

ANNEXE 3 RGPD

Article 1 : Objet de l'annexe

La présente annexe a pour objet de définir et de répartir les obligations incombant à l'Académie de Versailles, au Conseil départemental du Val d'Oise et au Collège en tant que responsables conjoints de traitement en application du Règlement général de la protection des données personnelles (UE) 2016/679 du 27 avril 2016.

Article 2 : Définition des traitements objet de la responsabilité conjointe

Le Conseil départemental, l'Académie de Versailles et les Collèges entendent exercer une responsabilité conjointe sur les traitements de données personnelles dont ils ont défini les moyens et finalités en commun selon les termes de l'article 26 du RGPD.

S'en trouvent exclus tous les traitements de données personnelles opérés par une des parties :

- pour la gestion de ses opérations propres,
- utilisant ses seuls moyens et/ou ses seules données,
- mettant en œuvre une compétence exclusive qui lui est dévolue expressément.

Les traitements n'entrant pas dans la description du paragraphe précédent devront obéir aux règles communes définies ci-après.

Article 3 - Mise en commun de moyens permettant la réalisation des obligations conjointes des parties

Un espace collaboratif dédié sécurisé permettant la mise en œuvre des obligations de la présente annexe est mis à disposition par l'académie de Versailles via la plateforme Tribu. Seuls les Délégués à la protection des données sont autorisés à y accéder.

Article 4 - Information et exercice des droits des personnes concernées

4.1. Information

Les personnes concernées devront recevoir une information complète et compréhensible sur le présent accord qui sera accompagné du détail des traitements conjoints ainsi que des procédures mises en place pour recevoir leurs demandes et leur permettre ainsi d'exercer les droits prévus aux articles 15 à 22 du RGPD.

Pour ce faire, l'Académie et le CDVO rédigent conjointement la charte d'information sur la protection des données relative aux traitements de données à caractère personnel dont ils sont responsables conjoints et respectueuse du principe de transparence du traitement.

Le Collège diffuse la charte d'information par tout autre moyen au sein de son établissement (message électronique adressé à l'ensemble des parents via l'ENT, affichage, etc.).

4.2. Exercice des droits

4.2.1. Modalités de traitement de la demande de droit

L'Académie, le Collège et le Département s'engagent à collaborer dans la gestion des demandes d'exercices des droits d'accès, de rectification, à l'effacement, d'opposition, de limitation du traitement.

Les demandes devront être traitées dans un délai de 1 à maximum 3 mois suivant la complexité de la demande et à compter de la date de la demande initiale d'exercice des droits.

Un modèle type d'accusé de réception de la demande ainsi que la liste des pièces justificatives permettant de vérifier systématiquement l'identité du demandeur, sont rédigés conjointement et utilisés par les deux parties pour toute demande de droit concernant les traitements communs.

Un point hebdomadaire est programmé entre les Délégués à la protection des données (DPD) de chaque entité. Le point peut se réaliser selon les besoins et les contraintes de chacun en présentiel, par visioconférence, par téléphone ou par email.

Ce point hebdomadaire a pour objectif de

- assurer la fluidité du processus et le respect des délais,
- faire un état des lieux des demandes en cours,
- effectuer leur répartition de la réponse entre les DPD.

Afin de permettre le respect des droits des personnes et la tenue des délais réglementaires de réponse aux demandes de droits, les Délégués à la protection des données doivent pouvoir recevoir, de la part de chaque sous-traitant d'un traitement de données à caractère personnel, un fichier contenant l'ensemble des données personnelles d'un demandeur dans un format structuré et lisible par un ordinateur.

4.2.2. Répartition du traitement des demandes de droit

Types de demandes de droits	Département	Académie	Collège
Demandes de droit effectuées par un membre du personnel académique, un parent d'élève ou un élève		Traite les demandes	Point de contact des personnes concernées
Demandes de droit effectuées par un agent de la collectivité	X		
Demande de droits effectuée directement auprès de l'Académie		X (sauf préemption du CD95 validée par les parties)	
Demande de droits effectuée directement auprès du CD95	X (sauf préemption de l'Académie validée par les parties)		

Article 5 - Notification des violations de données à caractère personnel auprès de la CNIL et communication auprès de la Personne concernée.

En cas de faille de sécurité impliquant des données personnelles, une chaîne d'alerte réactive doit être systématiquement mise en place.

5.1 Notification d'une faille de sécurité

La partie ou le sous-traitant de la partie ayant découvert une telle faille doit la notifier sous 12 heures maximum auprès des personnes suivantes :

- Le DPD de chaque entité
- Le RSSI de chaque entité le cas échéant

La notification prend la forme d'un formulaire standard de déclaration mis à la disposition de tous et contenant les catégories d'informations suivantes :

- Le service concerné et la localisation de l'hébergement
- La date début et fin de violation
- La nature violation
- Les catégories de données et de personnes
- Les mesures de sécurité prises ou envisagées.

Une mise à jour de l'ensemble de ces informations est effectuée et communiquée auprès des personnes indiquées toutes les 24 heures jusqu'à résolution de l'incident.

5.2 Cellule de crise et qualification de la faille

Une cellule de crise est convoquée dans les 24 heures à compter de la notification de la faille afin de décider de procéder ou non à sa notification auprès de l'autorité de contrôle.

Les différentes décisions possibles sont :

- La décision de non-notification en raison d'une absence de violation de données
- La décision de notification suite à la qualification d'une violation.

5.2.1 Décision de non-notification auprès de l'autorité de contrôle

Dans l'hypothèse d'une décision de non-notification, la documentation et l'argumentation de la décision sont conservées par les DPD dans leurs documentations respectives de conformité.

5.2.2 Décision de notification auprès de l'autorité de contrôle

En cas de notification, l'action incombe à la partie d'où la faille provient :

- Le DPD de l'Académie notifie la violation issue de l'action d'un membre du corps enseignant ou des familles.
- Le DPD du Département notifie la violation issue de l'action d'un agent du Département ou issue d'une faille de sécurité des outils mis à disposition par lui.

Chaque DPD conserve tout document utile relié à la notification effectuée dans l'espace commun aux Délégués à la protection des données ainsi que dans sa documentation de conformité

Article 6 - Sous-traitance d'un traitement sous responsabilité conjointe

6.1 Garanties suffisantes du sous-traitant d'un traitement de données à caractère personnel sous responsabilité conjointe.

Dans le cadre de la responsabilité conjointe, tout sous-traitant retenu doit présenter les garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles permettant d'assurer le respect de la réglementation applicable ainsi que les droits des personnes concernées.

6.2 Définition commune des exigences attendues du sous-traitant d'un traitement de données.

Dans l'hypothèse où la sous-traitance ne serait contractualisée qu'avec l'un des responsables conjoints de traitement, l'autre responsable de traitement sera associé à la définition des exigences requises dans les documents contractuels du marché.

Une grille d'évaluation des garanties en matière de protection des données personnelles est établie conjointement par les Délégués à la protection des données et devra nécessairement être prise en considération lors de l'évaluation des offres dans le cadre de prestations relevant du régime de la commande publique.

Si les règles de la commande publique le permettent, la partie non contractante sera associée à l'évaluation de la qualité de la réponse apportée par chaque candidat après anonymisation préalable des offres.

6.3 Communication entre la partie responsable conjointe non cocontractante et le sous-traitant de l'autre partie.

Une fois le sous-traitant choisi, le Département et l'Académie peuvent entrer directement en contact avec lui et lui faire part de demandes en lien avec les traitements de données sous responsabilité conjointe à condition que l'autre partie soit systématiquement associée à la demande.

Article 7 - Sécurité appliquée aux traitements

7.1 Engagement réciproque de respect des mesures de sécurité adéquates.

Chaque partie s'engage à respecter et faire respecter par ses personnels et ses sous-traitants toute mesure de sécurité visant notamment à empêcher que les données personnelles ne soient déformées, endommagées, perdues, détournées, corrompues, divulguées, transmises ou communiquées à des personnes non autorisées.

7.2 Engagement de conformité aux réglementations de sécurité en vigueur

La rectrice de l'académie de Versailles, en sa qualité de d'Autorité Qualifiée pour la SSI (AQSSI), est responsable de l'application de la Politique de Sécurité des Systèmes d'Information de l'Etat (PSSIE) et de la définition d'une politique de sécurité académique. Elle nomme un RSSI chargé de leur définition et de leur application dans les services académiques et l'ensemble des établissements scolaires.

Les parties et leurs sous-traitants s'assurent de la parfaite conformité et du respect de la politique de sécurité des systèmes d'information où transitent les données personnelles avec :

- les règles et bonnes pratiques, en application notamment du Référentiel Général de Sécurité version 2 (RGS) et ses évolutions ultérieures ;
- les recommandations de la Commission Nationale de l'Informatique et des Libertés (Cnil) et de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), en particulier de la conformité des règles de sécurité à la Politique de Sécurité des Systèmes d'Information de l'Etat (PSSIE).
- La politique de sécurité des systèmes d'information académique
- le référentiel Wi-fi de l'Education nationale et la loi n° 2015-136 du 9 février 2015 relative à la sobriété, à la transparence, à l'information et à la concertation en matière d'exposition aux ondes électromagnétiques.
- Le référentiel de l'Education nationale pour les services d'infrastructures d'EPL et d'écoles (CARINE)
- Le Cadre de référence de l'Education nationale pour l'Accès aux Ressources pédagogiques via un équipement Mobile (CARMO)

Article 8 - Analyse d'impact sur la protection des données et consultation préalable dans le cadre du respect par le responsable de traitement de ses obligations.

8.1 Analyse d'impact sur la protection des données.

Lorsqu'une analyse d'impact sur la protection des données s'avère obligatoire, l'Académie et le Conseil Départemental réalisent cette analyse en collaboration avec le Collège et l'ensemble des acteurs impliqués dans le traitement.

Une fois les avis des deux Délégués à la protection des données rendus, l'analyse d'impact est validée par les instances dédiées au sein de l'Académie et du Département.

8.2 Décision de consultation de la CNIL en cas de risque résiduel.

La décision de consulter la CNIL en cas de risque résiduel récurrent appartient à chacune des parties. Le cas échéant, la partie qui saisit la CNIL avertit l'autre par le biais de son Délégué à la protection des données de manière concomitante.

Article 9 - Tenue d'un registre des catégories d'activités de traitement.

L'Académie et le Département rédigent ensemble les fiches de traitements correspondant aux traitements communs aux trois parties.

Chaque partie conserve les fiches concernées dans leur propre registre de traitement.

Les parties tiennent seules un registre pour les activités de traitement dont elles sont seules responsables.

Article 10 - Localisation des données.

Les parties s'engagent à ce que les données personnelles traitées soient localisées de préférence sur le territoire de la France métropolitaine, et en toute hypothèse sur le territoire de l'Union européenne.

Article 11 - Documentation et audits

Chaque partie met à la disposition de l'autre sur simple demande la documentation nécessaire pour démontrer le respect de toutes ses obligations et pour permettre la réalisation d'audits.

L'audit pourra être effectué à tout moment, moyennant un préavis minimum de sept (7) jours, notifié par lettre recommandée avec accusé de réception par la partie sollicitant l'audit.

L'audit pourra être effectué par un auditeur professionnel ou par un collaborateur de la partie sollicitant l'audit.

Dans le cadre de son audit, la partie sollicitant l'audit pourra avoir accès à l'ensemble des éléments nécessaires ou utiles au bon accomplissement de son audit et l'autre partie s'engage à coopérer à cet audit, notamment en donnant à l'autre toute information pertinente.

Le rapport établi par la partie sollicitant l'audit sera remis à l'autre partie. Les frais d'audit seront pris en charge par la partie sollicitant l'audit.

Article 12 – Sensibilisation des Collèges à la protection des données

Pour accompagner le Collège dans la protection des données, l'Académie effectue régulièrement des actions de sensibilisation auprès des chefs d'établissement.

Dans le cas d'une sensibilisation concernant l'ENT, le Département coopère avec l'Académie pour la réalisation des supports nécessaires à cette sensibilisation.

Article 13 - Prise en considération de l'évolution du contexte ou de la réglementation en matière de protection des données à caractère personnel.

En cas d'évolution de la législation sur la protection des données à caractère personnel ou de création d'un nouveau traitement en cours d'exécution de la convention, les modifications éventuelles demandées l'une des parties, afin de se conformer aux règles nouvelles et de tenir compte des éventuelles nouvelles contraintes, donnent lieu à la révision de l'annexe par les parties à la convention.