

ACADÉMIE DE CRÉTEIL

POUR L'ÉCOLE  
DE LA CONFIANCE



L'académie  
s'engage

**académie  
Créteil**

RÉGION ACADÉMIQUE  
IL-DE-FRANCE

MINISTÈRE  
DE L'ÉDUCATION NATIONALE  
ET DE LA JEUNESSE

MINISTÈRE  
DE L'ENSEIGNEMENT SUPÉRIEUR,  
DE LA RECHERCHE  
ET DE L'INNOVATION

**R**ÈGLEMENT  
**RGPD**  
GÉNÉRAL  
DE PROTECTION  
**D**ES DONNÉES



# SOMMAIRE

ÉDITO .....	4
OBJECTIFS .....	5
ORGANISATION .....	6
GOUVERNANCE .....	7
ORGANIGRAMME .....	8
LES GRANDS PRINCIPES DU RGPD .....	9
RGPD : IDENTIFIER LES DONNÉES A CARACTÈRE PERSONNEL .....	10
DÉFINITIONS .....	11
RGPD : QUELQUES ARTICLES DE RÉFÉRENCE .....	12
ÉCHANGES DE DONNÉES ET STATISTIQUES .....	14
OUTILS PÉDAGOGIQUES ET D'ÉCHANGE (ENT, BLOGS, SOLUTIONS D'ÉDITEURS) .....	15
ACCOMPAGNEMENT DES EPLE ET ÉCOLES .....	17
RESSOURCES HUMAINES : QUELS ENJEUX POUR LA PROTECTION DES DONNÉES ? .....	20
DONNÉES SENSIBLES : QUEL CADRE POUR LEUR TRAITEMENT ? .....	22
QUELQUES SITUATIONS DE TRAITEMENT DE DONNÉES SENSIBLES .....	24
LA SÉCURITÉ DE L'INFORMATION, DOCTRINE ET DISPOSITIFS .....	25
FORMATION, SENSIBILISATION, COMMUNICATION .....	27
RESSOURCES .....	28
KIT DE RENTRÉE .....	29
INFORMATIONS PRATIQUES / CONTACTS .....	30

Depuis l'entrée en vigueur du Règlement Général de Protection des Données (RGPD), la communauté éducative est concernée par l'application de nouvelles mesures de traitement des données à caractère personnel.

Notre institution se trouve ainsi confrontée à un double défi : celui de la gestion conforme de données massives à caractère personnel, d'une part, et l'enseignement de savoirs et d'aptitudes relevant du bon usage du numérique, ainsi que l'acquisition par nos élèves de savoir-être favorisant l'émergence d'une citoyenneté numérique responsable, d'autre part.

Le plan académique de mise en œuvre du RGPD a pour objectif de répondre à ces enjeux en mettant en place une organisation et un programme à même d'étudier l'impact du RGPD dans les différents domaines de l'activité administrative et pédagogique et d'y apporter des solutions adaptées, avec le concours du délégué académique à la Protection des données (DPD).

Je salue l'engagement des équipes pédagogiques et administratives qui se sont mobilisées afin d'élaborer des outils pouvant garantir la conformité des traitements effectués dans les établissements scolaires et les services académiques.

La rentrée scolaire sera marquée par le déploiement généralisé du programme académique de protection des données. Celui-ci concerne les données à caractère personnel des enseignants, des agents, des élèves et leurs représentants légaux.

Je reste attentif à l'application des dispositions réglementaires ainsi que des mesures techniques et organisationnelles prises par les responsables de traitement, visant à garantir un niveau optimal de protection des données à caractère personnel de toute la communauté éducative.

Je vous encourage vivement à mettre en œuvre les solutions élaborées par l'académie ainsi que les ressources nationales de mise en conformité des traitements de données.

La protection et la valorisation de la donnée éducative participent de l'École de la confiance en résonance avec la confiance dans une société numérique.



---

**Daniel Auverlot**

Recteur de l'académie de Créteil  
Chancelier des universités

# OBJECTIFS

**L'**académie s'est engagée dans une démarche de mise en œuvre du Règlement Général de Protection des Données (RGPD), dans le but de mettre en conformité l'ensemble des traitements effectués dans les services académiques et les établissements scolaires.

**L'un des objectifs pour la rentrée scolaire est de mettre à disposition des acteurs de terrain un kit RGPD composé de livrables élaborés grâce à la contribution active des groupes de travail qui ont réuni des personnes ressources du rectorat, des DSDEN et des établissements scolaires.**

Ces livrables sont autant de solutions destinées aux corps d'inspection, aux chefs d'établissement, aux directeurs d'école, aux services académiques et aux usagers de l'académie. Ils constituent les premières briques du socle académique de conformité des traitements.

Le parcours de la conformité au RGPD sera jalonné d'autres étapes tout au long des années scolaires à venir :

- la tenue des registres de traitement des EPLE et Écoles ;
- la sensibilisation et la formation des enseignants et agents au RGPD ;
- la sécurisation des traitements et des circuits d'échanges de données ;
- la revue des conventions de partenariat d'échange de données ;
- l'amélioration de la prise en charge de l'exercice des droits des personnes ;
- l'instauration durable d'une culture académique de protection des données à caractère personnel.

D'ores et déjà, des avancées notables marquent l'année scolaire 2019-2020, notamment le kit de rentrée composé d'outils et de solutions d'aide à la conformité des traitements, accessible en ligne sur le site de diffusion académique ADN (<https://adn.ac-creteil.fr>). Des initiatives de renforcement de la sécurité de données sont également prises par le chiffrement des postes de travail vulnérables (terminaux nomades) et des circuits d'échange de données médicales.

Ce livret RGPD résume les mesures adoptées et fixe le cadre d'actions à entreprendre pour mieux protéger les données à caractère personnel des usagers du système d'information administrative, financière et pédagogique de l'académie.

Je vous invite à relever ensemble le défi de la conformité au RGPD.



**Sylvie Thirard**

Secrétaire générale d'académie

# ORGANISATION

Le RGPD définit le responsable de traitement (RT) comme la personne physique ou morale qui détermine les finalités et les moyens du traitement des données à caractère personnel.

Pour l'éducation nationale, on distingue 4 responsables de traitement (RT) :

- **le ministre et les directions nationales** au titre des traitements liés aux applications mises en œuvre par les directions nationales (Dgesco, DNE, Daf, DEEP, Delcom, etc.) ;
- **le recteur et les directions métiers académiques** au titre des traitements liés aux applications et services académiques (Dane, Damesop, Dap, DEEP, Dimmog, DPE, DSI, Papp, SAIO, etc.) ;
- **le Dasen** par délégation du recteur au titre des traitements déterminés en DSDEN et dans les écoles ;
- **le chef d'établissement** pour tous traitements décidés en EPLE à l'exclusion des traitements induits par les applications nationales et académiques.

Le périmètre de responsabilité de chacun est déterminé par le traitement de données dont il a la responsabilité directe.

En vertu de l'article 37 du RGPD, Monsieur le recteur a désigné **M. Ousmane Sow** comme délégué académique à la Protection des données (DPD), chargé d'orchestrer la mise en œuvre du RGPD auprès de tous les responsables de traitement de l'académie. Le DPD ou DPO (Data Protection Officer) est agréé par la Commission nationale de l'Informatique et des Libertés (CNIL), sous le numéro : DPO-23352.

L'organisation académique de mise en œuvre du RGPD reflète la triple dimension de responsabilité de traitement. Elle est placée sous l'autorité administrative de **M<sup>me</sup> Sandrine Connan**, correspondante RGPD de l'académie, Secrétaire générale adjointe, directrice de la modernisation, de l'informatique et de l'immobilier.

Les directeurs départementaux (Dasen) ont également désigné un correspondant départemental chargé de la mise en œuvre géographique du RGPD auprès des EPLE et Écoles, aidé en cela par une équipe de référents départementaux à la Protection des données, au niveau des premier et second degrés (RPD des 1<sup>er</sup> et 2<sup>d</sup> degrés).

Les secrétaires généraux de DSDEN ainsi que les directeurs métiers du rectorat ont désigné chacun en ce qui le concerne un référent métier à la Protection des données (RPD Métiers), en charge de la conformité des traitements de leur structure.

Le délégué académique à la Protection des données pilote le programme académique de mise en œuvre du RGPD en lien avec la CNIL.

# GOVERNANCE

La mise en œuvre du Règlement Général de Protection des Données (RGPD) nécessite des mesures techniques et organisationnelles aptes à garantir la conformité des traitements à l'échelle de l'académie.

Les instances de gouvernance académique permettent d'administrer cette mise en œuvre tant au niveau décisionnel qu'opérationnel :

- un comité de pilotage – le Copil, présidé par M. le recteur ;
- un comité de suivi – le Cosui, placé sous l'égide du Secrétariat général d'académie ;
- un comité opérationnel – le Comop, piloté par le délégué académique à la Protection des données (DPD) ;
- des cadres de concertation et d'échanges (réunions des corps d'inspection, CIEN, Groupe Blanchet, réunions des cadres, réunions des chefs d'établissement).

## LE COMITÉ DE PILOTAGE (COPIL)

Il est composé des décideurs institutionnels de l'académie : le recteur, la secrétaire générale d'académie, les Dasen, les doyens des corps d'inspection, la correspondante académique RGPD.

Son rôle :

- définir les objectifs stratégiques du RGPD ;
- nommer les responsables de sa mise en œuvre ;
- assurer le sponsoring du projet.

## LE COMITÉ DE SUIVI (COSUI)

Le comité de suivi est l'instance technique de conduite, de suivi et d'évaluation du programme académique de mise en conformité au RGPD.

Il est composé de responsables de directions métiers du rectorat et des DSDEN ayant un fort volume de traitements de données à caractère personnel (DCP), mais également du RSSI et du service juridique de l'académie.

Sous l'égide du Secrétariat général d'académie, son rôle consiste à valider le plan d'actions du DPD, déterminer les acteurs et définir les modalités ainsi que le calendrier de mise en œuvre.

## LE COMITÉ OPÉRATIONNEL (COMOP)

Le Comop est l'instance d'animation et de mise en œuvre opérationnelle des programmes académiques de mise en conformité au RGPD, auprès des établissements scolaires et des structures académiques. Il est essentiellement composé d'opérationnels désignés comme référents à la Protection des données (RPD) du domaine géographique ou fonctionnel auquel ils sont rattachés (rectorat, DSDEN, structures ou domaines métiers). Ses membres sont des acteurs agissant directement auprès des responsables de traitement (RT) afin de les accompagner dans la mise en œuvre du RGPD.

# ORGANIGRAMME

NIVEAU  
POLITIQUE

NIVEAU  
MANAGÉRIAL

NIVEAU  
OPÉRATIONNEL

**LE RECTEUR**

Maîtrise d'ouvrage académique du RGPD

**SG ACADEMIE**

Maîtrise d'œuvre académique du RGPD

**DASEN 94**

Garante du RGPD  
dans le 94

*Secrétaire  
général*  
**ANTOINE  
KAKOUSKY**

Correspondant  
départemental  
RGPD

*RPD  
1<sup>er</sup> degré 94*  
**SÉBASTIEN  
MOUNIE**

Référent  
Protection  
des données 94  
Écoles

*RPD  
2<sup>d</sup> degré 94*  
**CAROLE  
DUBARLE**

Référent  
Protection  
des données 94  
EPLÉ

**DASEN 93**

Garant du RGPD  
dans le 93

*DAASEN 93*  
**CATHERINE  
ALBARIC-  
DELPECH**

Correspondant  
départemental  
RGPD

*RPD  
1<sup>er</sup> degré 93*  
**BRIGITTE  
VENTRE**

Référent  
Protection  
des données 93  
Écoles

*RPD  
2<sup>d</sup> degré 93*  
**FRÉDÉRIC  
BROUZES**

Référent  
Protection  
des données 93  
EPLÉ

**DASEN 77**

Garante du RGPD  
dans le 77

*DAASEN 77*  
**FRANCK  
THENARD-  
DUVIVIER**

Correspondant  
départemental  
RGPD

*RPD  
1<sup>er</sup> degré 77*  
**JEAN-  
CHARLES  
POCHET**

Référent  
Protection  
des données 77  
Écoles

*RPD  
2<sup>d</sup> degré 77*  
**BENOÎT  
CHASTENET**

Référent  
Protection  
des données 77  
EPLÉ

**SGA - M2I**

Correspondante  
académique du RGPD

*DPD ou DPO  
Académie*  
**OUSMANE  
SOW**

Délégué académique  
à la Protection  
des données

*RPD métiers*  
**STRUCTURES  
RECTORAT  
& DSDEN**



# LES GRANDS PRINCIPES DU RGPD

**L**e règlement européen de protection des données RGPD (UE) 2016/679 régit le traitement des données à caractère personnel. C'est une réforme majeure qui harmonise le droit européen et s'applique dans tous les états de l'Union depuis le 25 mai 2018. Son but est de garantir la libre circulation des données, protéger la vie privée des personnes physiques à l'égard du traitement des données les concernant et rendre aux citoyens le contrôle de leurs données contre tout usage non autorisé.

Une « donnée à caractère personnel – DCP » se définit comme toute information se rapportant à une personne physique identifiée ou identifiable par tout procédé d'identification ou de recoupement.

Tous les organismes publics et privés sont tenus de respecter les dispositions du RGPD, constituées de principes juridiques fondamentaux et de mesures de sécurité visant à protéger les données des personnes physiques.

## **Ces principes fondamentaux juridiques se déclinent en 173 considérants, 91 articles et 56 renvois qui constituent la substance du Règlement :**

- principe de licéité (de ce qui est légal) ;
- principe de transparence et de loyauté ;
- principe de finalité ;
- principe de proportionnalité ;
- principe d'intégrité et de confidentialité ;
- principe de responsabilité (accountability).

## **Le RGPD consacre également des droits accrus aux personnes concernées :**

- le droit d'accès aux DCP qui concernent chaque personne ;
- le droit à la rectification ;
- le droit à l'effacement (droit à l'oubli) ;
- le droit à la limitation aux données juste nécessaires au traitement ;
- le droit d'opposition au traitement de ces données personnelles ;
- le droit de réclamation auprès de la CNIL ;
- le droit d'action collective (class action).

Le RGPD porte des changements majeurs du droit, en particulier le passage d'un régime administratif de déclaration préalable auprès de la CNIL à un régime de conformité globale désormais dévolue à chaque responsable de traitement.

## IDENTIFIER LES DONNÉES À CARACTÈRE PERSONNEL



### LE TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL

Traiter les données à caractère personnel au sens du RGPD, c'est :

COLLECTER /// ENREGISTRER /// CONSULTER /// MODIFIER /// ORGANISER ///  
LIMITER /// STRUCTURER /// UTILISER /// EXTRAIRE /// TRANSMETTRE ///  
METTRE À DISPOSITION /// PUBLIER /// EFFACER /// INTERCONNECTER ///

### 4.1. DONNÉES À CARACTÈRE PERSONNEL (DCP)

Toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée « personne concernée »). Est réputée être une « personne physique identifiable », une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.

### 4.2. TRAITEMENT

Toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, 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, la limitation, l'effacement ou la destruction.

### 4.7. RESPONSABLE DU TRAITEMENT (RT)

Personne physique ou morale, autorité publique, service ou autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement ; lorsque

les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre.

### 4.8. SOUS-TRAITANT (ST)

Personne physique ou morale, autorité publique, service ou autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement.

### 4.11. CONSENTEMENT DE LA PERSONNE CONCERNÉE

Toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement.

### 4.17. REPRÉSENTANT

Personne physique ou morale établie dans l'Union, désignée par le responsable du traitement ou le sous-traitant par écrit, en vertu de l'article 27, qui les représente en ce qui concerne leurs obligations respectives en vertu du présent règlement.

### ARTICLE 5

#### PRINCIPES RELATIFS AU TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL

##### 1. Les données à caractère personnel doivent être :

**a**/// traitées de manière licite, loyale et transparente au regard de la personne concernée (licéité, loyauté, transparence) ;

**b**/// collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités ; le traitement ultérieur à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques n'est pas considéré, conformément à l'article 89, paragraphe 1, comme incompatible avec les finalités initiales ;

**c**/// adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données) ;

**d**/// exactes et, si nécessaire, tenues à jour ; toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder (exactitude) ;

**e**/// conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées ;

**f**/// traitées de façon à garantir une sécurité appropriée, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle.

**2. Le responsable du traitement est responsable du respect du paragraphe 1 et est en mesure de démontrer que celui-ci est respecté (principe de responsabilité).**

## ARTICLE 6

### LICÉITÉ DU TRAITEMENT

**1. Le traitement n'est licite que si, et dans la mesure où, au moins une des conditions suivantes est remplie :**

**a** /// la personne concernée a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques ;

**b** /// le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci ;

**c** /// le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis ;

**d** /// le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique ;

**e** /// le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement ;

**f** /// le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant.

Le point **f** /// du premier alinéa ne s'applique pas au traitement effectué par les autorités publiques dans l'exécution de leurs missions.

**2. Les États membres peuvent maintenir ou introduire des dispositions plus spécifiques pour adapter l'application des règles du présent règlement pour ce qui est du traitement dans le but de respecter le paragraphe 1, points **c** /// et **e** ///, en déterminant plus précisément les exigences spécifiques applicables au traitement.**

# ÉCHANGES DE DONNÉES ET STATISTIQUES

Le RGPD considère (art. 4.2) que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'échange, le partage, la mise à disposition, l'extraction, la consultation ou l'utilisation sont autant de traitements quand ils s'appliquent à des données à caractère personnel. On désigne par « responsable de traitement » la personne physique ou morale qui détermine les finalités et les moyens du traitement.

Lorsque deux responsables de traitement partagent des données à caractère personnel, il y a lieu de s'interroger sur les termes de l'échange au regard de la légitimité de chacun à capter les données.

L'article 6.1 du RGPD stipule qu'un traitement n'est licite que si et dans la mesure où il est justifié par une base légale. Or, la base légale d'un traitement ne peut être conférée que par le contrat, le consentement explicite, libre et éclairé donné par la personne concernée ou par la loi (traitement nécessaire au respect d'une obligation légale ou nécessaire à l'exercice d'une mission d'intérêt public).

Par conséquent, la captation de données à caractère personnel est subordonnée à une base légale, nonobstant les finalités du traitement.

Ce sont donc les termes de cet échange qui engagent la responsabilité juridique des acteurs d'où découle le statut des parties prenantes de l'échange, selon qu'ils sont en coresponsabilité ou dans une relation de responsable de traitement à sous-traitant, au sens du RGPD et non de la loi N°75-1334 de 1975 sur le commerce. Cette situation se présente notamment dans le partenariat avec les collectivités territoriales.

En attendant une jurisprudence en la matière ou un code de conduite, il appartiendra à chaque responsable de traitement au moment du partage de données à caractère personnel, dûment collectées ou légalement reçues, d'apprécier la pertinence du véhicule juridique qui permet l'échange.

**En tout état de cause, un protocole d'échange est indispensable afin de légitimer ce partage qui peut être matérialisé par une convention, notamment avec les collectivités territoriales.**

S'agissant des statistiques, elles ne sont pas soumises aux dispositions du RGPD lorsqu'elles ne mettent pas en œuvre des données à caractère personnel. À noter que l'anonymisation irréversible de DCP exonère des dispositions du RGPD.

## PRÉCONISATIONS

- Toutes les conventions de partenariat mettant en œuvre des données à caractère personnel doivent être revues à l'aune du RGPD.
- Il n'y a pas de convention à établir entre partenaires endogènes concourant à la même finalité. En revanche les destinataires des DCP doivent être mentionnés dans le registre de traitement.

# OUTILS PÉDAGOGIQUES ET D'ÉCHANGE

## (ENT, BLOGS, SOLUTIONS D'ÉDITEURS)

**L**es outils et solutions numériques sont de plus en plus utilisés dans l'activité pédagogique comme moyen d'acquisition de compétences et d'aptitudes ou comme vecteurs de communication servant à établir des liens – hors de la classe – avec les élèves ou leurs familles (blog, applet, réseaux sociaux).

Ces outils font souvent appel aux données à caractère personnel (DCP) d'enseignants, d'élèves ou de parents d'élèves, qu'il s'agisse d'identifiants de connexion ou de données stockées, échangées ou mises à disposition (appréciations, évaluations, contacts, etc.).

Depuis le 25 mai 2018, date d'entrée en vigueur du RGPD, les initiateurs de ces traitements (chef d'établissement, enseignants, intervenants) doivent mettre ces opérations en conformité avec le Règlement.

Il faut noter que les prérequis de conformité au RGPD ne sont pas équivalents selon qu'on agit dans le cadre d'une mission de service public d'enseignement ou dans un autre contexte. En effet, dans une mission de service public d'éducation ou dans l'exercice de service du numérique pour l'éducation, le traitement opéré est réputé licite de par la loi (RGPD, art. 6.1.e et 6.2 qui renvoient au Code de l'Éducation).

Autrement dit, l'utilisation hors cadre scolaire de logiciel en ligne relevant de la société de l'information est impérativement soumise au consentement des élèves de plus de 15 ans ou de leurs parents quand ils sont mineurs.

De même qu'il est important, selon les préconisations nationales, de faire spécifier dans les contrats passés entre les établissements scolaires et les éditeurs de logiciels de vie scolaire, d'emploi du temps ou d'ENT, que les données doivent être stockées par les hébergeurs sous forme cryptée, les responsables de traitement étant seuls habilités à posséder la clef de décryptage.

Au niveau des établissements scolaires, les responsables de traitement sont : le chef d'établissement pour tous traitements effectués en EPLE et le DASEN par délégation du recteur au titre des traitements déterminés en DSDEN ou dans les écoles, à l'exclusion des traitements induits par les applications nationales et académiques;

Pour autant, l'enseignant qui met en œuvre ces outils ou solutions n'est pas exonéré de responsabilité puisque qu'il est considéré par le RGPD comme le « Représentant » du responsable de traitement (chef d'établissement). À ce titre il doit inscrire ledit traitement dans le registre de l'EPLE, le cas échéant, ou dans celui de la DSDEN, auprès de l'IEC de circonscription, pour ce qui concerne les professeurs des écoles.

La démarche de mise en conformité d'outils et solutions numériques est abordée dans les préconisations du chapitre « Accompagnement des EPLE et Écoles ». En outre, une notice de recommandations de bonnes pratiques et d'outils gratuits plus respectueux du RGPD est disponible dans les livrables (chapitre Kit de rentrée).

---



# ACCOMPAGNEMENT DES EPLE & ÉCOLES

Un an après l'entrée en vigueur du RGPD, très peu d'outils ou de solutions numériques satisfont aux critères de conformité au RGPD. Même si beaucoup d'éditeurs s'engagent ou proclament leur compatibilité au Règlement, la conformité annoncée n'est souvent qu'incantatoire ou partielle. Pour autant, il n'est pas réaliste de renoncer aux usages.

Mais on ne peut non plus recommander l'utilisation indifférenciée de solutions et outils numériques qui mettent en œuvre des traitements de données à caractère personnel d'élèves, parents, et de personnels. Au-delà des risques de non-conformité encourus, la probabilité de contrôle de la CNIL est accentuée par la facilité de saisine concédée par le RGPD aux personnes concernées, phénomène à corrélérer avec les éventuels risques de surenchère procédurière.

L'espace scolaire compte une population sensible que le RGPD qualifie de vulnérable (personnes mineures), c'est aussi un espace relationnel avec les parents d'élèves, leurs représentants et divers partenaires dont les données personnelles sont traitées.

Dès lors, il convient d'être particulièrement attentif à l'application des dispositions du RGPD en milieu scolaire afin qu'elle ne constitue pas un vecteur de réclamations récurrentes ou d'expression de rapport de force inapproprié.

Pour mener à bien l'accompagnement des EPLE et Écoles, les directeurs départementaux (Dasen) ont désigné, chacun en ce qui le concerne, un correspondant départemental RGPD et deux référents à la Protection des données (RPD) ; un pour le 1<sup>er</sup> degré et un pour le 2<sup>d</sup> degré.

## PRÉCONISATIONS

Voici quelques critères de compatibilité au RGPD qui permettent de discriminer les outils et solutions du marché :

- privilégier les modalités d'accès par des identifiants spécifiques plutôt qu'hérités de plateformes qui présentent un risque de cession implicite de vos données ;
- s'assurer du lieu de stockage des données (de préférence interne à l'institution ou auprès d'hébergeurs européens soumis aux garanties du RGPD) ;
- vérifier l'existence d'un contrat de service dans l'acquisition de l'outil (engagements de fiabilité, attention au gratuit, il a forcément un coût caché) ;
- évaluer le niveau de sécurité des accès aux données (l'existence d'une norme, RGS, mesure d'authentification forte, procédure de sauvegarde) ;

- vérifier que les CGU sont explicites et pertinentes avec des garanties de maîtrise des données ;
- en cas de gratuité, examiner le modèle économique (non intrusif et non captif) ;
- s'interroger sur les réponses à l'exercice des droits ;
- vérifier la présence de publicité pouvant entraîner un défaut de neutralité commerciale ;
- rechercher les engagements RGPD de l'éditeur ;
- apprécier les fonctionnalités pédagogiques au regard des finalités de l'outil ;

---

**L**es enjeux de l'accompagnement des EPLE & Écoles ne se limitent pas au choix de bons outils et services numériques. Cette étape est cependant nécessaire à la conformité des traitements mis en œuvre, mais d'autres critères sont aussi à prendre en compte :

- des mesures techniques telles que la sécurisation des lieux de stockage des données numériques tout autant que des supports en papier (fermeture des lieux de stockage, destruction mécanique de documents inusités, règles de sécurisation des postes de travail au-delà des verrous digitaux, etc.) ;
- la sensibilisation et la responsabilisation des acteurs notamment par la signature d'une charte de bon usage de l'information (confidentialité, discrétion, vigilance) ;
- la détermination du circuit de l'information, son mode de communication, l'identification des failles humaines de protection des données ;
- la veille sur le cycle de vie des données et la mise en place de processus de destruction ou d'archivage quand la durée de conservation nécessaire est atteinte ;
- la tenue d'un registre des habilitations et son maintien à jour (beaucoup de personnels changent de fonction ou quittent l'établissement en conservant des accès et habilitations sur des données).



Ces mesures de veille et de sécurisation des données sont à coupler avec le second pilier du RGPD, à savoir les principes juridiques fondamentaux et les droits des personnes. C'est dans ce domaine qu'on compte les changements réglementaires les plus significatifs :

- les personnes dont les DCP sont traitées doivent être informées de ces données ainsi que des finalités des traitements (principe de transparence, de loyauté et de finalité).

**Un formulaire d'information aux familles a été élaboré à cet effet pour les EPLE et Écoles, disponible en ligne dans le kit de rentrée (sur ADN) ;**

- chaque responsable de traitement doit tenir un registre de tous ses traitements (RGPD, art. 30) ; ce registre peut être mis à disposition des personnes concernées à leur demande (exercice du droit d'accès, art. 15) ;
- les échanges de données entre responsables de traitement doivent faire l'objet d'une convention où est rappelée la responsabilité de chaque partie dans le respect des dispositions du RGPD ;
- chaque (RT) responsable de traitement (recteur, DASEN, chef d'établissement) doit désigner un délégué à la Protection des données (DPD). Pour Créteil, le recteur a désigné un seul DPD pour tous les RT de l'académie, conformément au schéma d'organisation préconisé par le ministère. Le DPD académique est agréé par la CNIL qui est l'autorité nationale indépendante de contrôle de la mise en œuvre du RGPD.

# RESSOURCES HUMAINES

## QUELS ENJEUX POUR LA PROTECTION DES DONNÉES ?

La gestion des ressources humaines est le domaine par excellence de traitement de données à caractère personnel. C'est également le secteur qui peut être force d'innovation dans les règles de traitement des données, à condition de relever certains défis organisationnels :

- être en capacité de répondre à de potentielles demandes massives d'exercice des droits des personnes concernées ;
- gérer le consentement au regard de sa révocabilité et ses conséquences en termes de rupture d'égalité ;
- organiser la destruction ou l'archivage des données atteignant leur limite de conservation ;
- administrer l'échange de données avec les partenaires en conformité avec la loi.

Ces problématiques inhérentes au RGPD se présentent également dans toutes les académies. Aussi, une réponse nationale visant à adapter les systèmes d'information académiques au nouveau cadre juridique des traitements est souhaitable.

La réponse efficiente à l'exercice des droits des personnes est assurément un enjeu de réussite de la mise en œuvre du RGPD dans les académies. La loi informatique et Libertés de 1978 accordait des droits substantiels aux personnes dont les données sont traitées. Non seulement ces droits ont été reconduits et renforcés par le RGPD mais de nouveaux droits viennent s'y ajouter.

### LES DROITS DES PERSONNES

- **Transparence (loyauté, finalité)**

#### DROITS RENFORCÉS

- **Information**
- **Accès**
- **Rectification**
- **Opposition**
- **Réclamation (auprès de la CNIL)**

#### NOUVEAUX DROITS

- **Oubli (effacement)**
- **Limitation du traitement**
- **Portabilité<sup>1</sup>**
- **Retrait de consentement**
- **Actions de groupe**

<sup>1</sup> L'article 20.3 du RGPD exonère du droit de portabilité les organismes publics dont le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement.

---

## QUELQUES CAS PARTICULIERS

Au-delà des sujets structurels de prise en compte de l'exercice des droits des personnes, les directions métiers de gestion de ressources humaines sont également confrontées à la transmission spontanée de données sensibles qui ne peuvent être traitées sans consentement préalable, libre, explicite et éclairé des personnes concernées.

Le traitement des congés pour fête religieuse pose question quand on ne peut traiter les données concernant les convictions religieuses d'un agent. Il en est de même en établissement scolaire quand il faut traiter le régime alimentaire afin de proposer un repas de substitution car le RGPD interdit de traiter les mentions révélatrices d'allergies ou de convictions religieuses entraînant des choix alimentaires, toutes données sensibles dont le traitement est interdit.

D'autres situations individuelles sont à prendre en compte, notamment le cas des conjoints qui, dans la constitution de leur dossier administratif, donnent à connaître et à traiter des informations révélant leurs problèmes de santé ou d'orientation sexuelle (donnée sensible), par exemple le cas du conjoint de même genre.

Sur tous ces sujets et en attendant l'adoption d'un code de conduite du ministère, les réponses académiques, même transitoires, devront être harmonisées.

---

## SÉCURISATION ET DURÉE DE CONSERVATION DES DONNÉES

Des mesures techniques et organisationnelles telles que la sauvegarde des données sur des supports fiables et la sécurisation des lieux de stockage des données numériques ou conservées sur des supports en papier sont autant de critères de conformité des traitements :

- fermeture à clé des lieux de stockage des dossiers papier ;
- destruction mécanique de documents inusités (broyeurs) ;
- mesures de sécurisation des postes de travail au-delà des verrous digitaux ;
- chiffrement des postes de travail relativement exposés (terminaux nomades, données sensibles) ;
- règles partagées de conservation des données (classification par catégorie et par durée de rétention) ;
- cartographie des données ;
- tenue à jour du registre des traitements.

# DONNÉES SENSIBLES

## QUEL CADRE POUR LEUR TRAITEMENT ?

Parmi les données à caractère personnel (DCP), on distingue deux catégories : **les données courantes** permettant l'identification directe ou indirecte d'une personne physique et **les données sensibles** révélant une situation particulière de la personne. Pour cette dernière catégorie de données que le RGPD reconnaît comme sensibles, le traitement sous quelque forme que ce soit est formellement interdit.

### QUELLES SONT LES DONNÉES SENSIBLES ?

- Les opinions politiques, les convictions religieuses ou philosophiques
- l'appartenance syndicale
- l'origine raciale ou ethnique
- le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique
- les données concernant la santé
- les données concernant la vie sexuelle ou l'orientation sexuelle

Il arrive que le traitement de données sensibles soit nécessaire à la gestion ou l'étude des droits de la personne, dans ces cas il y a lieu d'examiner les exceptions prévues par la loi (consentement, nécessité vitale, etc.), article 9.2 du RGPD.

Le responsable de traitement doit prendre des mesures techniques et organisationnelles permettant d'encadrer le traitement de données sensibles conformément au Règlement.

A contrario, certaines situations ou données peuvent être ressenties comme sensibles sans pour autant être des données sensibles au sens du RGPD. C'est par exemple le cas des données financières ou plus généralement la donnée éducative qui demeure une question sensible, sans être une donnée sensible.

## PRÉCONISATIONS

Voici quelques situations qui appellent de nouvelles réponses :

- il est nécessaire de repenser les pratiques de gestion afin de les rendre conformes au traitement des données sensibles (cas des champs autres dans les applications) ;
- les professionnels de santé sont les seuls habilités à traiter des données de santé sans consentement préalable ;
- les personnels non couverts par le secret médical doivent recourir au consentement de la personne concernée pour traiter des données médicales, biologiques ou génétiques ;
- un formulaire de recueil de consentement doit être disponible dans tous les services de gestion afin de prévenir le traitement de données sensibles, car le consentement ne peut être implicite, de plus le RT doit être en mesure d'en apporter la preuve matérielle ;
- l'article 9.2 du RGPD, dans certaines circonstances, autorise les organismes publics à traiter les données sensibles. Il y a lieu, dans ces cas, de faire la balance entre le risque encouru et la nécessité de traiter sans consentement.

# QUELQUES SITUATIONS DE TRAITEMENT DE DONNÉES SENSIBLES

## LE TRAITEMENT DES DONNÉES BIOMÉTRIQUES

La biométrie est un procédé technique spécifique par lequel des caractéristiques physiques, physiologiques ou comportementales permettent d'identifier ou de confirmer l'identification unique d'une personne physique. Ce type de données tombe sous le coup des données sensibles dont le traitement est interdit (art. 9.1), sauf en cas de consentement libre et éclairé des personnes concernées.

Le contrôle des accès à la cantine par un système d'identification du contour de la main ou le recueil de données biométriques associées à des performances sportives relèvent du traitement biométrique.

Cinq conditions permettent de garantir la conformité d'un traitement biométrique en milieu scolaire :

- délibération du CA ou avis du Conseil d'école ;
- **étude d'impact** approuvée par la CNIL (analyse de risques sur les droits et libertés des personnes et mesures de maîtrise) ;
- information des personnes concernées sur le dispositif et les mesures de sécurité et de conservation des données (organisation, accès, durée) ;
- **recueil obligatoire de consentement** des intéressés ou de leurs représentants ;
- inscription du traitement dans le registre de l'établissement.

Une fiche CNIL ainsi qu'une FAQ sur la vidéosurveillance sont disponibles sur ADN : <https://adn.ac-creteil.fr> – Rubrique RGPD

## LA VIDÉOSURVEILLANCE

La mise en place d'un dispositif de vidéosurveillance est un traitement au sens du RGPD, dès lors qu'il s'agit de capter, d'enregistrer et de conserver des images permettant d'identifier des personnes physiques.

Ce dispositif est très encadré et les mesures de conformité dépendent du contexte d'utilisation (surveillance de locaux sans présence humaine, surveillance de lieux privés ou publics en présence d'individus ou des lieux de vie ou de passage).

En EPLE, la vidéosurveillance relève de la responsabilité du chef d'établissement. En École, c'est la responsabilité conjointe du DASEN et du maire qui est requise, sauf si le système s'opère hors présence d'élèves, dans ce cas le maire est seul responsable de traitement.

Si le dispositif se limite à surveiller les lieux d'accès ou de passage d'un établissement scolaire, sans captation d'images des lieux de vie (salle de classe, cantine, préau, etc.), le consentement n'est pas nécessaire, mais certaines précautions sont à prendre :

- délibération du CA ou avis du Conseil d'école ;
- nécessité d'une étude d'impact ;
- information préalable des personnes concernées (personnels, élèves et parents d'élèves) sur la finalité du traitement et les conditions de sécurité ;
- inscription de ce traitement dans le registre de l'établissement indiquant les destinataires des enregistrements et les personnes habilitées à les visionner.



# LA SÉCURITÉ DE L'INFORMATION, DOCTRINE ET DISPOSITIFS

**L**a sécurité des données est le second pilier du RGPD à côté des principes fondamentaux juridiques et des droits des personnes concernées par les données à caractère personnel (DCP). C'est également un des aspects les plus structurels de la conformité, tant la mise en œuvre de la sécurité des données est liée à l'environnement technique dépendant des infrastructures.

Mettre en place des mesures de sécurité des DCP conduit à s'interroger sur la sécurité des données en général, et donc à examiner la pertinence des dispositifs et des stratégies de sécurité du système d'information déjà en place.

L'enjeu de sécurité des données consiste à les préserver contre toute action pouvant entraîner de manière accidentelle ou illicite, la perte, l'altération, l'accès non autorisé ou la divulgation, que ces données soient conservées, traitées ou transmises.

Dans un contexte de généralisation de la micro-informatique, l'automatisation des tâches administratives et des processus métiers, mais également l'appropriation des réseaux (internet, réseaux sociaux) et la facilité d'accès à de multiples sources d'information, notamment au travers de terminaux nomades, font de l'individu un maillon incontournable de la chaîne de sécurité des systèmes d'information.

Dans le même temps, les nouvelles techniques de traitement des données massives (Big data), le recours insidieux à l'analyse prédictive de données personnelles (le profilage), mais aussi le développement de l'intelligence artificielle, tous ces modes de traitement des données soulignent avec acuité la nécessité de protéger les données personnelles comme gage de confiance dans la société numérique.

## PRÉCONISATIONS

Quelques mesures de sécurité à l'initiative du RSSI :

- procéder au chiffrement de certains postes de travail particulièrement exposés (terminaux nomades, circuits d'échanges médicaux, etc.) ;
- faire signer aux administrateurs systèmes, réseaux et systèmes d'information de l'académie une charte de confidentialité ;
- porter à la connaissance des collaborateurs la charte sur l'usage des technologies de l'information et de la communication ;
- vulgariser le guide juridique de l'utilisateur du système d'information de l'académie de Créteil.

## MESURES TECHNIQUES ET ORGANISATIONNELLES

Les mesures techniques et organisationnelles nécessaires pour garantir le niveau adéquat de protection des données ne peuvent s'apprécier au regard de la seule obligation de moyens mis en œuvre par le responsable de traitement (RT), car il s'agit de déployer des moyens suffisants, en qualité et adaptés à chaque situation de risque encouru.

La sécurité des données est une compétence de l'opérateur du système d'information. Les processus métiers des intervenants informatiques et réseaux embarquent nativement la dimension sécurité du système d'information.

De plus, le RSSI de l'académie a pour mission de veiller à la pertinence des processus et protocoles de sécurité et à leur efficacité. Aussi les préconisations académiques sont-elles importantes, car on ne sécurise bien que ce que l'on maîtrise. Pour autant, le RGPD reconnaît le responsable de traitement comme garant de la sécurité des traitements qui lui incombent. Il lui revient donc de s'assurer auprès de tous les intervenants que tout est mis en œuvre pour garantir l'intégrité des données.



La sécurité des données s'analyse en fonction de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement, ainsi que des risques sur les droits et libertés des personnes physiques. Ces considérations, dans la mesure où elles sont variables, ne permettent pas de préconiser un niveau de sécurité type. Toutefois quelques mesures réglementaires sont de rigueur :

- en cas de violation de données à caractère personnel, le responsable du traitement notifie la violation à l'autorité de contrôle qui est compétente, conformément à l'article 55, dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance, à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques (art. 33) ;
- lorsqu'une violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique, le responsable du traitement communique la violation de données à caractère personnel à la personne concernée dans les meilleurs délais (art. 34) ;
- lorsqu'un traitement, compte tenu des finalités, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement effectue, avant le traitement, une **analyse de l'impact** des opérations de traitement envisagées sur la protection des données à caractère personnel (art. 35).

# FORMATION, SENSIBILISATION, COMMUNICATION

**D**ans le rapport au ministre N° 2018-016<sup>1</sup> de février 2018, intitulé « Données numériques à caractère personnel dans l'éducation », les auteurs préconisent de :

« *Former rapidement les enseignants et les chefs d'encadrement sur l'utilisation des données scolaires numériques dans des situations pédagogiques et administratives avec une attention particulière aux traitements susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes physiques dans le sens de l'article 9 du RGPD* ».

En effet, la formation, la sensibilisation et la communication sont des enjeux de conformité des traitements autant que des facteurs d'émergence d'une culture partagée de la protection des données.

Ces leviers d'appropriation du cadre juridique sont des axes du programme académique de mise en œuvre du RGPD, avec des contenus opérationnels évolutifs en fonction de la maturité du dispositif.

## LA FORMATION

La formation académique au RGPD s'adaptera à chaque public concerné avec un objectif double :

- permettre aux équipes pédagogiques d'être aptes à transmettre des connaissances et des compétences à même de préparer progressivement les élèves au plein exercice de leur responsabilité numérique avant que ne survienne l'âge légal du consentement (15 ans) ;
- donner aux acteurs les clés d'analyse des situations de traitement de données à caractère personnel afin qu'ils prennent les décisions de conformité de leur traitement en toute connaissance de cause.

Pour atteindre ces objectifs, le concours des Erun ainsi que l'appui de la Dane seront nécessaires à la formation des enseignants. Le Paf sera mis à contribution dans le cadre de l'adaptation à l'emploi des agents. D'ores et déjà, un espace collaboratif et de formation est mis en place dans la plateforme M@gistère sous l'égide de la Dafpen. Les personnels peuvent y accéder via l'offre de formation académique de leur espace m@gistère ou au travers du lien :

<https://magistere.education.fr/ac-creteil/course/view.php?id=11466>

## LA COMMUNICATION ET LA SENSIBILISATION

Le site académique est la clé de voûte du dispositif de communication sur le RGPD. Les outils qu'il recèle devraient permettre aux responsables de traitement de prendre des initiatives de communication et de sensibilisation avec l'aide du DPD ou des référents géographiques à la protection des données (réunions de district, séminaires, présentations, etc.).

<sup>1</sup> Rapport au ministre N° 2018-016 de février 2018, par les IGEN Gilles BRAUN (DPD du MEN) et IGAEN Jean-Marc MERRIAUX (Dgesco).

## DOCUMENTS OFFICIELS

### SITOGRAPHIE

Rapport de l'inspection générale par Gilles Braun (DPD du MEN) et Jean-Marc Merriaux (Directeur du Numérique Éducatif – DNE)

<https://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/184000536.pdf>

RGPD sur le site académique

<http://www.ac-creteil.fr/pid38979/rgpd>

Site de Diffusion académique – Base de connaissances RGPD

<https://adn.ac-creteil.fr> (accès au kit de RGPD de rentrée)

Espace académique de formation RGPD (dans la plateforme M@gistère)

<https://magistere.education.fr/ac-creteil/course/view.php?id=11466>

Le RGPD sur le site de la CNIL

[www.cnil.fr/reglement-europeen-protection-donnees](http://www.cnil.fr/reglement-europeen-protection-donnees)

Guide Canopé – Les données à caractère personnel

[https://www.reseau-canope.fr/fileadmin/user\\_upload/Projets/RGPD/RGPD\\_WEB.pdf](https://www.reseau-canope.fr/fileadmin/user_upload/Projets/RGPD/RGPD_WEB.pdf)

LIL / Loi Informatique et Libertés version du 20 juin 2018 (n° 78-17 du 6 janvier 1978)

<https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000886460>

CNIL : Accompagner la rentrée scolaire des parents et des chefs d'établissement

<https://www.cnil.fr/fr/rentree-scolaire-ce-que-les-etablissements-scolaires-et-periscolaires-peuvent-vous-demander>

Mooc de la CNIL

<https://atelier-rgpd.cnil.fr/>

### BIBLIOGRAPHIE

**RGPD – Le comprendre et le mettre en œuvre (Edition ENI)**

par Jacques Foucault, Loïc Panhaleux, Dominique Renaud et Pierre Becasse

# KIT DE RENTRÉE

## LES LIVRABLES DU KIT DE RENTRÉE RGPD

Il s'agit pour la plupart de documents destinés aux responsables de traitement (RT) en vue de les outiller pour la rentrée scolaire 2019-2020. Il appartiendra à chaque responsable de les adapter à son contexte et à sa cible. Les livrables sont disponibles en téléchargement sur le site INTRANET de diffusion académique ADN : <https://adn.ac-creteil.fr>

LIVRABLES	CIBLE	DESTINÉS		
		au rectorat	aux DSDEN	aux EPLE
Livret RGPD de mise en œuvre	Responsables de structure			
Lettre d'information aux familles	Parents d'élèves			
Lettre d'information aux personnels	Personnels			
Formulaire de recueil de consentement pour le traitement de données sensibles (santé, biométrie, vidéosurveillance, etc.)	Personnels et usagers			
Modèle de convention de partenariat d'échange de données	Collectivités territoriales			
Notice : utilisation des outils numériques gratuits, quelques règles de prudence	Personnels			
Charte : administration des systèmes d'information	Administrateurs de systèmes d'information			
Charte : usage des technologies de l'information et de la communication	Personnels			
Webinaires de sensibilisation au RGPD	Personnels			
Modèle de mentions légales à insérer dans tous les sites	Webmestres			
Modèle de fiche de traitement	Registres RT			
Fiche synoptique du RGPD	Responsables de structure			
Affiche de sensibilisation au RGPD	Responsables de structure			
Cecoa : guichet unique d'assistance RGPD	Agents / Référénts RGPD			

Pour tous les usagers de l'académie, l'information générale sur le dispositif RGPD se trouve sur le site académique : [www.ac-creteil.fr](http://www.ac-creteil.fr)

# INFORMATIONS PRATIQUES

Le guichet d'assistance Cecoia est le cadre de prise en charge de toutes les demandes concernant le RGPD. Les agents munis d'identifiants de messagerie académique peuvent poster leurs demandes d'assistance RGPD 7 jours/7 pour tous les sujets (incidents, informations, demande d'exercices des droits) : <https://cecoia.ac-creteil.fr> – Rubrique : RGPD

## CONTACTS

Pour tous les autres usagers de l'académie, voici les adresses des différents contacts selon la localisation et le niveau scolaire concernés par la demande. Les demandes concernant les établissements scolaires peuvent leur être adressées directement.

### DÉLÉGUÉ ACADÉMIQUE À LA PROTECTION DES DONNÉES (DPD)

Rectorat de l'académie de Créteil – Secrétariat général – 4, rue Georges-Enesco 94000 Créteil  
[dpd@ac-creteil.fr](mailto:dpd@ac-creteil.fr)

### RÉFÉRENTS DÉPARTEMENTAUX À LA PROTECTION DES DONNÉES - MÉTIERS & ÉTABLISSEMENTS

#### SEINE-ET-MARNE

##### **DSDEN**

**M. Benoît Chastenet**

*Secrétariat général DSDEN 77*  
20, quai Hippolyte-Rossignol  
77010 Melun Cedex  
[ce.RPDM77@ac-creteil.fr](mailto:ce.RPDM77@ac-creteil.fr)

##### **ÉCOLES**

**M. Jean-Charles Pochet**

*Inspecteur de l'éducation nationale – Circonscription d'Ozoir-la-Ferrière*  
*DSDEN 77*  
43, av. du Général-De-Gaulle  
Place de la Mairie  
77330 Ozoir-la-Ferrière  
[ce.RPD1D77@ac-creteil.fr](mailto:ce.RPD1D77@ac-creteil.fr)

##### **EPLÉ**

**M. Benoît Chastenet**

*Responsable du Service juridique*  
*DSDEN 77*  
20, quai Hippolyte-Rossignol  
77010 Melun Cedex  
[ce.RPD2D77@ac-creteil.fr](mailto:ce.RPD2D77@ac-creteil.fr)

#### SEINE-SAINT-DENIS

##### **DSDEN**

**M. Jean-Louis Anthoner**

*Secrétariat général DSDEN 93*  
8, rue Claude-Bernard  
93008 Bobigny Cedex  
[ce.RPDM93@ac-creteil.fr](mailto:ce.RPDM93@ac-creteil.fr)

##### **ÉCOLES**

**M<sup>me</sup> Brigitte Ventre**

*Inspectrice de l'éducation nationale – Circonscription de Bagnole*  
*DSDEN 93*  
8, rue Claude-Bernard  
93008 Bobigny Cedex  
[ce.RPD1D93@ac-creteil.fr](mailto:ce.RPD1D93@ac-creteil.fr)

##### **EPLÉ**

**M. Frédéric Brouzes**

*Proviseur de Vie scolaire*  
*DSDEN 93*  
8, rue Claude-Bernard  
93008 Bobigny Cedex  
[ce.RPD2D93@ac-creteil.fr](mailto:ce.RPD2D93@ac-creteil.fr)

#### VAL-DE-MARNE

##### **DSDEN**

**M<sup>me</sup> Véronique Cadet**

*Secrétariat général DSDEN 94*  
68, av. du Général-De-Gaulle  
94000 Créteil  
[ce.RPDM94@ac-creteil.fr](mailto:ce.RPDM94@ac-creteil.fr)

##### **ÉCOLES**

**M. Sébastien Mounié**

*Inspecteur de l'éducation nationale*  
*ASH – CT 94 1<sup>er</sup> et 2<sup>d</sup> degrés*  
*DSDEN 94*  
68, av. du Général-De-Gaulle  
94000 Créteil  
[ce.RPD1D94@ac-creteil.fr](mailto:ce.RPD1D94@ac-creteil.fr)

##### **EPLÉ**

**M<sup>me</sup> Carole Dubarle**

*Cheffe de Service RH*  
*DSDEN 77*  
68, av. du Général-De-Gaulle  
94000 Créteil  
[ce.RPD2D94@ac-creteil.fr](mailto:ce.RPD2D94@ac-creteil.fr)



 [facebook.fr/academie.creteil](https://facebook.fr/academie.creteil)  
 [@accreteil](https://twitter.com/accreteil)  
[www.ac-creteil.fr](http://www.ac-creteil.fr)