GUIDE PRATIQUE DE SENSIBILISATION A LA PROTECTION DES DONNEES A CARACTERE PERSONNEL

Ce guide pratique a pour objectif de sensibiliser les chefs d'établissements des établissements en gestion directe de l'Union Européenne à la mise en œuvre d'un dispositif de protection des données à caractère personnel, conforme au Règlement Général de la Protection des Données (ci-après « *RGPD* »). Il précise le périmètre d'application du RGPD, et rappelle les principales notions à connaître ainsi que les actions essentielles à engager afin de permettre la mise en œuvre de cette nouvelle réglementation.

Ce document n'est pas définitif et est susceptible d'évoluer. En effet, d'une part les ressources documentaires proposées par la Commission Nationale de l'Informatique et des Libertés (ci-après «*CNIL* ») s'enrichissent régulièrement, et d'autre part, vos différents retours nous permettront d'améliorer la démarche proposée.

Il sera mis en ligne sur le site internet de l'Agence, dans la rubrique « Délégué à la protection des données ».

Loi 78-17 du 6 janvier 1978 modifiée – Article premier : « 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.»

RGPD du 27 avril 2016 –Chapitre 1- Article premier : « Le présent règlement établit des règles relatives à la protection des personnes physiques à l'égard du traitement des données et des règles relatives à la libre circulation de ces données.

Le présent règlement protège les libertés et droits fondamentaux et personnes physiques, et en particulier leur droit à la protection des données »

Sommaire

I. Périmètre

1.1 Objet

Entré en vigueur le 25 mai 2018, le RGPD constitue le nouveau cadre européen concernant le traitement et la circulation des données à caractère personnel.

Le RGPD affirme la primauté des droits des personnes physiques à l'égard de leurs données tout en présentant un cadre d'utilisation de ces données, notamment le respect impératif des 3 critères suivants obligatoires : **Licéité / transparence / Loyauté**.

Le législateur européen vise 3 objectifs principaux:

1. Renforcer les droits des personnes, notamment par la création d'un droit à l'**effacement**, à la **portabilité** et à la **limitation** des données à caractère personnel ;
2. Responsabiliser les acteurs traitant des données (responsables de traitement et sous-traitants) ;
3. Uniformiser les principes fondamentaux et les obligations de chacun des acteurs.

1.2 Champ d'application

Le RGPD s'applique :

- aux traitements de données mis en œuvre par les établissements situés sur le **territoire de l'Union européenne** (*critère de l'établissement*),
- aux traitements de données mis en œuvre par les établissements situés en-dehors de l'Union européenne dès lors que les données concernent des **ressortissants de l'Union Européenne** (*critère de ciblage).*

II. Principes fondamentaux de la Protection des données à caractère personnel

2.1 Définitions des notions clés

2.1.1 Données à caractère personnel

Des données sont considérées comme à caractère personnel dès lors qu'elles permettent d'identifier **directement** ou **indirectement** des personnes physiques.

Exemple : nom, n° d'immatriculation, n° de téléphone, photographie, éléments biométriques tels que l'empreinte digitale, ADN, informations permettant de discriminer une personne au sein d'une population telles que, par exemple, le lieu de résidence, la profession, le sexe, l'âge, etc…

Il peut s'agir d'informations qui ne sont pas associées au nom d'une personne mais qui peuvent permettre de l'identifier et de connaître ses habitudes ou ses goûts.

Les données relatives à des personnes physiques appartiennent à ces personnes physiques : elles doivent pouvoir contrôler en permanence l'utilisation qui en est faite – et juger ainsi si l'utilisation de l'informatique porte atteinte à leur identité, à leur vie privée ou à leurs libertés.

Aussi, tout dépositaire de données à caractère personnel doit-il :

- pouvoir expliquer et démontrer dans quels buts il collecte et traite ces données,
- pouvoir prouver aux personnes qu'il prend soin et protège leurs données,
- manifester son respect des critères de conformité définis par la loi Informatique et Libertés et le RGPD.

2.1.2 Traitements de données

Constitue un traitement de données à caractère personnel toute opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction.

Exemples :

- *Fichiers de gestion des élèves et des personnels,*
- *Annuaires en ligne des anciens diplômés,*
- *Espaces numériques de travail……*

2.1.3 Responsable de traitement

Est considéré comme le responsable du traitement la personne physique ou morale qui **détermine les finalités et les moyens** de toute opération (*collecte, enregistrement, modification...)*, appliquée à des données à caractère personnel.

Le responsable du traitement est **la personne pour le compte de laquelle** est réalisé le traitement.

Afin de déterminer l'identité du responsable du traitement, il est possible de faire appel aux critères suivants :

- « *maîtrise d'ouvrage* » du traitement : à quoi servira-t-il et comment fonctionnera-t-il ?

- « *mise en œuvre* » du traitement : qui décide de s'en servir et qui s'en sert ?

Le responsable du traitement doit être distingué des personnes qui interviennent dans le cadre de sa mise en œuvre telles que, par exemple, les sous-traitants.

Toute personne traitant des données à caractère personnel pour le compte du responsable du traitement est considérée comme un sous-traitant au sens de la loi.

La sous-traitance ne décharge pas le responsable du traitement de sa responsabilité.

Exemple : Dans le cas d'un hébergement externe de l'un des sites web de l'établissement scolaire, l'hébergeur est considéré comme le sous-traitant.

2.2 Principes fondamentaux de la Protection des données

2.2.1 Finalité du traitement

Les données à caractère personnel ne peuvent être recueillies et traitées que pour un usage **déterminé et légitime**, correspondant aux missions de l'établissement, responsable du traitement. C'est au directeur d'établissement qu'il appartient de fixer la finalité des traitements mis en œuvre pour le compte de son établissement et de la faire respecter.

Tout détournement de finalité est passible de sanctions pénales.

Exemple : Le fichier de gestion administrative et pédagogique des élèves ne peut être utilisé à des fins commerciales ou politiques.

2.2.2 Licéité du traitement

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 ;
- au respect d'une obligation légale à laquelle le responsable du traitement est soumis ;
- à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique ;
- 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 ;
- 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.

Important : Le fondement du traitement va conditionner l'exercice de certains droits pouvant être exercés par les personnes.

2.2.3 Proportionnalité

Seules doivent être enregistrées les informations **pertinentes et nécessaires** pour assurer la gestion des services de l'établissement scolaire.

Exemple : Demander le revenu des parents de l'élève pour recevoir la « newsletter » de l'établissement n'est ni pertinent ni nécessaire au regard de la finalité poursuivie par le traitement.

2.2.4 Durée de conservation

Les informations **ne peuvent être conservées de façon indéfinie** dans les fichiers informatiques. Une durée de conservation doit être établie en fonction de la finalité de chaque fichier.

Cette durée va donc varier selon les différents objectifs poursuivis par l'utilisation de données personnelles.

Exemple : Les informations collectées dans le cadre de l'organisation d'un examen sont conservées pour la durée de la session de l'examen.

2.2.5 Sécurité et confidentialité

Le responsable du traitement est astreint à une **obligation de sécurité** : il doit prendre les mesures nécessaires pour garantir la **confidentialité** des données et éviter leur divulgation.

• Les données contenues dans les fichiers ne peuvent être consultées que par les services habilités à y accéder en raison de leurs fonctions.

Exemple : Veiller à ce que chaque utilisateur ait un mot de passe individuel régulièrement changé et que les modalités d'accès soient précisément définies en fonction des besoins réels.

• Le responsable du traitement doit prendre toutes les mesures pour empêcher que les données soient déformées, endommagées ou que des tiers non autorisés y aient accès.

Exemple : S'il est fait appel à un prestataire externe, des garanties contractuelles doivent être envisagées[1].

• Les mesures de sécurité, tant physiques que logiques, doivent être prises.

Exemple : Protection anti-incendie, copies de sauvegarde, installation de logiciel antivirus, changement fréquent des mots de passe alphanumériques d'un minimum de 8 caractères.

• Les mesures de sécurité doivent être adaptées à la nature des données et aux risques présentés par le traitement.

Exemple : Authentification forte pour l'accès aux résultats d'examen.

2.2.6 Respect du droit des personnes

• Informer les intéressés : Lors de l'informatisation de tel ou tel service, ou lorsque des données sont recueillies par exemple par voie de formulaire, les **personnes concernées par le traitement doivent**

1 Annexe 1 – Modèle de clause de confidentialité dans le cadre d'un marché ou d'un contrat de sous-traitance.

être **informées de la finalité du traitement**, du caractère obligatoire ou facultatif du recueil, des destinataires des données et des **modalités d'exercice des droits** qui leur sont ouverts au titre de la « *loi Informatique et Libertés* » à savoir : un droit d'accès, de rectification, d'effacement et d'opposition[2], droit à la limitation du traitement, droit à la portabilité des données.

Cette information doit être diffusée, par exemple, au moyen d'affiches apposées dans les services recevant du public et portée sur les formulaires établis par l'établissement, ainsi que sur les courriers adressés aux personnes dont les données sont collectées[3].

2.2.7 Transfert de données hors Union Européenne

Un responsable d'un traitement ne peut transférer des données à caractère personnel vers un État n'appartenant pas à la Communauté européenne (*dit « pays tiers »)* que si cet État assure un niveau de protection adéquat ou suffisant de la vie privée et des libertés et droits fondamentaux des personnes à l'égard du traitement dont ces données font l'objet ou peuvent faire l'objet.

La Commission européenne a le pouvoir de reconnaître qu'un pays accorde une protection adéquate ou suffisante, dans une décision prise à cet effet, dénommée « ***décision d'adéquation*** ».

Constitue ainsi un transfert de données vers un pays tiers toute communication, copie ou déplacement de données par l'intermédiaire d'un réseau, ou toute communication, copie ou déplacement de ces données d'un support à un autre, quel que soit le type de ce support, dans la mesure où ces données ont vocation à faire l'objet d'un traitement dans le pays destinataire.

La loi Informatique et Libertés modifiée prévoit qu'un responsable de traitement peut cependant transférer des données à caractère personnel vers un État n'accordant pas une protection adéquate si :

a) la personne à laquelle se rapportent les données **a consenti expressément** à leur transfert ou si,

b) le transfert est nécessaire à l'une des conditions suivantes :

- À la sauvegarde de la vie de cette personne ;
- À la sauvegarde de l'intérêt public ;
- Au respect d'obligations permettant d'assurer la constatation, l'exercice ou la défense d'un droit en justice ;
- À la consultation, dans des conditions régulières, d'un registre public qui, en vertu de dispositions législatives ou réglementaires, est destiné à l'information du public et est ouvert à la consultation de celui-ci ou de toute personne justifiant d'un intérêt légitime ;
- À l'exécution d'un contrat entre le responsable du traitement et l'intéressé, ou de mesures pré-contractuelles prises à la demande de celui-ci ;
- À la conclusion ou à l'exécution d'un contrat conclu ou à conclure, dans l'intérêt de la personne concernée, entre le responsable du traitement et un tiers.

[2] Toute personne a le droit de s'opposer, pour des motifs légitimes, à ce que des données la concernant soient enregistrées dans un fichier informatique, sauf si celui-ci présente un caractère obligatoire.
Exemple Le fichier de gestion administrative des élèves ou encore le fichier de gestion de prêts de livres de la bibliothèque présentent un caractère obligatoire à l'inverse de l'annuaire des anciens élèves.

[3] Annexe 2 – Modèle de mention d'information

2.2.8 Consentement

a) Le consentement

Un traitement est licite (*sans consentement*) s'il est fondé sur une base juridique : tel un contrat auquel la personne concernée est partie, une obligation légale, une sauvegarde des intérêts vitaux d'une personne physique, ou encore une mission d'intérêt public, des fins d'intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, dans la limite des intérêts, libertés et droits fondamentaux de la personne concernée.

C'est également le cas lorsque le traitement est nécessaire à la personne concernée en matière de droit du travail, de la sécurité sociale et de la protection sociale, dans la mesure où ce traitement est autorisé par le droit européen ou le droit français ou une convention collective respectant le droit européen et français.

Le consentement est requis dans tous les autres cas.

En fonction des risques inhérents aux traitements envisagés, il doit être **libre-spécifique-éclairé-univoque et explicite.**

Un consentement explicite est donc requis pour tout traitement (*mis en œuvre par l'AEFE en sa qualité de Responsable de traitement):*

- Débouchant sur une *décision individuelle automatisée* (y compris le *profilage)* affectant la personne ou ses droits de manière significative,
- Sur des données sensibles, ou relevant de catégories particulières sauf si le droit de l'UE ou du pays prévoit l'impossibilité de la levée d'interdiction par le consentement de la personne concernée,
- Ou en cas de *transferts vers des pays hors UE* qui ne présentent pas les garanties suffisantes de réutilisation des données à d'autres fins : mise en œuvre d'un traitement ultérieur incompatible avec la finalité pour laquelle les données ont été initialement collectées,
- D'utilisation de cookies pour certaines finalités.

b) Consentement des enfants en ce qui concerne les services de la société d'information

L'AEFE étant un réseau scolaire international d'établissements scolaires du 1er et 2ème degré, les traitements que les établissements peuvent mettre en œuvre concernent dans sa grande majorité des personnes mineures.

Le traitement des données à caractère personnel relatives à un enfant est licite lorsque l'enfant est âgé d'au moins 16 ans. Lorsque l'enfant est âgé de moins de 16 ans, ce traitement n'est licite que si, et dans la mesure où, le consentement est donné ou autorisé par le titulaire de la responsabilité parentale à l'égard de l'enfant.

Le responsable du traitement s'efforce raisonnablement de vérifier, en pareil cas, que le consentement est donné ou autorisé par le titulaire de la responsabilité parentale à l'égard de l'enfant, compte tenu des moyens technologiques disponibles.

2.2.9 'Accountability", principe du rendu-compte

L'accountability est l'obligation pour un responsable du traitement de rendre des comptes. Elle consiste en un processus permanent et dynamique de mise en conformité d'une entreprise à la réglementation relative à la protection des données grâce à un ensemble de règles, d'outils et de bonnes pratiques correspondantes.

Selon les termes du RGPD, elle doit également consister en un mécanisme permettant de démontrer l'efficacité des mesures prises et l'effectivité de la protection des données.

III. Recommandations générales applicables à l'ensemble des traitements

Ces recommandations générales valent pour la plupart des traitements et visent le problème le plus fréquent en matière de conformité « *Data Protection* » :

Trop d'utilisateurs voient
trop de données
relatives à **trop** de personnes
pendant **trop** longtemps.

Il convient d'adopter une politique de Conformité "*Protection des données*" dont les points ci-dessous doivent être respectés :

3.1 Principe de Transparence

Les responsables de fichiers de données à caractère personnel ont l'obligation légale d'informer les personnes concernées par les informations qu'ils détiennent.

Cette information doit figurer sur chaque formulaire, papier ou dématérialisé ainsi que sur tout support.

En outre, les documents généraux de communication vers les personnes concernées (*élèves et leurs familles, agents, Candidats, Public)* devront intégrer une présentation des principes en matière de protection des données (ex : *Charte Informatique, politique générale de protection des données*), et présenter de manière générale les traitements identifiés.

Plan d'actions proposé :

- Contrôler l'origine des données *:* cartographie des données avec leur origine de collecte, cartographie des échanges de données avec les partenaires, documentation sur l'origine des données, trace de chaque cession de données,
- Inventorier les mentions en place : vérifier l'existence des mesures d'informations sur tout support et leur contenu (*formulaires papiers, dématérialisés, clauses contractuelles, clauses « Privacy » ou « Politique de confidentialité » sur les sites internets),*
- Mettre à jour les supports d'informations,
- Rédiger et actualiser le catalogue des mentions selon les thématiques.

3.2 Recommandation générique de mentions

La loi impose que les personnes soient informées, lors du recueil, de l'enregistrement ou de la première communication des données : [4]

- de la finalité poursuivie par le traitement ;
- du caractère obligatoire ou facultatif des réponses ;
- des conséquences d'un défaut de réponse ;
- de l'identité du responsable du traitement ;
- des destinataires ou catégorie de destinataires des données ;
- de leurs droits (*droit à l'information, d'accès et de rectification, droit d'opposition, droit à l'effacement, droit à la portabilité, à la limitation*) ;

[4] Annexe 2 – Modèle de mention d'information

- la durée de conservation (obligation du Règlement Européen) ;
- le cas échéant, des transferts de données vers des pays hors UE.

Afin d'établir la politique en matière d'Information et des Droits des Personnes, conformément aux textes en vigueur, 4 critères ont été retenus :

- la population concernée
- la finalité du traitement
- les mesures d'informations
- les mentions à rédiger.

3.3 Sécurité des données

La loi impose au responsable de traitement de prendre toutes les précautions utiles pour préserver la sécurité des données dont il est responsable, en fonction de leur nature et des risques supposés. Il doit en particulier empêcher l'accès à ces données aux tiers non autorisés à les consulter et prendre un certain nombre de précautions lorsqu'il envisage de conserver, de communiquer ou de rendre accessibles des données à caractère personnel.

L'accès aux données à caractère personnel doit être sécurisé, c'est à dire que la confidentialité, l'intégrité et l'authenticité des informations doivent être assurées par le responsable de traitement.

Le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, y compris entre autres, selon les besoins :

a) la pseudonymisation et le chiffrement des données à caractère personnel ;

b) des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;

c) des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ;

d) une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement. »

Lors de l'évaluation du niveau de sécurité approprié, il est tenu compte en particulier des risques que présente le traitement, résultant notamment de la destruction, de la perte, de l'altération, de la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou de l'accès non autorisé à de telles données, de manière accidentelle ou illicite.

La CNIL incite les responsables des traitements au « *contrôle de la fiabilité des matériels et des logiciels qui doivent faire l'objet d'une étude attentive afin que des erreurs, lacunes et cas particuliers ne puissent conduire à des résultats préjudiciables aux personnes ; la capacité de résistance aux atteintes accidentelles ou volontaires extérieures ou intérieures en étudiant particulièrement l'implantation géographique, les conditions d'environnement, les aménagements des locaux et de leurs annexes* ».

Plan d'action proposé :

- Concevoir une procédure de création et de suppression des **comptes utilisateurs**

L'accès aux postes de travail et aux applications doit s'effectuer à l'aide de comptes utilisateurs nominatifs, et non « *génériques* » (compta1, compta2…), afin de pouvoir éventuellement être capables de tracer les actions faites sur un fichier et, ainsi, de responsabiliser l'ensemble des intervenants. En effet, les comptes « *génériques* » ne permettent pas d'identifier précisément une personne.

Cette règle doit également s'appliquer aux comptes des administrateurs systèmes et réseaux et des autres agents chargés de l'exploitation du système d'information.

Les demandes d'ouverture ou de modifications de droits doivent être écrites et tracées ; les habilitations accordées doivent être auditables à l'instant *t* ; les actions des administrateurs doivent être loggées de manière inviolable

- **Identifier** précisément qui peut avoir accès aux Traitements et les droits associés

L'accès aux données à caractère personnel traitées dans un fichier doit être limité aux seules personnes qui peuvent légitimement y avoir accès pour l'exécution des missions qui leur sont confiées.

De cette analyse, dépend « *le profil d'habilitation* » de l'agent concerné.

Pour chaque mouvement ou nouvelle affectation d'un agent à un poste, le supérieur hiérarchique concerné doit identifier le ou les fichiers auxquels celui-ci a besoin d'accéder et faire procéder à la mise à jour de ses droits d'accès.

Une vérification périodique des profils des applications et des droits d'accès aux répertoires sur les serveurs est donc nécessaire afin de s'assurer de l'adéquation des droits offerts et de la réalité des fonctions occupées par chacun.

Créer une revue périodique des droits, des habilitations et authentifications

- Anticiper le risque de perte ou de divulgation des données et formaliser les **analyses de risques** et d'impacts lorsqu'il s'agit de données sensible ;

- Mettre en œuvre la politique de sécurité du système d'information de l'AEFE ;

A ce titre, l'ensemble des règles relatives à la sécurité informatique doit être formalisé dans un document accessible à l'ensemble des salariés. Sa rédaction requiert l'inventaire préalable des éventuelles menaces et vulnérabilités qui pèsent sur un système d'information.

Il convient de faire évoluer régulièrement ce document, au regard des modifications des systèmes et outils informatiques utilisés par l'organisme concerné. Enfin, le paramètre « *sécurité* » doit être pris en compte en amont de tout projet lié au système d'information.

- Sécuriser le réseau local, **l'accès physique** aux locaux et aux postes de travail

- Sécuriser les échanges des données

- **Sensibiliser** les utilisateurs aux « risques informatiques » et à la Loi Informatique et Libertés et au RGPD

- **Tracer** et horodater les accès selon les utilisateurs

Auditer régulièrement les comptes inactifs depuis plus de 6 semaines.

- Revue périodique des Droits d'accès

Vérifier périodiquement les profils des applications et les droits d'accès aux répertoires sur les serveurs afin de s'assurer de l'adéquation des droits ouverts et de la réalité des fonctions occupées par les utilisateurs :

• Type de contrôle	• Fréquence	• Moyen
• Droits d'accès utilisateurs & administrateurs	• Trimestriel	• Remontée automatique d'alertes relatives aux changements • sur les comptes (création/suppressions…) à la SSI
• Comptes des administrateurs	• Mensuel	• Revue réalisée par la SSI
• Comptes internes	• Trimestriel	• Revue réalisée par la SSI

- Formaliser les process de reporting des incidents et des violations de sécurité informatique
- Un système d'information doit être sécurisé vis-à-vis des attaques extérieures.

Un premier niveau de **protection** doit être assuré par des dispositifs de sécurité logique spécifiques tels que des routeurs filtrants (ACL), pare-feu, sonde anti intrusions.

Une protection fiable contre les virus et logiciels espions suppose une veille constante pour mettre à jour ces outils, tant sur le serveur que sur les postes des agents.

L'utilisation de la messagerie électronique doit faire l'objet d'une vigilance particulière.

Il est également indispensable de sécuriser les réseaux sans fil compte tenu de la possibilité d'intercepter à distance les informations qui y circulent : utilisation de clés de chiffrement, contrôle des adresses physiques des postes clients autorisés.

Les accès par internet aux outils d'administration électronique nécessitent également des mesures de sécurité fortes, notamment par l'utilisation de protocoles sécurisés (exemple : IPsec ...).

- Veiller à **stocker** les données sur des espaces serveurs prévus à cet effet et faisant l'objet de sauvegardes régulières.

Les supports de sauvegarde doivent être stockés dans un local distinct de celui qui héberge les serveurs, idéalement dans un coffre ignifugé.

Les serveurs hébergeant des données sensibles ou capitales pour l'activité l'organisme concerné doivent être sauvegardés et pourront être dotés d'un dispositif de tolérance de panne.

Il est recommandé d'écrire une procédure « *urgence – secours* » qui décrira comment remonter rapidement ces serveurs en cas de panne ou de sinistre majeur.

- Les postes des agents doivent être **paramétrés** afin qu'ils se verrouillent automatiquement au-delà d'une période d'inactivité.

Les utilisateurs doivent également être incités à **verrouiller** systématiquement leur poste dès qu'ils s'absentent de leur bureau.

Le blocage de **l'usage des ports USB** sur les postes « *sensibles* » est fortement recommandé.

L'accès aux locaux sensibles, tels que les salles hébergeant les serveurs informatiques et les éléments du réseau, doit être limité aux personnels habilités.

Ces locaux doivent faire l'objet d'une sécurisation particulière (*exemple : vérification des habilitations, gardiennage, portes fermées à clé, digicode, contrôle d'accès par badge nominatifs, etc.)*

- Les données qui peuvent être considérées « *sensibles* » au regard de la loi, par exemple des données liées à des difficultés sociales ou des données relatives à des moyens de paiement, doivent au surplus faire l'objet d'un **chiffrement**.

- Veiller à ce que les utilisateurs nettoient régulièrement leurs vieux documents et messages électroniques sur leurs postes. De même, **nettoyer** régulièrement le répertoire d'échange partagé entre les différents services afin qu'il ne se transforme pas en espace « fourre-tout » (*fichiers personnels des agents mélangés avec des dossiers sensibles*).

Sous-traitance :

Les interventions des divers sous-traitants du système d'information d'un responsable de traitement doivent présenter les garanties suffisantes en termes de sécurité et de confidentialité à l'égard des données auxquels ceux-ci peuvent, le cas échéant, avoir accès.

Veiller à la confidentialité des données vis-à-vis des prestataires et prévoir des clauses de Responsabilité Informatique et Libertés en cas de Sous-traitance.

Plan d'action proposé :

- Imposer aux prestataires de mettre en œuvre les mesures de sécurité au regard de l'art34 de loi Informatique et Libertés modifiée et l'art 32 du RGPD et prévoir de les auditer.
- Imposer aux prestataires de communiquer toute perte ou piratage de données.
- Imposer aux prestataires de détruire les données en fin de mission, avec PV de destruction.
- Interdire aux prestataires d'utiliser les données pour tout autre usage.
- Interdire aux prestataires de sous-sous-traiter, de stocker ou de traiter les données hors UE.

3.4 Principe de Légalité

Condition de légalité : Déterminer un objectif précis au préalable et autorisé par les textes en vigueur.

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, comme incompatible avec les finalités initiales (*limitation des finalités*) ;

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*)

Plan d'action proposé :

- Maîtriser le contexte légal et réglementaire
- Documenter le fondement juridique des traitements
- Déterminer et prouver le contexte d'intérêts légitimes
- Effectuer au préalable l'analyse de conformité avant tout déploiement d'un nouveau projet informatique comportant des données à caractère personnel

3.5 Principe du Droit à « l'Oubli » ou à l'effacement

Les données à caractère personnel doivent être 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.

Plan d'action proposé

- Déterminer une durée de conservation adaptée, précise et proportionnelle à la finalité pour chaque traitement mis en œuvre.
- Mettre en place les mesures garantissant le respect de cette durée
- Mettre à jour les durées de conservation selon les exigences législatives et réglementaires ou le référentiel CNIL (*doctrine*)

La loi permet de mettre en place les solutions suivantes :

- **Suppression ou purge** des données : cette solution est généralement complexe à mettre en œuvre techniquement, et supprime quasi-totalement la possibilité de réaliser des suivis dans le temps et des statistiques.

- **Anonymisation** des données : il s'agit d'un processus irréversible. Les statistiques demeurent possibles.

- **Archivage** des données (*elles demeurent accessibles – mais ne sont plus présentes dans le système actif, de production*) : cette solution est généralement complexe à mettre en œuvre techniquement (*car généralement non prévue par les éditeurs de solutions*), et rend les statistiques complexes.

- **Minimisation :** qui vise à limiter la collecte d'informations sur les particuliers

- Paramétrer les applications ou les logiciels selon les durées de conservation définies (*évolution logicielle*)

- Procéder à un **audit annuel ou bi-annuel** de l'effectivité des durées de conservation (*contrôle effectif des purges)* selon le type de traitements (*RH, instruction et versement des aides publiques...)*

Recommandations génériques :

Il est important que les durées de conservation des données et les règles techniques implémentant ces durées soient définies systématiquement – ce qui implique en particulier de prendre en compte ces obligations dans la gestion des projets dès l'amont, avec une supervision par le SSI ou le référent Métier. Lorsque la durée de conservation n'est pas définie par les textes, le SSI ou le référent métier veille à choisir une durée de conservation proportionnelle et non excessive à la finalité poursuivie.

Les mesures peuvent se traduire par : un Workflow Go / No go imposé dans les process projet ; la mise en place d'un dispositif d'alertes en cas d'échéance de la durée de conservation

Créer un Process « Contrôle référentiel des durées de conservation » de manière annuelle

3.6 Principe de Pertinence des données (P)

L'article 5-1c) du Règlement impose que les données soient : adéquates, **pertinentes** et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données);

Exemple : Demander les revenu des parents d'un élève pour recevoir la « newsletter » de l'établissement n'est ni pertinent ni nécessaire au regard de la finalité poursuivie par le traitement.

Plan d'action proposé

- Extraire les zones de textes libres / commentaires des bases de données et de les tester sur http://detector.cabinet-cilex.com
- Veiller à ce que les informations collectées sur les personnes et renseignées dans les zones de commentaires libres soient adéquates, pertinentes et non excessives au regard de la finalité du traitement envisagé, qu'il soit automatisé ou au format papier. Les commentaires ne doivent donc pas être inappropriés, subjectifs et insultants.
- Prévoir la formation des utilisateurs
- Mettre en place un contrôle semestriel ou annuel
- Définir une durée de conservation de 12 mois par défaut

3.7 Formalisation de la politique de conformité Informatique et Libertés

Les responsables et sous-traitants devront établir et conserver un enregistrement interne des traitements de données et des éléments attestant du respect des principes posés par le Règlement.

Plan d'action proposé

- Rédactions et mise à jour des chartes d'information et d'utilisation des systèmes d'information
- Rédaction des mesures d'informations (*mentions CNIL à insérer dans les contrats de travail, mettre à jour : lettre d'information aux élèves, familles d'élèves, agents réseau et agents siège le cas échéant, sites internets …)*
- Mise en place d'un service chargé des demandes d'accès, de rectification et d'opposition
- Formalisation des procédures internes de sécurité informatique
- Formalisation d'un registre de suivi des traitements
- Formalisation de la tenue d'un registre des incidents et failles de sécurité concernant les données à caractère personnel
- Formalisation des contrôles et des audits liés à la conformité.

3.8 Politique d'habilitation et d'authentification :

Chaque utilisateur ne devant accéder qu'aux données strictement nécessaires à l'exercice de son activité professionnelle, des profils d'habilitation doivent être définis pour déterminer les types de données accessibles à une catégorie d'utilisateur.

Une procédure de gestion des habilitations doit être formalisée afin d'assurer leur mise à jour, notamment pour supprimer les permissions d'accès des utilisateurs qui ne sont plus habilités ou qui ont quitté l'organisme.

Cette procédure doit également prévoir des contrôles des habilitations afin de s'assurer que les permissions d'accès aux données ne sont pas détournées *(ex : partage d'un seul compte utilisateur utilisé par différentes personnes).*

La charte informatique doit être rédigée afin d'informer et responsabiliser les utilisateurs et mentionner :

- Le rappel des règles de protection des données et les sanctions encourues en cas de non-respect de la loi

- les modalités d'intervention du service de l'informatique interne, notamment en cas de télémaintenance
- les moyens d'authentification
- les règles de sécurité informatique
- les modalités d'utilisation des moyens informatiques et de télécommunications mis à disposition
- les responsabilités et sanctions encourues en cas de non-respect de la charte.

3.9 Échange et communication des données

L'article 3-II de la loi « *Informatique et Libertés* » définit un destinataire de données à caractère personnel comme étant « *toute personne habilitée à recevoir communication de ces données autres que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, en raison de leurs fonctions, sont chargées de traiter les données* ».

Parmi les organismes et personnes susceptibles de recevoir des données de l'AEFE, on doit distinguer :

- les agents chargés de traiter les données en raison de leurs fonctions, qualifiés comme étant des « personnes habilitées à y accéder »,
- les sous-traitants,
- les destinataires des données, soit les personnes ou organismes extérieurs auxquels le responsable de traitement transmet des données de sa propre initiative, à l'exclusion des sous-traitants, ou à la suite d'une demande non prévue par la loi qu'il estime légitime,
- les « tiers autorisés », c'est-à-dire les personnes ou organismes pouvant obtenir la communication de données en vertu d'une disposition législative ou réglementaire.

Plan d'action proposé :

- Identifier l'ensemble des personnes susceptibles de recevoir des données, classifier selon s'il s'agit de destinataire ou de tiers autorisés.

3.10 Maîtrise de la chaîne de sous-traitance

En vertu de l'article 28 du RGPD, il est recommandé de s'assurer que les sous-traitants présentent des garanties suffisantes pour que les traitements confiés répondent aux obligations issues du RGPD.

Plan d'action proposé :

- Récupérer des modèles d'appels d'offres et de contrats
- Définir une stratégie d'évaluation de la conformité des sous-traitants
- Grille d'évaluation
- Processus de transmission et d'analyse des résultats
- Identifier les sous-traitants les plus à risques : prestataire développement d'applications informatiques, hébergement, maintenance
- Identifier le type d'accès aux données : sans accès, accès via les moyens de l'AEFE, export des données par le Sous-traitant.

IV- Les 6 étapes : méthode

4.1 Etape 1 : Désigner un correspondant – délégué à la protection des données

Pour piloter la gouvernance des données personnelles, le directeur de l'AEFE a nommé un délégué à la protection des données (DPD) qui exerce une mission d'information, de conseil et de contrôle en interne. Cette nomination a fait l'objet d'une information auprès de la CNIL et porte la référence DPO-22304.

Chaque établissement doit procéder à la désignation d'une personne compétente en matière de protection des données[5]. Le Directeur Administratif et Financier est la personne la plus placée pour exercer ces missions.

Ce **Correspondant - délégué à la protection des données, relai du DPD de l'AEFE** sera chargé de s'assurer de la mise en conformité au règlement européen.

Ce correspondant possède une vision transverse des activités et des processus, ce qui lui permet :

- de **relayer les principes** et les règles de protection des données au sein de l'établissement ;
- de **sensibiliser les acteurs** au sein de de l'établissement à la protection des données à caractère personnel ;
- de constituer un **premier niveau de réponse et de conseil** sur les bonnes pratiques de protection des données à caractère personnel au sein de de l'établissement ;
- de contribuer à la **mise en œuvre des mesures** de protection des données ;
- d**'alerter le DPD** et le responsable de la mise en œuvre du traitement en cas de constatation d'une non-conformité.

4.2 Etape 2 - Cartographier vos traitements de données personnelles

Pour mesurer concrètement l'impact du règlement européen sur la protection des données, chaque établissement doit recenser de façon précise les traitements de données personnelles mis en œuvre et tenir un registre des traitements[6].

Dans le cadre de leur plan d'action pour se mettre en conformité au RGPD, chaque établissement doit tenir une **documentation interne complète** sur leurs traitements de données personnelles et s'assurer qu'ils respectent bien les nouvelles obligations légales.

Pour être en capacité de mesurer l'impact du règlement sur l'activité de l'établissement et de répondre à cette exigence, le correspondant - délégué à la protection des données doit recenser :

- Les différents traitements de données personnelles ;
- Les catégories de données personnelles traitées ;
- Les objectifs poursuivis par les opérations de traitements de données ;
- Les acteurs (*internes ou externes*) qui traitent ces données : identifier les prestataires sous-traitants afin d'actualiser les clauses de confidentialité ;

5 Annexe 3 – Modèle lettre de mission du correspondant - DPD

6 Annexe 4 – Exemple de registre de traitements

- Les flux en indiquant l'origine et la destination des données, afin notamment d'identifier les éventuels transferts de données hors de l'Union européenne.

Conformément à l'article 30 du RGPD, le registre comporte pour chaque traitement les informations suivantes :

- le nom et les coordonnées du responsable du traitement et de tout responsable conjoint du traitement, du représentant du responsable du traitement et du correspondant - délégué à la protection des données désigné ;
- les finalités du traitement ;
- une description des catégories de personnes concernées et des catégories de données à caractère personnel ;
- les catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées, y compris les destinataires dans des pays tiers ;
- dans quels pays les données sont éventuellement transférées ;
- dans la mesure du possible, les délais prévus pour l'effacement des différentes catégories de données ;
- dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles.

4.3 Etape 3 - Prioriser les actions à mener

Sur la base du registre des traitements, identifier les actions à mener pour se conformer aux obligations actuelles et à venir.

Prioriser ces actions au regard des risques que font peser les traitements sur les droits et les libertés des personnes concernées.

Points d'attention quels que soient les traitements

- S'assurer que **seules les données strictement nécessaires** à la finalité sont collectées et traitées.
- Identifier **le fondement juridique** sur lequel se fonde le traitement (*par exemple : consentement de la personne, intérêt légitime, contrat, obligation légale)*
- Réviser les **mentions d'information** afin qu'elles soient conformes aux exigences du règlement (*articles 12, 13 et 14 du règlement*) (***Exemple de modèle de mention d'information en annexe 3).***
- Vérifier que les **sous-traitants** connaissent leurs nouvelles obligations et leurs responsabilités (*clauses contractuelles rappelant les obligations du sous-traitant en matière de sécurité, de confidentialité et de protection des données personnelles traitées*) ***(cf- 3.3 et 3.10).***
- Prévoir les modalités d'exercice des **droits des personnes** concernées (*droit d'accès, de rectification, droit à la portabilité, retrait du consentement...)*
- Vérifier les **mesures de sécurité** mises en place ***(cf- 3.3).***

4.4 Etape 4 - Gérer les risques

Si des traitements de données personnelles susceptibles d'engendrer des risques élevés pour les droits et libertés des personnes concernées ont été identifiés, pour chacun de ces traitements, une

analyse d'impact sur la protection des données doit être menée (**Data protection impact assessment ou Privacy Impact Assessment).**

Une analyse d'impact sur la protection des données (PIA) est une étude aidant à construire des traitements de données respectueux de la vie privée et permettant de démontrer la conformité de son traitement au RGPD. Un PIA est un outil d'évaluation d'impact sur la vie privée.

Un PIA contient :

- Une description du traitement étudié et de ses finalités
- Une évaluation de la nécessité et de la proportionnalité des opérations de traitement au regard des finalités
- une évaluation des risques pour les droits et libertés des personnes concernées
- les mesures envisagées pour faire face aux risques

Le PIA doit être réalisé avant la mise en œuvre du traitement. C'est un processus itératif, les analyses doivent être revues et corrigées de manière régulière, en particulier lors de changements majeurs des modalités d'exécution du traitement.

Mener un PIA est obligatoire pour tout traitement susceptible d'engendrer des risques élevés pour les droits et libertés des personnes concernées (*Article 35 du RGPD*).

Pour déterminer si un traitement est susceptible d'engendrer des risques élevés, les 9 critères suivant sont définis dans les lignes directrices du G29 :

1. Evaluation ou notation;
2. Décision automatisée avec effet juridique ou effet similaire significatif;
3. Surveillance systématique ;
4. Données sensibles ou données à caractère hautement personnel ;
5. Données personnelles traitées à grande échelle ;
6. Croisement d'ensembles de données ;
7. Données concernant des personnes vulnérables ;
8. Usage innovant ou application de nouvelles solutions technologiques ou organisationnelles ;
9. Exclusion du bénéfice d'un droit, d'un service ou contrat.

Si le traitement rencontre au moins 2 de ces critères, alors il est vivement conseillé de faire un PIA.

Elaboration du PIA :

- **Le responsable de traitement** : valide le PIA et s'engage à mettre en œuvre le plan d'action défini dans le PIA ;
- **Le correspondant - délégué à la protection des données :** élabore le plan d'action et se charge de vérifier son exécution ;
- **Le(s) sous-traitant(s) :** fournit les informations nécessaires à l'élaboration du PIA ;
- **Les métiers** (SSI, maîtrise d'ouvrage, maîtrise d'œuvre) : aident à la réalisation du PIA en fournissant les éléments adéquats ;
- **Les personnes concernées** : donnent leurs avis sur le traitement.

La CNIL a élaboré une méthode et un catalogue de bonnes pratiques qui vous aident à mener un PIA et déterminer les mesures proportionnées aux risques identifiés.

Un logiciel PIA, en version Beta, facilite la formalisation de cette analyse. >Téléchargez l'outil PIA

4.5 Etape 5 - Organiser les processus internes

Pour garantir un haut niveau de protection des données personnelles en permanence, mettre en place des procédures internes qui garantissent la protection des données à tout moment, en prenant en compte l'ensemble des événements qui peuvent survenir au cours de la vie d'un traitement (*ex : faille de sécurité, gestion des demande de rectification ou d'accès, modification des données collectées, changement de prestataire*).

Organiser les processus implique notamment :

- **de prendre en compte de la protection des données personnelles dès la conception** d'une application ou d'un traitement (*minimisation de la collecte de données au regard de la finalité, cookies, durée de conservation, mentions d'information, recueil du consentement, sécurité et confidentialité des données s'assurer du rôle et de la responsabilité des acteurs impliqués dans la mise en œuvre de traitements de données*). Pour cela, s'appuyer sur les conseils du délégué à la protection des données;
- **de sensibiliser et d'organiser la remontée d'information** en construisant notamment un plan de formation et de communication auprès des agents ;
- **de traiter les réclamations et les demandes des personnes concernées quant à l'exercice de leurs droits** *(droits d'accès, de rectification, d'opposition, droit à la portabilité, retrait du consentement*) en définissant les acteurs et les modalités (*l'exercice des droits doit pouvoir se faire par voie électronique, si les données ont été collectées par ce moyen*) ;
- **d'anticiper les violations de données** en prévoyant, dans certains cas, la notification à l'autorité de protection des données dans les 72 heures et aux personnes concernées dans les meilleurs délais.

4.6 Etape 6 - Documenter la conformité

Pour prouver la conformité au règlement, constituer et regrouper la documentation nécessaire. Les actions et documents réalisés à chaque étape doivent être réexaminés et actualisés régulièrement pour assurer une protection des données en continu.

La documentation devra notamment comporter les éléments suivants :

<u>La documentation sur les traitements de données personnelles</u>

- Le registre des traitements (*pour les responsables de traitements*) ou des catégories d'activités de traitements (*pour les sous-traitants*)
- Les analyses d'impact sur la protection des données (PIA) pour les traitements susceptibles d'engendrer des risques élevés pour les droits et libertés des personnes

<u>L'information des personnes</u>

- Les mentions d'information
- Les modèles de recueil du consentement des personnes concernées
- Les procédures mises en place pour l'exercice des droits

<u>Les contrats qui définissent les rôles et les responsabilités des acteurs</u>

- Les contrats avec les sous-traitants
- Les procédures internes en cas de violations de données
- Les preuves que les personnes concernées ont donné leur consentement lorsque le traitement de leurs données repose sur cette base.

Annexe 1 – Modèle de clause de confidentialité dans le cadre d'un marché ou d'un contrat de sous-traitance

Les supports informatiques fournis par l'établissement et tous documents, de quelque nature qu'ils soient, résultant de leur traitement par le sous-traitant restent la propriété de l'établissement.

Conformément aux articles du Règlement Européen 2016-679 du 27 avril 2016, relatif à la protection des données à caractère personnel et de la Loi Informatique et Libertés modifiée, le sous-traitant s'engage à prendre toutes précautions utiles afin de préserver la sécurité des informations et notamment d'empêcher qu'elles ne soient déformées, endommagées ou communiquées à des personnes non autorisées.

Le sous-traitant s'engage donc à respecter, de façon absolue, les obligations suivantes et à les faire respecter par son personnel, c'est-à-dire à :

- Ne prendre aucune copie des données qui lui sont confiées, à l'exception de celles nécessaires à l'exécution du contrat, l'accord préalable du responsable de Traitement étant nécessaire,
- Ne pas utiliser les données traitées à des fins autres que celles limitativement spécifiées au contrat,
- Ne pas divulguer ces données à d'autres personnes, qu'il s'agisse de personnes privées ou publiques, physiques ou morales quelles qu'elles soient,
- Prendre toute mesures permettant d'éviter toute utilisation détournée ou frauduleuse des fichiers informatiques en cours d'exécution du contrat,
- prendre toutes les mesures, notamment de sécurité matérielle, pour assurer la conservation des documents et informations traités tout au long de la durée du présent contrat ;

Et en fin de contrat à :

- procéder à la destruction de tous les fichiers manuels ou informatisés stockant les informations saisies ; ou à :
- restituer intégralement les supports d'informations selon les modalités prévues au présent contrat.

Le sous-traitant s'engage à garantir la confidentialité des données à caractère personnel traitées et veiller à ce que les personnes autorisées à traiter les données à caractère personnel s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité.

Lorsque le sous-traitant recrute un autre sous-traitant pour mener des activités de traitement spécifiques pour le compte du responsable du traitement, les mêmes obligations en matière de protection de données que celles fixées dans le présent marché entre le responsable du traitement et le Titulaire, sont imposées à ce sous-traitant par contrat ou au moyen d'un autre acte juridique au titre du droit de l'Union ou du droit d'un État membre, en particulier pour ce qui est de présenter des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du RGPD. Lorsque ce sous-traitant ne remplit pas ses obligations en matière de protection des données, le soumissionnaire demeure pleinement responsable devant le responsable du traitement de l'exécution par le sous-traitant de ses obligations.

Annexe 2 – Exemple de mention ou note d'information

L'AEFE propose un modèle de mention ou note d'information à adapter selon le traitement.

La mention d'information doit indiquer :

- de la finalité poursuivie par le traitement
- du caractère obligatoire ou facultatif des réponses
- des conséquences d'un défaut de réponse
- de l'identité du responsable du traitement
- des destinataires ou catégorie de destinataires des données
- de leurs droits (*droit à l'information, d'accès et de rectification, droit d'opposition, droit à l'effacement, droit à la portabilité, à la limitation*)
- la durée de conservation (*obligation du Règlement Européen*)
- le cas échéant, des transferts de données vers des pays hors UE.

Modèle de de mention d'information à porter sur les formulaires de collecte :

En application des articles 12 et 13 du Règlement Européen 2016-679 du 27 avril 2016, relatif à la protection des données à caractère personnel et de la Loi Informatique et Libertés modifiée, nous vous informons que A COMPLETER (l'établissement) en sa qualité de Responsable de Traitement collecte des données vous concernant à des fins de A COMPLETER.

Vos données seront strictement réservées à A COMPLETER et aux services habilités et seront conservées A COMPLETER. Aux termes de notre Politique de protection des données, nous nous engageons à protéger vos données de toute atteinte. Conformément aux art.15 à 22 du Règlement Européen 2016-679 du 27 avril 2016, relatif à la protection des données à caractère personnel , vous pourrez demander à tout moment et gratuitement à accéder aux données vous concernant, à les rectifier ou à les effacer, auprès de A COMPLETER ou à la CNIL en l'absence de réponse satisfaisante dans le délai d'un mois. L'agent pourra également s'opposer au traitement le concernant pour des motifs légitimes.

Modèle de de mention d'information à porter sur les dossiers d'inscription des élèves :

En application des articles 12 et 13 du Règlement Européen 2016-679 du 27 avril 2016, relatif à la protection des données à caractère personnel et de la Loi Informatique et Libertés modifiée, nous vous informons que A COMPLETER (le lycée) en sa qualité de Responsable de Traitement collecte des données vous concernant à des ***fins de gestion administrative et pédagogique des élèves et établir des statistiques.***

Vos données seront strictement réservées à A COMPLETER et aux services habilités et seront conservées A COMPLETER. Aux termes de notre Politique de protection des données, nous nous engageons à protéger vos données de toute atteinte. Conformément aux art.15 à 22 du Règlement Européen 2016-679 du 27 avril 2016, relatif à la protection des données à caractère personnel , vous pourrez demander à tout moment et gratuitement à accéder aux données vous concernant, à les rectifier ou à les effacer, auprès de A COMPLETER ou à la CNIL en l'absence de réponse satisfaisante dans le délai d'un mois. L'agent pourra également s'opposer au traitement le concernant pour des motifs légitimes.

Annexe 3 – Modèle lettre de mission du Correspondant - DPD

L'Etablissement (**A COMPLETER)** vous a désigné en tant que Correspondant - Délégué à la protection des données (DPD) au titre du règlement (UE) 2016/678 du 27 avril 2016 le (**JJ/MM/AAAA**).

Cette désignation prendra effet à compter du (**A COMPLETER)**.

Vous exercez vos missions pour tous les traitements mis en œuvre par l'établissement (**A COMPLETER)**.

Par la présente, je vous précise quelles sont vos missions en tant que Correspondant – DPD :

- informer et conseiller sur les obligations qui incombent à l'établissement en vertu du RGPD et d'autres dispositions en matière de protection de données à caractère personnel ;
- si besoin, informer des manquements constatés, conseiller dans les mesures à prendre pour y remédier, soumettre les arbitrages nécessaires ;
- permettre de démontrer que les traitements sont effectués conformément au RGPD, et si besoin, réexaminer et actualiser ces mesures ;
- veiller à la mise en œuvre de mesures appropriées pour veiller à la bonne application du principe de protection des données dès la conception et par défaut dans tous les projets comportant un traitement de données personnelles ;
- piloter la production et la mise en œuvre de politiques, de lignes directrices, de procédures et de règles de contrôle pour une protection efficace des données personnelles et de la vie privée des personnes concernées ;
- assurer la bonne gestion des demandes d'exercice de droits, de réclamations et de requêtes formulées par des personnes concernées par les traitements, assurer de leur transmission aux services intéressés et apporter à ces derniers un conseil dans la réponse à fournir aux requérants ;
- alerter le DPD et le responsable de la mise en œuvre du traitement en cas de constatation d'une non-conformité ;
- communiquer au DPD les éventuelles violations de données ;
- tenir l'inventaire et documenter les traitements de données à caractère personnel en tenant compte du risque associé à chacun d'entre eux compte tenu de sa nature, sa portée, du contexte et de sa finalité ;
- présenter un bilan annuel des activités au DPD.

Pour vous permettre de mener à bien ces différentes missions, l'établissement s'engage à :

- ce que vous soyez associé, d'une manière appropriée et en temps utile, à toutes les questions relatives à la protection des données ;
- vous aider à exercer vos missions en :
    - vous fournissant les ressources et moyens qui vous sont nécessaires ;
    - vous fournissant l'accès aux données et aux opérations de traitement ;
    - vous fournissant les formations afin d'entretenir vos connaissances spécialisées et de vous tenir informé des meilleures pratiques propres à votre métier.
- veiller à ce que vos éventuelles autres missions et tâches n'entrainent pas de conflit d'intérêts avec celles relatives à votre qualité de Correspondant – DPD ;
- donner une importance prépondérante à vos analyses et conseils en matière de protection des données personnelles et, dans le cas où vos recommandations ne seraient pas retenues, à en documenter les raisons ;

- s’assurer de votre accord avant mise en production de tout nouveau traitement comportant des données personnelles.

En fin de mission, vous vous engagez à me remettre à l’établissement tous les éléments relatifs à votre mission et, dans la mesure du temps dont vous disposerez à cet effet, à informer votre éventuel successeur sur les travaux en cours.

Je vous rappelle que vous êtes soumis au secret professionnel en ce qui concerne l’exercice de vos missions.

Annexe 4 – Exemple de registre des traitements

Pour faciliter la tenue du registre, l'AEFE propose un modèle de registre de base destiné à répondre aux besoins les plus courants en matière de traitements de données.

Ce document vise à recenser les traitements de données personnelles mis en œuvre dans votre établissement en tant que responsable de traitement. Centralisé et régulièrement mis à jour, il vous permet de répondre à l'obligation de tenir un registre prévue par le RGPD.

Composition du document

Nom du traitement	
Date de mise en œuvre :	
Date de dernière mise à jour :	
Finalité principale :	
Détail des finalités du traitement	Décrire précisément la finalité du traitement
Service chargé de la mise en œuvre	
Fonction de la personne ou du service auprès duquel s'exerce le droit d'accès	
Catégories de personnes concernées par le traitement	Lister les différents types de personnes dont vous collectez ou utilisez les données *Exemple : élèves personnels, parents ….*
Catégories des données collectées	Lister les différentes données traitées *Exemple : données d'identifications, professionnelles …*
Catégories de destinataires des données	Destinataire interne (*catégorie de personnes habilitées, service …)* et externe (*partenaire…)*

Durée de conservation des données	Si vous ne pouvez pas indiquer une durée chiffrée, précisez les critères utilisés pour déterminer le délai d'effacement.
Transfert des données hors UE	Des données sont-elles transmises hors de l'UE ? Si oui vers quels pays ?
Mesures de sécurité	Décrire les mesures de sécurité organisationnelles et techniques prévues pour préserver la confidentialité des données. Le niveau de sécurité doit être adapté aux risques soulevés par le traitement. Les exemples suivants constituent des garanties de base à prévoir et peuvent devoir être complétés. ☐ Contrôle d'accès des utilisateurs Décrivez les mesures : ☐ Mesures de traçabilité Précisez la nature des traces (*exemple : journalisation des accès des utilisateurs*), les données enregistrées (*exemple : identifiant, date et heure de connexion, etc.)* et leur durée de conservation : ☐ Mesures de protection des logiciels (*antivirus, mises à jour et correctifs de sécurité, tests, etc.)* Décrivez les mesures : ☐ Sauvegarde des données Décrivez les modalités : ☐ Contrôle des sous-traitants Décrivez les modalités :