PROCEDURE NOTIFICATION EN CAS DE VIOLATION DES DONNEES A CARACTERE PERSONNEL

En cas de violation de sécurité concernant des données à caractère personnel (perte, modification, accès ou divulgation non autorisée … de données élèves, anciens élèves, parents élèves, personnels agence …), les articles 33 et 34 du règlement européen relatif à la protection des données à caractère personnel du 27 avril 2016 imposent à l'AEFE, en sa qualité de Responsable de traitement d'informer :

1/ la Commission Nationale Informatique et Libertés (CNIL) sous 72h maximum sauf exception,

2/ les personnes concernées (*élèves, anciens élèves, parents élèves, personnels agence, personnels réseau, partenaires institutionnels…)* individuellement et rapidement, si le risque pour leur vie privée est élevé.

Procédure à appliquer

Tâches	Responsable	Description	Points de vigilance	Règles et Moyens
1. Signaler immédiatement toute perte, destruction, modification ou divulgation non autorisée de données à caractère personnel	Agent ou toute personne constatant la violation	Signaler l'incident sans délai par : envoi formulaire spécifique au DPP/ téléphone ou tout autre moyen	Ne pas dépasser 24 heures	Gestion des incidents Vie Privée (formulaire CNIL)
2. Identifier la nature de la violation de sécurité	DPD / SSI / Service concerné	Consigner la date et l'heure de l'incident : tracer et horodater l'envoi de la déclaration interne de l'incident, identifier la nature de la violation : perte, destruction, modification, divulgation, fuite ou autre	Ne pas confondre les natures de violation (Faille, Incident technique, Causes extérieures?)	Gestion des failles de Sécurité Informatique et Gestion des incidents Vie Privée (formulaire CNIL)
3. Identifier les données compromises et les catégories de personnes concernées.	DPD / SSI / Service ou salarié ayant découvert la faille	Identifier la nature des données : volume et nombre approximatif de personnes concernées - identifier le(s) type(s) de personnes concernées : élèves, anciens élèves, parents d'élèves		

4. Analyser les données compromises.	DPD	Analyser la nature des données et leurs sensibilité pour les personnes concernées / Vérifier si existence d'une PIA /		Analyse du DPO de l'incident en référence aux EIVP existantes (Catalogue des Incidents Vie Privée et mesures correctives)
5. Évaluer le risque : mesures techniques et d'organisation	DPD / SSI	Si destruction ou altération : vérifier s'il existe un back-up et si oui, s'il fonctionne - Si divulgation ou accès non autorisé : vérifier si les données sont compréhensibles pour l'auteur de la violation, ou s'il est encore possible de les rendre incompréhensibles, de les détruire à distance, ou de pister leur exploitation / duplication.		
6. Si possible : prendre des mesures de réduction ou de limitation du risque	DPD / SSI	Si destruction ou altération : reconstituer les données. - Si divulgation ou accès non autorisé : prendre toute mesure possible pour rendre les données illisibles, les détruire, ou en pister l'utilisation.	Mesures à prendre le plus tôt possible pour qu'elles puissent être efficaces.	

7. Évaluer le risque : vie privée	DPD	Analyser les risques et l'impact sur la vie privée des personnes concernées, Prendre en considération les mesures de sécurité et de réduction du risque, utiliser une échelle de 1 (aucun risque) à 4 (risque très élevé) pour caractériser la gravité de l'incident (après mesures de réduction du risque), mettre à jour le Registre des Incidents Vie Privée et mesures correctives si nouveaux risques identifiés et évalués.	Les mesures prises conformément au point 6 peuvent n'avoir aucun impact sur l'évaluation du risque pour la vie privée si elles sont prises tardivement. Le niveau de risque final s'entend après avoir évalué les mesures de sécurité et de réduction du risque (points 5 et 6).	
8. Si un risque est identifié (échelle 2 à 4) : Notifier à la CNIL dans les meilleurs délais et sous 72h au plus tard d'une violation de données à caractère personnel.	DPD	Décrire la nature de la violation y compris les catégories de personnes concernées + leur nombre approximatif. - Mentionner les coordonnées du DPO - Décrire les conséquences probables de la violation. - Décrire les mesures de sécurité et de limitation / réduction du risque (points 5 et 6 ci-dessus).		

9. Si un risque élevé est possible (échelle 3 et 4) Informer le plus tôt possible les personnes concernées et impactées par la divulgation de leurs données.	Service habilité (DPD, SSI, Service communication)	Informer les personnes concernées individuellement de la divulgation de leurs données le plus tôt possible en indiquant : - la nature de la violation et ses conséquences probables. - les mesures de sécurité ou de réduction du risque prises ou prévues. - les coordonnées du DPD		
10. Consigner les actions correctives suite à l'incident	DPD	Identifier et consigner les mesures correctives tout au long de la gestion de l'incident		
11. Former et sensibiliser les agents AEFE	Service habilité (DPD, service Formation)	Organiser des sessions de formation ou de sensibilisation des utilisateurs		

Précautions

Prévenir sans délai le DPD dès la découverte de la violation.

Horodater et tracer la date/heure de la découverte de la violation en précisant sa nature et sa portée.