Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE
DE L'AGRICULTURE
ET DE
L'ALIMENTATION

Ordre de service d'action

Direction générale de l'enseignement et de la recherche **Départementale des affaires transversales** **78 rue de Varenne** **75349 PARIS 07 SP** **0149554955**	**Note de service** **DGER/MAPAT/2021-5** **06/01/2021**

Date de mise en application : Immédiate
Diffusion : Tout public

Cette instruction n'abroge aucune instruction.
Cette instruction ne modifie aucune instruction.
Nombre d'annexes : 2

Objet : Mise en œuvre du Règlement Général sur la Protection des Données (RGPD) dans les EPLEFPA

Destinataires d'exécution
DRAAF / SRFD DAAF / SFD Hauts commissariats de la république des C.O.M Etablissements publics d'enseignement agricole

Résumé : L'instruction présente le Règlement Général sur la Protection des Données (RGPD) et ses enjeux pour les EPLEFPA. Elle complète l'instruction SG/SM/2018-227 du 21 mars 2018 qui décline la mise en œuvre de ce règlement au sein des services du MAA.
Elle définit l'organisation mise en place et définit les rôles et responsabilités au sein des EPLEFPA.

Textes de référence :
la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;
la loi n°2016-1320 pour une République numérique du 7 octobre 2016 ;
Règlement (UE) n° 2016/679 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel ;
Instruction technique MAA - SG/SM/2018-227 du 21/03/2018
la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles.

INTRODUCTION :

Le développement de l'e-administration au sein des établissements constitue un levier majeur de la modernisation de l'action publique. De ce fait, les établissements d'enseignement recourent de plus en plus aux technologies et usages numériques.

Dans le même temps, le nombre de cyberattaques ne cesse d'augmenter, et ce, quelle que soit la taille des organisations visées.

Par ailleurs, les usagers se montrent de plus en plus soucieux de la manière dont leurs données sont utilisées. A ce titre, la loi pour une République numérique du 7 octobre 2016 a institué le droit à l'auto-détermination informationnelle en modifiant l'article 1er de la loi « Informatique et Libertés » du 7 janvier 1978 :

« *L'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques. Toute personne dispose du droit de décider et de contrôler les usages qui sont faits des données à caractère personnel la concernant, dans les conditions fixées par la présente loi* ».

Cette nécessité pour les établissements de prendre en compte ces exigences est aujourd'hui d'autant plus importante que le RGPD renforce encore les obligations en matière de transparence des traitements et de respect des droits des personnes.
La présente instruction destinée aux seuls EPLEFPA complète l'instruction SG/SM/2018-227 du 21 mars 2018 qui décline la mise en œuvre de ce règlement au sein des services du MAA.

1-Présentation du RGPD et des notions associées

Le nouveau cadre juridique de protection des données repose sur deux textes :

* le règlement UE 2016/679 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 (dit RGPD).

* la loi *n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles*. Elle adapte au droit de l'Union Européenne la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et transpose le nouveau cadre juridique européen constitué notamment par le règlement 2016/679 du 27 avril 2016.

Deux notions doivent être préalablement définies au plan réglementaire :

La notion de donnée personnelle :
Par donnée personnelle, il faut entendre toute information se rapportant à une personne physique identifiée ou identifiable. 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. Dans un EPLEFPA, il peut s'agir des apprenants, de leurs tuteurs légaux, des commensaux mais aussi des agents, qu'ils soient titulaires, contractuels ou vacataires ainsi que les clients des activités commerciales de l'établissement. **Le traitement des données personnelles des apprenants n'est donc pas le seul à devoir être mis en**

conformité avec la nouvelle réglementation.

L'identification d'une personne physique peut être réalisée :
• à partir d'une seule donnée (*exemple : numéro de sécurité sociale*) ;
• à partir du croisement d'un ensemble de données.
La vidéosurveillance constitue une donnée personnelle qui entre dans le périmètre de la nouvelle réglementation.
La donnée personnelle est dite sensible lorsqu'elle concerne l'origine ethnique, les opinions politiques, philosophiques ou religieuses, l'appartenance syndicale, la santé ou la vie sexuelle.

La notion de traitement de données personnelles :
Par traitement de données personnelles, il faut entendre toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliqués 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.

Par contre, un fichier ne contenant que des coordonnées d'entreprises ou d'associations (par exemple, entreprise « Compagnie A » avec son adresse postale, le numéro de téléphone de son standard et un email de contact générique « compagnieA@email.fr ») n'est pas un traitement de données personnelles; en conséquence de quoi il n'entre pas dans le champ d'application du RGPD.

Un traitement de données doit avoir un objectif, une finalité. À chaque traitement de données doit être assigné un but, qui doit être légal et légitime au regard des cinq missions que le code rural et de la pêche maritime confie aux EPLEFPA.

NB : Les traitements de données portant sur les activités commerciales des exploitations agricoles et des ateliers technologiques des EPLEFPA demeurent cependant licites bien qu'ils ne soient pas rattachables aux missions précitées des EPLEFPA.

Pour les données personnelles des associations ayant leur siège dans l' EPLEFPA (*exemple : fichier d'adhérents*), il appartient au président de l'association de s'en préoccuper. Cependant, le directeur de l'établissement veillera à le lui rappeler, d'autant que les données concernent probablement les apprenants scolarisés dans son établissement.

Les principaux apports du RGPD et de la loi de transposition sont :

- Création un cadre unifié et protecteur pour les données personnelles, applicable à l'ensemble des opérateurs producteurs de données, administrations comprises.

- Renforcement des droits pour la personne physique visée par la donnée.

- Simplification des règles juridiques auxquelles sont soumis les opérateurs traitant des données personnelles tout en maintenant un haut niveau de protection pour les citoyens. **La loi remplace ainsi le système de contrôle a priori, basé sur les régimes de déclaration et d'autorisation préalables auprès de la CNIL, par un système de contrôle a posteriori, fondé sur l'appréciation par le responsable de traitement des risques que présente ce dernier.** En contrepartie, les pouvoirs de la CNIL sont renforcés et les sanctions encourues sont considérablement augmentées.

2- L'organisation interne

La nouvelle réglementation exige qu'il y ait au sein de chaque structure un responsable de traitement (RT) et un délégué à la protection des données (DPD).
Le directeur de l'EPLEFPA est le RT.

En termes de responsabilité,
Le RGPD établit clairement que c'est le RT qui est tenu de s'assurer et d'être en mesure de démontrer que le traitement est effectué conformément à ses dispositions (article 24.1 du règlement). Le respect de la protection des données relève donc de la seule responsabilité du RT.
Le DPD n'est pas responsable en cas de non-respect du RGPD et il n'est pas possible pour le RT de lui transférer, par délégation de pouvoir ou de signature, la responsabilité incombant au RT.

2-1 Le responsable du traitement (RT)

Le responsable de traitement est le directeur de l'EPLEFPA.

- Il cartographie les traitements locaux des données personnelles et pour ceux qui le nécessitent (voir chapitre 3-1-2) réalise une étude d'impact ;
- Il met en œuvre les mesures techniques et organisationnelles appropriées pour garantir que seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont collectées et traitées.
- Il doit mettre en place les dispositifs permettant la bonne information et l'exercice des droits des personnes concernées, y compris pour les données qui n'ont pas été collectées au sein de l'établissement.
- Il communique les coordonnées du DPD au sein de l'établissement et notamment auprès des personnes dont les données personnelles font ou peuvent faire l'objet d'un traitement.

2-2 Le délégué à la protection des données (DPD)

Il est souhaitable de mutualiser la fonction de DPD au niveau régional. Le DPD pressenti est le DRTIC.
Sa désignation est obligatoire et le DRAAF en tant qu'autorité académique procède à sa nomination sur avis des RT.
La décision de nomination est diffusée à l'ensemble des directeurs d' EPLEFPA de la région avec copie au SAJ (DPD Ministériel), à la DGER (DAT), au SGAR (DPD de la préfecture de région) et aux rectorats des académies respectives.
Une fois le DPD nommé, il appartient à chaque RT de le télédéclarer sur le site de la CNIL

Le DPD est principalement chargé :

- d'informer et de conseiller les RT, ainsi que les personnes concernées au sein de l'établissement ;
- de contrôler le respect du règlement européen et du droit national en matière de protection des données ;
- de conseiller les EPLEFPA de sa région sur la réalisation d'une analyse d'impact relative à la protection des données et d'en vérifier l'exécution ; de coopérer avec la CNIL et d'être le point de contact de celle-ci ;

Le DPD en tant que de besoin pourra se rapprocher des DPD académiques désignés au sein de chaque rectorat ainsi que de ceux des DASEN du rectorat.

Les questions juridiques et contentieuses liées à la mise en application du RGPD pourront être relayées auprès des agents en SRFD chargés de l'appui juridique aux établissements.

A terme le ministère veillera à organiser l'animation des DPD pour les établissements.

Une formation avant la prise de fonction de DPD est nécessaire et sera organisée au niveau national.

Les DPD sont invités à organiser dans leur région à l'intention des personnels de direction des EPLEFPA une formation de présentation du RGPD et des conséquences à en tirer dans l'organisation et le fonctionnement des établissements. Cette formation pourra le cas échéant être conjointe avec les actions de formation organisées par les DPD académiques.

3- Les obligations auxquelles sont tenus les EPLEFPA en application du RGPD

Comme n'importe quel autre opérateur traitant des données personnelles, les EPLEFPA entrent dans le champ d'application du RGPD et leurs directeurs doivent en tant que RT mettre en place une organisation adéquate pour les traitements de données personnelles.
Il y a lieu de distinguer entre les traitements de données personnelles réalisés localement par l' EPLEFPA pour la mise en œuvre de ses missions (3-1) des traitements de données personnelles qu'utilise l'établissement mais qu'il n'a pas conçu (3-2). Les obligations du RT sont variables selon la nature du traitement.

3-1 Les traitements locaux

Pour ces traitements, les RT sont tenus de:

- cartographier et trier les données concernées ;
- faire (ou faire faire) une analyse d'impact relative à la protection des données (AIPD) pour certaines données ou certains traitements ;
- rappeler leurs droits aux personnes concernées par la donnée.

3-1-1 Cartographier et trier les données concernées

Le RT doit veiller à la tenue d'un registre des traitements locaux de données personnelles dans le but **d'inventorier les données personnelles de son établissement**. Ce registre doit être tenu à jour pour recenser de nouveaux traitements ou supprimer ceux qui n'ont plus à y figurer (*Exemple : les fichiers liés aux menus alimentaires des demi-pensionnaires de l'année scolaire passée*).
Le registre permet d'avoir une vision globale au niveau de l'établissement. C'est pourquoi il ne peut pas être tenu par centre constitutif. Il est recommandé d'utiliser le modèle de registre disponible sur le site de la CNIL (https://www.cnil.fr/fr/rgpd-et-tpepme-un-nouveau-modele-de-registre-plus-simple-et-plus-didactique).

Dans le registre, il est nécessaire de créer une fiche pour chaque activité recensée, en précisant :

- l'objectif poursuivi (*exemple : fichier pour l'insertion professionnelle des stagiaires en CFPPA*) ;
- les catégories de données utilisées (*exemple : pour la paie des agents contractuels sur budget: nom, prénom, date de naissance, salaire, etc.*) ;
- les personnes ayant accès aux données (*exemple : service chargé du recrutement, service informatique, direction, etc...*) ;
- la durée de conservation de ces données.

Pour chaque fiche de registre créée, il faut vérifier que :

- les données sont nécessaires à la mise en œuvre des missions de l'établissement; seules les données nécessaires pouvant être collectées en vertu du principe de minimisation de la collecte des données (*exemple : il n'est pas utile de savoir si les enseignants titulaires ont des enfants, si l'EPLEFPA n'offre aucun service ou rémunération attachée à cette caractéristique. En revanche, cette donnée est utile pour les agents contractuels sur budget pour le calcul du SFT) ;*
- seules les personnes habilitées ont accès aux données dont elles ont besoin. Les données ne sont pas conservées au-delà de ce qui est nécessaire ;
  (poser des règles automatiques d'effacement ou d'archivage au bout d'une certaine durée dans les applications).

Après cette vérification, le RT supprimera les données dont la conservation est tardive ou non nécessaire à l'exercice de la mission de l'établissement. Il devra ensuite identifier les données soumises à analyse d'impact (3-1-2).

3-1-2 Faire (ou faire faire) une analyse d'impact relative à la protection des données (AIPD) pour certaines données ou certains traitements

L'article 35 du RGDP prévoit que lorsqu'un traitement de données personnelles est susceptible d'engendrer un risque pour les droits et libertés de la personne concernée, le responsable de traitement doit effectuer, avant de procéder au traitement, une analyse de l'impact de ce traitement sur les droits et libertés de la personne.

L'analyse d'impact consiste en la réalisation d'une étude interne faisant apparaître :

- les caractéristiques des traitements effectués ;
- les risques engendrés par ces traitements ;
- et les mesures adoptées pour y faire face.

Cette analyse doit avoir lieu en amont, avant la mise en place du traitement et faire l'objet d'un suivi et d'une mise à jour continue.
(Voir https://www.cnil.fr/fr/etude-dimpacts-sur-la-vieprivee-suivez-la-methode-de-la-cnil).

Il appartient au RT appuyé par son DPD d'évaluer le risque inhérent à la donnée ou à son traitement. Un « risque sur la vie privée » est un événement redouté (*exemple : accès non autorisé, modification non désirée ou disparition de données, et ses impacts potentiels sur les droits et libertés des personnes*) et toutes les menaces qui permettraient qu'il survienne.
Il est estimé en termes de gravité et de vraisemblance. La gravité doit être évaluée pour les personnes concernées, et non pour l'établissement.

Le DPD réunira les RT des EPLEFPA de sa région :

- pour identifier les traitements communs aux établissements dans le but de réaliser une seule AIPD ;
- pour vérifier la nécessité de mener une AIPD pour les autres traitements.

Le DPD en accord avec les RT se rapprochera des DASEN, rectorat et conseil régional pour voir dans quelle mesure les traitements de données qui seraient similaires, identiques ou comparables pourront faire l'objet d'une AIPD commune. Cette mutualisation, outre la réduction des coûts liée à l'ingénierie, contribuera à une certaine homogénéité s'agissant de la mise en œuvre du RGPD au sein de la région.
Les AIPD, une fois finalisées par chaque RT, seront à transmettre au DPD.

Les données personnelles dont le traitement ne présente pas de risque pour la vie privée ou pour lesquelles une AIPD concernant un traitement similaire a déjà été réalisée n'ont pas à donner lieu à une nouvelle AIPD. En revanche, celles dont le traitement présente ce risque nécessitent une AIPD sous peine de sanction de la part de la CNIL.

Les traitements qui remplissent au moins un des critères suivants doivent faire l'objet d'une AIPD :

- révélant l'origine prétendument raciale ou ethnique ;
- portant sur les opinions politiques, philosophiques ou religieuses (*Exemple : menu lié à une religion*);
- relatives à l'appartenance syndicale ;
- concernant la santé ou l'orientation sexuelle ;
- données génétiques ou biométriques.

Lorsque le traitement a pour objet ou pour effet :

- l'évaluation d'aspects personnels ou notation d'une personne ;
- une prise de décision automatisée ;
- la surveillance systématique de personnes (exemple : télésurveillance) ;
- le traitement de données sensibles (exemple : santé, biométrie, etc.) ;
- **le traitement de données concernant des personnes vulnérables (exemple : mineurs) ;**
- le traitement à grande échelle de données personnelles ;
- le croisement d'ensembles de données ;
- des usages innovants ou l'application de nouvelles technologies (*exemple : objet connecté*).

NB : Pour tous les fichiers comportant des données élèves, le critère lié aux personnes vulnérables est rempli.

Les questions relatives sur l'AIPD sont traitées dans l'annexe 1.

3-1-3 Rappeler leurs droits aux personnes concernées par la donnée

À chaque fois que des données personnelles sont collectées par l'EPLEFPA, le support utilisé (formulaire, questionnaire, etc...) doit comporter des mentions d'information (des exemples de mentions sont disponibles sur le site internet de la CNIL). Cette obligation de transparence vaut pour les nouveaux traitements comme ceux déjà en cours d'utilisation.

Remarque : Pour éviter des mentions trop longues au niveau d'un formulaire en ligne, il est possible de donner un premier niveau d'information en fin de formulaire et renvoyer à une politique de confidentialité/page vie privée sur site internet de l'EPLEFPA .

Deux hypothèses sont à distinguer :

- Soit la donnée ou son traitement est accessible pour la personne concernée via un support (site internet de l'EPLEFPA, télé service, etc.) :
Dans ce cas, le rappel de ses droits est inscrit dans les mentions légales,

- *si l'EPLEFPA dispose d'un site web, un formulaire de contact spécifique est à prévoir*
- *un numéro de téléphone ou une adresse de messagerie dédiée (y compris celui et celle du DPD).*

- Soit la donnée ou son traitement ne sont pas directement accessibles pour la personne concernée :
Dans ce cas, le rappel de ses droits fera l'objet de mentions légales spécifique à chaque traitement.

Les personnes dont les données sont collectées et traitées ont des droits sur ces données, qui sont d'ailleurs renforcés par le RGPD : droit d'accès, de rectification, d'opposition, d'effacement, à la

portabilité et à la limitation du traitement (voir détail en annexe 2). L'idée générale est de pouvoir recueillir leur consentement.

Un processus interne permettant de garantir l'identification et le traitement des demandes formulées par les personnes au sujet de leurs données dans des délais courts (1 mois au maximum) est à mettre en place.

Le consentement des enfants est encadré par le RGDP. Il fixe entre 13 et 16 ans l'âge à partir duquel un mineur peut consentir seul au traitement de ses données personnelles pour utiliser un service sur internet, typiquement les réseaux sociaux. On parle de majorité numérique. En deçà de ce seuil, l'autorisation des parents est nécessaire. La France l'a fixé à 15 ans.

3-2 Les traitement non locaux

Les données personnelles utilisées par l'EPLEFPA mais qui n'ont pas été collectées en son sein (données du conseil régional, d'un EPL relevant du ministère de l'éducation nationale, d'une université, de la DGER, etc...) n'ont pas être « inventoriées » ni soumises à étude d'impact au niveau de l'établissement. Ce travail de cartographie de la donnée sera réalisé par la structure à l'origine de la collecte et du traitement des données considérées. Cependant, en application de l'article 14 du RGPD, il appartient à l'établissement d'enseignement de :

- faire connaître les droits dont sont titulaires les personnes y étant associées, quelle que soit la source de la donnée ;
- indiquer la procédure à suivre.

EX : Les EPLEFPA doivent permettre aux apprenants de connaître et d'activer les droits qu'ils détiennent sur les données contenues dans le livret scolaire unique (LSU) alors même que ce traitement n'est pas local et relève du ministère de l'éducation nationale.

EX : Les EPLEFPA doivent permettre aux apprenants de connaître et d'activver les droits qu'ils détiennent sur les données contenues dans les espaces numériques de travail (ENT) alors même que ce traitement n'est pas local et relève du conseil régional.

Les obligations de l'EPLEFPA seront donc variables selon que le traitement considéré est ou non local :

- pour les traitements locaux : cartographie + études d'impact + information des personnes sur leurs droits ;
- pour les traitements non locaux : information des personnes sur leurs droits.

4- La violation de données à caractère personnel

Si une violation de données à caractère personnel intervient, le RT, au-delà de la procédure de remontée d'incident informatique telle que prévue dans la politique de sécurité des systèmes d'information avec l'appui de son DPD, prend toute mesure pou
r faire cesser aussi rapidement que possible la situation ayant permis cette violation, en informe la CNIL par une notification sur son site, avec copie au Chef du DAT de la DGER et au référent CNIL de la préfecture. Il définit la modalité adaptée pour informer les personnes concernées de cette violation dans les meilleurs délais, sans que la divulgation de cette information puisse être susceptible d'augmenter les difficultés rencontrées, notamment en rendant publique une vulnérabilité non encore corrigée.

5- Le transfert de données personnelles

Jusqu'alors le transfert de données personnelles à des tiers était possible moyennant une déclaration CNIL et une convention entre l'EPLEFPA et son partenaire dont les clauses encadraient l'utilisation de la donnée transférée.
Désormais pour les nouvelles données qui seraient transférées à partir du 25 mai 2018, il n'y a plus lieu de faire une déclaration à la CNIL. En revanche la convention conclue entre l'EPLEFPA et son partenaire devra comprendre des clauses qui garantissent le respect du RGPD par le partenaire. Dans ce cas de transfert, le RT reste responsable de ses obligations concernant les données transférées quand bien même n'en assure-t-il plus le traitement. C'est pourquoi il doit veiller à ce que le partenaire mette en place des procédures spécifiques pour garantir la sécurité, la confidentialité de la donnée et les droits qui y sont attachés.

Je remercie les directeurs d'établissement de veiller à la mise en œuvre de cette organisation dans les meilleurs délais en veillant à y associer tant les apprenants et le cas échéant leurs parents que les équipes au travers notamment des instances de l'établissement. Les modalités de cette organisation devront donner lieu à des modifications du règlement intérieur en tant que de besoin.

La Directrice générale de l'enseignement et de la recherche

Valérie Baduel

ANNEXE 1 : questions concernant l'Analyse d'Impact relative à la Protection des Données (AIPD)

Une AIPD peut-elle porter sur un ou plusieurs traitements ?

Une AIPD peut concerner un seul traitement ou un ensemble de traitements similaires.

Par exemple : deux EPLEFPA qui mettent chacun en place un système de vidéosurveillance similaire pourraient effectuer une seule analyse qui porterait sur ce système bien que celui-ci soit ultérieurement mis en œuvre par des responsables de traitements distincts.

NB : En tant que bonne pratique, une AIPD peut également être menée par le fournisseur d'un produit matériel ou logiciel pour évaluer l'impact sur la protection des données de son produit. Les différents responsables de traitement qui utilisent ensuite ce produit doivent mener leurs propres AIPD mais, le cas échéant, ceux-ci peuvent être alimentés par l'AIPD du fournisseur du produit.

À quel moment faut-il mener une AIPD ?

L'AIPD doit être menée avant la mise en œuvre du traitement. Elle doit être démarrée le plus en amont possible et sera mise à jour tout au long du cycle de vie du traitement. Il est également recommandé de revoir une AIPD de manière régulière pour s'assurer que le niveau de risque reste acceptable.

Faut-il mener une AIPD pour les traitements déjà mis en œuvre avant le 25 mai 2018 ?

Une AIPD ne sera pas exigée pour :

- les traitements qui ont fait l'objet d'une formalité préalable (déclaration ou autorisation) auprès de la CNIL avant le 25 mai 2018
- les traitements qui ont été consignés au registre d'un correspondant « informatique et libertés(CIL)».

Cette dispense d'obligation de réaliser une AIPD, pour les traitements en cours régulièrement mis en œuvre, sera limitée à une période de 3 ans : à l'issue de ce délai, les responsables de traitement devront avoir effectué une telle étude si le traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes.

Une AIPD sera exigée pour :

- pour tout nouveau traitement mis en œuvre après le 25 mai 2018 ;
- pour les traitements antérieurs n'ayant pas fait l'objet de formalités préalables auprès de la CNIL(déclaration ou autorisation) ;
- pour les traitements antérieurs au 25 mai 2018 qui ont fait l'objet d'une déclaration ou d'une autorisation préalable mais qui sont modifiés postérieurement à cette date.

Comment réaliser une AIPD ?

Une AIPD contient à minima :

- 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 et ;
- 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.

Que faire après l'AIPD ?

- Soit la gravité du risque pourra être maîtrisée par des mesures de sécurité ad hoc décrites par l'AIPD et le RT devra les mettre en œuvre avant de pouvoir procéder au traitement des données.
- Soit le risque est trop élevé notamment suite à l'impossibilité technique de le maîtriser par des mesures adéquates et qu'il induit pour les personnes des conséquences importantes voire irréversibles. Dans ce cas, le RT doit consulter le DPD et la CNIL (référent en préfecture) préalablement au traitement pour avis en lui communiquant l'AIPD. Aucun traitement n'est possible avant que la CNIL n'émette un avis.

ANNEXE 2 sur les droits des personnes dont les données sont collectées

Le droit à l'information (articles 13 et 14 RGPD)

Lorsque des données à caractère personnel relatives à une personne concernée sont collectées auprès de cette personne, le responsable du traitement lui fournit, au moment où les données en question sont obtenues, toutes une série d'informations.

• **Le droit d'accès** (article 15 RGPD)

La personne concernée a le droit d'obtenir du responsable du traitement la confirmation que ses données personnelles sont ou ne sont pas traitées et, lorsqu'elles le sont, elle a le droit d'obtenir l'accès auxdites données. Ce droit comprend également celui d'obtenir une copie des données qui font l'objet d'un traitement.

• **Le droit de rectification** (article 16 RGPD)

La personne concernée a le droit de demander que ses données soient rectifiées ou complétées, et ce dans les meilleurs délais.

• **Le droit d'effacement ou « droit à l'oubli »** (article 17 RGPD)

La personne concernée a le droit de demander l'effacement de ses données, dans les meilleurs délais si le traitement n'entre pas dans le champ de la mission de service public de l'éducation. Si les données de la personne concernée ont été transmises à d'autres entités, le mécanisme du « droit à l'oubli » s'enclenche : le responsable de traitement devra prendre toutes les mesures raisonnables pour informer les autres entités que la personne concernée a demandé l'effacement de tout lien vers ses données personnelles, ou de toute copie ou reproduction de celles-ci.

• **Le droit à la limitation du traitement** (article 18 RGPD)

La personne concernée a le droit, dans certains cas prévus par la loi, d'obtenir du responsable du traitement la limitation de ses données. Lorsqu' une telle limitation est demandée, le responsable de traitement ne pourra plus que stocker les données. Aucune autre opération ne pourra, en principe, avoir lieu sur ces données personnelles.

• **L'obligation de notification du responsable** (article 19 RGPD)

Cet article met en place une obligation de notification à charge du responsable de traitement qui l'oblige à communiquer à chaque destinataire des données toute rectification, effacement ou limitation du traitement

• **Le droit à la portabilité des données** (article 20 RGPD)

La personne concernée a le droit de récupérer les données qu'elle a fournies au responsable de traitement, dans un format structuré, couramment utilisé et lisible par machine, et a le droit de transmettre ces données à un autre responsable du traitement. Ce droit ne peut être utilisé que si le traitement des données est basé sur le consentement de la personne concernée ou sur un contrat.

• **Le droit d’opposition** (article 21 RGPD)

La personne concernée a le droit de s’opposer à tout moment, pour des raisons tenant à sa situation particulière, à un traitement des données à caractère personnel la concernant fondé sur l’intérêt public ou l’intérêt légitime du responsable de traitement, y compris le profilage basé sur ces dispositions.

• **Le droit de ne pas être soumis à une décision individuelle automatisée** (article 22 RGPD)

La personne concernée a le droit de ne pas être soumise à une décision résultant exclusivement d’un traitement automatisé produisant des effets juridiques la concernant ou l’affectant de manière significative de façon similaire. Le profilage y est expressément inclus.

• **Le droit à la communication d’une violation de données à caractère personnel** (article 34 RGPD).

Le responsable de traitement est obligé de notifier à la personne concernée les violations de données susceptibles de l’exposer à un risque élevé à ses droits et libertés.