défaut.
* Ne pas effectuer d’études statistiques sur les données à caractère personnel sans l’accord préalable du Rectorat pour chaque type d’étude.
* Respecter la durée de conservation des données à caractère personnel au regard des finalités pour lesquelles elles ont été collectées ou transmises et les supprimer à expiration de la durée de conservation.
* Supprimer ou modifier à première demande du Rectorat, à bref délai et en tout état de cause dans un délai de 15 jours calendaires maximum, les données à caractère personnel identifiées par le Rectorat.
* Fournir, à première demande du Rectorat, un certificat de suppression des données à caractère personnel au Rectorat.
* Notifier immédiatement toute modification ou changement pouvant impacter le traitement des données à caractère personnel.
* Coopérer avec le Rectorat pour envisager les hypothèses dans lesquelles la pseudonymisation et le chiffrement des données à caractère personnel pourraient être appropriés pour l’ensemble des phases de l’accord-cadre.
* Mettre à disposition du Rectorat la documentation nécessaire pour démontrer le respect de toutes ses obligations et pour permettre, le cas échéant, la réalisation d’audits, y compris des inspections, par le Rectorat ou un auditeur mandaté par lui, et à contribuer à ces audits.
* Supprimer dans un délai de 15 jours à compter de la fin de l’accord-cadre, l’intégralité des données à caractère personnel qui lui ont été confiées par le Rectorat, et ce quelle que soit la raison pour laquelle l’accord-cadre prend fin, et justifier par écrit de la destruction.

Le titulaire s’interdit par ailleurs :

* La consultation et le traitement de données à caractère personnel autres que celles concernées par le présent accord-cadre, et ce même si l’accès à ces données est techniquement possible.
* De prendre copie ou de stocker, qu’elles qu’en soient la forme et la finalité, tout ou partie des données à caractère personnel qui lui ont été transmises ou qu’il a collectées au cours de l’exécution de l’accord-cadre, en dehors de l’exécution du présent accord-cadre.
* De divulguer, sous quelque forme que ce soit, tout ou partie des données à caractère personnel à des tiers, excepté dans les conditions prévues au présent accord-cadre ou sous réserve du consentement écrit du Rectorat.

# **Délégué à la protection des données (articles 37 à 39 du RGPD)**

Le titulaire communique au Rectorat dès la notification de l’accord-cadre 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 général sur la protection des données, ou, à défaut, l’identité et les coordonnées d’un point de contact dédié à ces questions.

# **Tenue du registre des activités de traitement (article 30 du RGPD)**

Conformément à 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 applicable depuis le 25 mai 2018, le RGPD, le titulaire est soumis à l’obligation de tenue d’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 du 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 de traitement.
* Le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale et dans le cas des transferts visés à l’article 49, paragraphe 1, deuxième alinéa du règlement général sur la protection des données, les documents attestant de l’existence de garanties appropriées.
* Dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles, notamment, 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.

# **Sécurité des données à caractère personnel**

Le titulaire s’engage à assurer la sécurité et la confidentialité des données à caractère personnel qui lui sont communiquées et auxquelles il pourrait avoir accès sur son environnement (Poste de travail par exemple). Les dispositions du présent article visent expressément les mesures associées à un accès aux données à caractère personnel sur le système d’information du titulaire et de ses sous-traitants le cas échéant.

A ce titre, le titulaire s’engage à :

* Mettre en place des mesures de sécurité organisationnelles et techniques appropriées pour préserver la sécurité et l’intégrité des données à caractère personnel, les protéger contre toute déformation, altération, destruction fortuite ou illicite, endommagement, perte, divulgation ou accès à des tiers non autorisés.
* Garantir la disponibilité et la résilience des systèmes et des services de traitement.
* En cas d’incident physique ou technique, à rétablir la disponibilité des données à caractère personnel et l’accès à celles-ci dans des délais appropriés.
* Maintenir ces mesures et moyens pour toute la durée de l’accord-cadre et à défaut, à en informer immédiatement le Rectorat.
* En cas de changement des moyens visant à assurer la sécurité, l’intégrité et la confidentialité des données à caractère personnel, les remplacer par des moyens équivalents ou d’une performance supérieure.

## Mesures de sécurité organisationnelles

Le titulaire s’engage à mettre en place a minima les mesures de sécurité organisationnelles suivantes :

* Une politique d’habilitations individuelles et de sécurité appropriées pour restreindre l’accès aux données à caractère personnel aux seules personnes qui ont à en connaître.
* Un engagement de confidentialité visant à ce que les personnes autorisées à traiter les données à caractère personnel soient soumises à une obligation de confidentialité, étant entendu que cette obligation peut être prise par le biais du contrat de travail de la personne concernée.
* Des mesures restrictives d’accès aux données à caractère personnel permettant de s’assurer que les personnes habilitées à utiliser le système de traitement de données à caractère personnel ne puissent accéder qu’aux données à caractère personnel auxquelles elles sont habilitées à accéder, conformément à leurs droits d’accès et que, dans le cadre du traitement et de l’utilisation après stockage, les données à caractère personnel ne puissent être lues, copiées, modifiées ou supprimées sans autorisation.
* Des mesures pour empêcher le transfert des données à caractère personnel à toute personne/entité non autorisée.

## Mesures de sécurité techniques

De manière générale, il est formellement interdit au titulaire de faire transiter des données à caractère personnel sans que le canal de communication de celles-ci soit sécurisé ou sans que les données elles-mêmes soient chiffrées, étant entendu que le titulaire utilisera exclusivement les moyens mis à la disposition du Rectorat pour accéder aux données personnelles.

Le titulaire s’engage à mettre en place a minima les mesures de sécurité techniques suivantes :

* Des outils permettant de s'assurer que les données à caractère personnel ne peuvent être lues, copiées, modifiées ou supprimées sans autorisation au cours de leur transfert électronique, de leur transport ou de leur stockage, et que les entités destinataires de tout transfert de données à caractère personnel via les installations servant au transfert de données peuvent être identifiées et vérifiées.
* Des contrôles permettant de s’assurer que les données à caractère personnel sont protégées contre les destructions ou les pertes accidentelles.
* Des mesures permettant de veiller à ce que les données à caractère personnel fournies par le Rectorat puissent être traitées distinctement des données à caractère personnel de ses autres clients en utilisant des séparations logiques.
* Des mesures sécurisées d’authentification pour l’accès à ses équipements.
* Des mesures de sécurisation physique des locaux, du réseau interne, des matériels, des serveurs et des applications.
* En tout état de cause, tous les moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement, ainsi que 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.
* L’engagement d’une procédure visant à tester, à analyser et évaluer régulièrement l'efficacité des mesures techniques et organisationnelles afin d’assurer la sécurité du traitement.

# **Sous-traitance des activités de traitement (articles 28.2 et 28.4 du RGPD)**

Lorsque le titulaire fait appel à un sous-traitant pour mener des activités de traitement spécifiques, il informe préalablement et par écrit le Rectorat de tout changement envisagé concernant l’ajout ou le remplacement de sous-traitants. Cette information doit indiquer clairement les activités sous-traitées, l’identité et les coordonnées du sous-traitant, ainsi que les dates d’intervention.

Afin d’obtenir l’acceptation et l’agrément du Rectorat, le titulaire doit présenter son sous-traitant par le biais de l’acte spécial de sous-traitance, dont les formalités sont comprises dans le formulaire DC4 ou tout autre document équivalent téléchargeable sur <http://www.economie.gouv.fr/daj/formulaires-declaration-candidat>.

Dans le cas où le rectorat a autorisé par écrit, expressément et préalablement le titulaire à sous-traiter les prestations objets du présent accord-cadre, le titulaire s’oblige à :

* Signer un contrat écrit avec son sous-traitant, lequel fera expressément référence aux présentes et mettra à la charge du sous-traitant des obligations identiques à celles contenues à la présente annexe et qui lui incombent ; le titulaire s’engage à communiquer à ses sociétés affiliées l’ensemble de leurs obligations résultant de la présente annexe.
* Informer le rectorat de tout projet de modification des dispositions du contrat signé et/ou des obligations relatives à la protection des données à caractère personnel mises à la charge du sous-traitant.
* Répondre aux demandes d’audit du Rectorat, effectuées par lui-même ou par un tiers de confiance qu’il aura sélectionné et missionné à cette fin. Les audits doivent permettre une analyse du respect par le titulaire et ses sous-traitants des termes de la présente annexe et des dispositions applicables en matière de protection des données à caractère personnel, notamment que des mesures de sécurité et de confidentialité adéquates sont mises en œuvre, qu’elles ne peuvent pas être contournées sans que cela ne soit détecté, et que, dans une telle hypothèse ou dans toute autre hypothèse de survenance d’une faille de sécurité, une procédure de notification et de traitement est mise en œuvre pour y remédier sans délai.

Le titulaire est et demeure pleinement responsable devant le Rectorat de l’exécution par ses sous-traitants de leurs obligations en matière de protection des données à caractère personnel.

# **Exercice du droit des personnes concernées (articles 13 à 15 du RGPD)**

Le titulaire s’engage à respecter les droits d’accès, de rectification, d’opposition, de portabilité et de suppression, le droit à la limitation du traitement ainsi que le droit des personnes concernées de ne pas faire l’objet d’une décision individuelle automatisée, y compris le profilage.

Dès lors, si une personne dont les données à caractère personnel ont été traitées dans le cadre du présent accord-cadre devait contacter directement le titulaire pour exercer son droit d’accès, de rectification, d’opposition, de portabilité et de suppression, de limitation du traitement, ce dernier communiquera au Rectorat dans un délai de trois (3) jours ouvrés, à l’adresse mail qui lui sera communiquée après la notification de l’accord-cadre, les demandes d’exercice de ces droits qui lui seront parvenues.

Le titulaire ne fera droit à ces demandes que sur instruction écrite du Rectorat à cette fin.

# **Notification des violations de données à caractère personnel (article 33 du RGPD)**

Une violation de données à caractère personnel survient de manière accidentelle ou illicite, lors de la destruction, la perte, l’altération, la divulgation ou l’accès non autorisés à des tiers de données à caractère personnel.

Le titulaire s’engage à notifier à l'acheteur toute violation de données à caractère personnel dans un délai maximum de 24h après en avoir pris connaissance, par courrier électronique au Rectorat, et plus particulièrement à la Direction des Systèmes d’Information et de l’Innovation (l’adresse sera communiquée lors de la réunion de lancement), ainsi qu’au Délégué à la protection des données (dpd@ac-montpellier.fr). Cette notification est accompagnée de toute documentation utile afin de permettre au Rectorat, si nécessaire, de notifier cette violation à l’autorité de contrôle compétente (CNIL).

Dès qu’il est informé d’un incident dont il est à l’origine, le titulaire procède à toutes les investigations utiles sur les manquements aux règles de protection afin d’y remédier dans un délai aussi rapide que possible et de faire en sorte d’en diminuer l’impact pour les personnes concernées. Le titulaire s’engage à informer le Rectorat de ses investigations et ce de manière régulière.

Les parties s’engagent à collaborer activement afin d’être en mesure de répondre à leurs obligations réglementaires et contractuelles.

Il revient au Rectorat, en tant que responsable de traitement, de notifier cette violation de données à caractère personnel à l’autorité de contrôle compétente, ainsi que, le cas échéant, à la personne concernée, dans un délai maximum de 72 heures, à moins que la violation en question ne soit pas susceptible d’engendrer un risque pour les droits et libertés des personnes physiques.

Cette notification doit préciser a minima :

* 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, ainsi que 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 Rectorat 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 toutes ces informations ne peuvent pas être fournies en même temps, elles pourront être communiquées de manière échelonnée, sans retard indu.

# **Aide du titulaire dans le cadre du respect par le Rectorat de ses obligations**

Le titulaire aide le Rectorat dans la réalisation d'éventuelles analyses d'impact relatives à la protection des données à caractère personnel, ainsi que dans les possibles interactions entre le Rectorat et les autorités de contrôle.

## Analyse d’impact

Conformément à 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 applicable depuis le 25 mai 2018, le RGPD, le titulaire s’engage à collaborer avec le Rectorat pour permettre à celui-ci de réaliser toute analyse d’impact conformément à l’article 35 du RGPD, que ce dernier décidera de mener afin d’évaluer la probabilité et la gravité des risques inhérents à un traitement de données à caractère personnel, compte tenu de sa nature, de sa portée, de son contexte, de ses finalités et des sources du risque.

Le titulaire assiste efficacement le Rectorat, afin que cette analyse puisse comporter obligatoirement les éléments suivants :

* Une description systématique des opérations de traitement envisagées et les finalités du traitement, y compris, le cas échéant, l'intérêt légitime poursuivi par le responsable du traitement.
* Une évaluation de la nécessité et de la proportionnalité des opérations de traitement au regard des finalités.
* Une évaluation des risques sur les droits et libertés des personnes concernées.
* Les mesures envisagées pour faire face aux risques, y compris les garanties, mesures et mécanismes de sécurité visant à assurer la protection des données à caractère personnel et à apporter la preuve du respect du règlement.

## Coopération avec les autorités de contrôle

En cas de contrôle d’une autorité compétente en relation avec les données à caractère personnel traitées dans le cadre du présent accord-cadre, les parties s’engagent à coopérer entre elles et avec l’autorité de contrôle.

Dans le cas où le contrôle mené ne concerne que les traitements mis en œuvre par le titulaire en tant que responsable du traitement, le titulaire fait son affaire d’un tel contrôle et s’interdit de communiquer ou de faire état des données à caractère personnel du Rectorat.

Dans le cas où le contrôle mené chez le titulaire concerne les traitements mis en œuvre au nom et pour le compte du Rectorat, le titulaire s’engage à en informer immédiatement ce dernier, dans la mesure permise par la loi, et à ne prendre aucun engagement pour lui.

En cas de contrôle d’une autorité compétente au Rectorat, portant notamment sur les prestations réalisées par le titulaire, ce dernier s’engage à coopérer avec le Rectorat et à lui fournir toute information demandée dont il pourrait avoir besoin ou qui s’avérerait nécessaire.

# **Transfert de données à caractère personnel en dehors de l’Union Européenne**

Dans le cas où l’exécution des prestations selon les modalités envisagées par le titulaire impliquerait des transferts de données à caractère personnel hors Union Européenne, les parties conviennent de respecter la procédure suivante :

* Si le titulaire est tenu de procéder à un transfert de données vers un pays tiers (hors de l'Union européenne) ou à une organisation internationale, en vertu du droit de l'Union Européenne ou du droit de l'Etat membre auquel il est soumis, il doit informer le Rectorat de cette obligation juridique avant le traitement, sauf si le droit concerné interdit une telle information.
* Tout transfert de données à caractère personnel en dehors de l’Union Européenne ne pourra avoir lieu qu’après autorisation écrite du Rectorat. Toute modification de flux ou de territoire de transfert en dehors de l’Union Européenne requiert également l’autorisation écrite du Rectorat.
* Tout transfert de données à caractère personnel en dehors de l’Union Européenne ne peut avoir lieu que conformément aux dispositions des articles 44 à 46 du règlement général sur la protection des données.

# **Obligations du Rectorat vis-à-vis du titulaire**

Le Rectorat s’engage à :

* Fournir au titulaire les données à caractère personnel visées dans la clause “Description du traitement objet du présent accord-cadre”.
* Documenter par écrit toute instruction concernant le traitement des données à caractère personnel par le titulaire.
* Veiller, au préalable et pendant toute la durée du traitement, au respect des obligations prévues par le règlement général sur la protection des données de la part du titulaire.
* Superviser le traitement des données à caractère personnel, y compris réaliser les audits et les inspections auprès du titulaire.