POLITIQUE GENERALE DE PROTECTION DES DONNEES A CARACTERE PERSONNEL DE L'AGENCE POUR L'ENSEIGNEMENT FRANÇAIS A L'ETRANGER

Préambule

L'Agence pour l'enseignement français à l'étranger (AEFE) est particulièrement attachée au respect de la vie et de la protection des données à caractère personnel.

L'AEFE a élaboré une politique en matière de protection des données à caractère personnel, afin de se conformer à la réglementation applicable, et notamment au règlement n° 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation des données (*règlement général sur la protection des données – RGPD).*

Cette politique de protection des données (ci-après la « *Politique de Protection des Données* ») a pour objectif de vous informer sur les engagements pris par l'AEFE afin de veiller au respect de vos données à caractère personnel.

Sommaire

I. Périmètre

1.1 Objet :

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

La collecte, le traitement et la communication des données à caractère personnel sont encadrés par le Règlement Général sur la Protection des Données (RGPD UE 2016/679) et dans la continuité de la Loi Informatique et Libertés du 6 janvier 1978 modifiée (*LOI n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles).*

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 :

Cette Politique générale de Protection des Données s'applique à tous les traitements de données à caractère personnel, mis en œuvre par l'AEFE, en tant que Responsable de traitement.

1.3 Définitions :

Données à caractère personnel : 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.

Destinataire : la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données à caractère personnel, qu'il s'agisse ou non d'un tiers.

Responsable du traitement : la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement.

Traitement : toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction.

Sous-traitant : la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement.

II. Principes généraux applicables

L'AEFE applique les principes suivants :

2.1 Principe de 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 ;
c) le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis ;
d) le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique ;
e) le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement ;
f) le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant.

2.2 Délai de conservation des données :

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.

2.3 Principe de Transparence :

Fondement juridique : Loi Informatique et Libertés du 6 janvier 1978 modifiée Section 1 Art.32 et RGPD Chapitre III art.12 : Obligations incombant aux Responsables de Traitements et aux Sous-traitants.

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

La loi impose que « ***les données [soient] collectées et traitées de manière loyale et licite*** » (article 6), dictant ainsi au responsable du traitement un principe de transparence lors du traitement.

La Loi et le Règlement imposent d'informer les personnes de la mise en œuvre des traitements de données à caractère personnel.

2.4 Obligation d'information des personnes :

Fondement juridique : Loi Informatique et Libertés du 6 janvier 1978 modifiée Section 1 Art.32 et RGPD Chapitre III art.12 : Obligations incombant aux Responsables de Traitements et aux Sous-traitants.

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

- 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.

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.

2.5 Consentement des personnes :

a) Le consentement

Fondement juridique : Loi Informatique et Libertés du 6 janvier 1978 modifiée article 7 et RGPD article 7.

Le traitement est licite (*sans consentement*) s'il est fondé sur une base juridique : ainsi, 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 qu'elle met en œuvre concerne dans sa grande majorité des personnes mineures : le suivi de la scolarité conformément au code de l'éducation français mais aussi la mise à disposition d'un réseau social AGORA sur le WEB.
L'article 8. du RGPD présente les conditions applicables au consentement des enfants en ce qui concerne les services de la société de l'information.

Lorsque l'article 6 relatif au consentement s'applique, en ce qui concerne l'offre directe de services de la société de l'information aux enfants, 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.

2.6 Principe de Légalité :

Les données « *sont collectées pour des finalités **déterminées**, **explicites** et **légitimes** et ne sont pas traitées ultérieurement de manière incompatible avec ces finalités* » (LIL, Art. 6-2°).
Le RGPD confirme ce principe par son Art.5.

Les données à caractère personnel doivent être :
a) traitées de manière licite, loyale et transparente au regard de la personne concernée *(licéité, loyauté, transparence) ;*
b) collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités ; le traitement ultérieur à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques n'est pas considéré, conformément à l'article 89, paragraphe 1 [*Archives – Minimisation des données, pseudonymisation*], 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*).

2.7 Principe du rendu-compte (ou «Accountability ») :

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.

2.8 Principe du Droit à « l'Oubli » ou à l'effacement :

Fondement juridique : Loi Informatique et Libertés du 6 janvier 1978 modifiée article 6-5° et RGPD article 5.1e).

L'article 6-5° de la loi impose que les données à caractère personnel sont conservées sous une forme permettant l'identification des personnes concernées pendant une durée qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées.

L'article 5.1e) du Règlement reprend cette formulation :

- 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;
- Comme dans la plupart des organisations, l'obligation de fixer et de respecter une durée de conservation est méconnue ; elle n'est donc pas intégrée dans les réflexes des responsables d'application – et donc n'est pas intégrée dans le système d'information.
- Cette obligation est fixée par l'article 6 de la loi Informatique et Libertés et l'art. 5 du RGPD; elle est systématiquement vérifiée par la CNIL lors de ses contrôles, en particulier par l'exécution de requêtes SQL sur les bases de production, incluant les dates de clôture des contrats.

2.9 Principe de Pertinence des données :

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

La CNIL s'appuie dès à présent sur une disposition similaire de la Loi pour contrôler les données **im-**pertinentes telles que les jugements de valeurs, les insultes ou les appréciations sur les personnes.

2.10 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).*

2.11 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* ». A ce jour, la Commission européenne a pris plusieurs décisions dans ce sens.

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 :

- la personne à laquelle se rapportent les données *a consenti expressément* à leur transfert ou si le transfert est nécessaire à l'une des conditions suivantes :

1° A la sauvegarde de la vie de cette personne ;
2° A la sauvegarde de l'intérêt public ;
3° Au respect d'obligations permettant d'assurer la constatation, l'exercice ou la défense d'un droit en justice ;
4° A 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 ;
5° A 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 ;
6° A 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.

2.12 Principe de sécurité des données :

Fondement juridique : Loi Informatique et Libertés du 6 janvier 1978 modifiée article 34 et RGPD article 32.

L'article 34 de la loi « *Informatique et Libertés* » et l'article 32 du RGPD imposent 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.

Le responsable de traitement doit mettre en œuvre des 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.

Le responsable du traitement et le sous-traitant prennent des mesures afin de garantir que toute personne physique agissant sous l'autorité du responsable du traitement ou sous celle du sous-traitant, qui a accès à des données à caractère personnel, ne les traite pas, excepté sur instruction du responsable du traitement, à moins d'y être obligée par le droit de l'Union ou le droit d'un État membre.

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

La CNIL précise que des mesures générales de sécurité nécessaires doivent être prises « *préalablement à toute mise en œuvre d'une application informatique* » et en tenant compte « *de la finalité du traitement, du volume des informations traitées et de leur degré de sensibilité au regard des risques d'atteinte à la personne humaine* ». À ce titre, elle 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* ».

2.13 Analyses d'impact relative à la protection des données (AIPD – PIA) :

En vertu de l'article 35 du RGPD, lorsqu'un type de traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement doit effectuer, avant toute mise en œuvre, une analyse d'impact.

L'AEFE mettra en œuvre une analyse d'impact :
- si elle effectue un traitement de données à grande échelle (*considérant les opérations de traitement à grande échelle qui visent à traiter un volume considérable de données à caractère personnel pouvant affecter un nombre important de personnes concernée*) ;
- si les traitements mis en œuvre répondent à certaines caractéristiques.

En effet, dès lors qu'il répondra à plus de deux des neuf critères déterminés par la CNIL et par le G29 (*collecte de données sensibles ; collecte de données à caractère personnel à large échelle ; croisement de données ; personnes vulnérables ; usage innovant ; exclusion du bénéfice d'un droit / contrat*), le traitement sera, par principe, soumis à analyse d'impact.

Sur ce point, l'AEFE prend connaissance des « *lignes directrices* » sur les AIPD et les traitements susceptibles d'engendrer des risques :
https://www.cnil.fr/sites/default/files/atoms/files/wp248_rev.01_fr.pdf

S'il met en place une analyse d'impact, l'AEFE utilise le logiciel open source PIA facilitant la conduite et la formalisation d'analyses d'impact sur la protection des données telles prévues par le RGPD : https://www.cnil.fr/fr/outil-pia-nouvelle-version-beta-du-logiciel

2.14 Tenue d'un registre des activités de traitement :

L'AEFE tient un registre des différents traitements de données à caractère personnel mis en œuvre sous sa responsabilité.

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 délégué à la protection des données éventuellement 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 ;
- le cas échéant, les transferts de données vers un pays tiers ou à une organisation internationale, y compris leur identification respective et, dans le cas des transferts vers des pays ne bénéficiant pas d'un niveau de protection adéquat, les documents attestant l'existence de garanties appropriées ;
- 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.

2.15 Nomination d'un délégué à la protection des données (DPD) :

L'AEFE a nommé un DPD le 24 mai 2018, cette désignation a fait l'objet d'une information auprès de la Commission nationale informatique et libertés (CNIL) sous le numéro : DPO-22304.

Le cadre des fonctions du délégué est fixé par le règlement qui dispose :

- qu'il est associé de manière appropriée et en temps utile, à toutes les questions relatives à la protection des données ;
- que lui sont fournies les ressources nécessaires à l'exercice de ses missions et l'entretien de ses connaissances ;
- qu'il peut accéder aux données et aux opérations de traitement ;
- qu'il ne reçoit aucune instruction en ce qui concerne l'exercice de ses missions et ne peut être relevé de ses fonctions ou pénalisé pour l'exercice de ses missions ;

- qu'il rapporte directement à l'instance de direction ;
- qu'il peut être directement contacté par les personnes concernées par les traitements ;
- qu'il est soumis à une obligation de confidentialité ;
- qu'il ne peut exercer d'autres misions ou tâches susceptibles d'entraîner un conflit d'intérêts.

Missions du délégué à la protection des données :

- Missions d'information et conseil :

Le DPD, avec l'appui de la Direction des Ressources humaines et du service communication et évènementiels, contribue à mettre en place des actions d'information et de formation des collaborateurs de l'AEFE afin de favoriser une culture de la protection des données à caractère personnel et de permettre l'acquisition de compétences spécifiques dans les activités où elles sont utiles.

Il apporte un conseil aux Directions pour la mise en œuvre de traitements de données à caractère personnel que ce soit dans le cadre de projets d'évolution des systèmes d'information ou d'opérations de toutes natures impliquant la collecte, le transfert ou l'utilisation de données à caractère personnel.

Il conduit ou intervient pour avis dans les analyses d'impacts relatives à la protection des données.

- Missions de contrôle :

Il contrôle l'application des dispositions réglementaires en matière de protection des données à caractère personnel par les structures de l'Agence et ses sous-traitants, notamment en s'appuyant sur les fonctions d'audit et de contrôle interne en place.

Il est autorisé à prendre toute initiative pour conduire les vérifications, et les directions contrôlées coopèrent à leur réalisation.

Il rend compte des résultats des contrôles aux responsables concernés et à la Direction générale.

- Missions d'interlocuteur de l'autorité de contrôle :

Le DPD est désigné auprès de l'autorité de contrôle, avec laquelle il coopère, il est le point de contact de cette dernière y compris pour les consultations préalables à la mise en œuvre de traitements à risques pour les personnes.

Il instruit les réclamations des personnes et coopère avec la CNIL dans le cadre de l'instruction des plaintes reçues par l'autorité.

III. Vos droits concernant le traitement de vos données à caractère personnel

Conformément au RGPD, vous disposez sur vos données des droit d'accès, droit de rectification, droit à l'effacement (*droit à l'oubli*), droit d'opposition, droit à la limitation du traitement, droit à la portabilité.

3.1 Le droit d'accès, de rectification ou de suppression :

Vous pouvez demander à tout moment l'accès aux données à caractère personnel vous concernant et aussi des informations relatives à leur traitement (*comme par exemple les catégories de données traitées*). Ce droit vous permet aussi de demander de vous communiquer l'intégralité de ces données.

Vous disposez également du droit de modifier ou de retirer, à tout moment, les consentements que vous nous avez accordés pour le traitement de vos données à caractère personnel.

3.2 Le droit d'opposition et à la portabilité de vos données :

Vous disposez du droit de vous opposer à un traitement de vos données à caractère personnel et du droit à leur portabilité, dans les conditions fixées par la Réglementation.

3.3 Votre droit à la limitation des traitements de données :

Vous pouvez demander la limitation du traitement de vos données personnelles dans les conditions fixées par la Réglementation.

3.4 Les modalités d'exercice de vos droits :

Vous pouvez exercer l'ensemble de ces droits auprès du Délégué à la Protection des Données (ou - Data Protection Officer) par courrier électronique à l'adresse e-mail suivante : rgpd@lycee-chateaubriand.eu

Dans ce cadre, nous vous prions de bien vouloir accompagner votre demande des éléments nécessaires à votre identification (*nom, prénom, email*) ainsi que toute autre information nécessaire à la confirmation de votre identité.

IV. Suivi de la politique de protection des données à caractère personnel

La présente politique, accessible à tous sur le site internet de l'AEFE, est actualisée régulièrement pour prendre en compte les évolutions législatives et réglementaires, et tout changement dans l'organisation de l'AEFE.