MINISTÈRE
DE L'ÉDUCATION
NATIONALE
ET DE LA JEUNESSE

Liberté
Égalité
Fraternité

Guide « Gestion des incidents »

Document d'accompagnement du kit sécurité des systèmes d'information pour les espaces numériques de travail

ENT

Espace numérique de travail

Document d'accompagnement
version 1.0
Juin 2022

Direction du numérique pour l'éducation – bureau SN1

Table des matières

1. Introduction

1.1. Avant-propos

Dans le cadre du déploiement et de la mise en œuvre des espaces numériques de travail dans le 1er et 2ème degré de l'enseignement scolaire, le ministère de l'Éducation nationale a élaboré un schéma directeur des espaces numériques de travail (SDET) dont l'objectif est de fournir un cadre de cohérence national pour les projets ENT et d'orienter l'offre de solutions ENT.

Le SDET pose « les principes directeurs de l'élaboration et de la mise en œuvre d'une solution ENT en partenariat avec les collectivités territoriales qui les financent et les académies qui assurent l'accompagnement des utilisateurs ».

Dans cette volonté d'accompagner les partenaires et acteurs, l'Éducation nationale propose un ensemble de guides thématiques portant sur la sécurité des espaces numériques de travail à destination des différents acteurs conçu comme un cadre de référence commun.

Ce kit SSI est proposé dans un contexte de sécurisation nécessaire et pour répondre tout à la fois aux exigences sociales des usagers et à la réglementation en termes de protection des données ou de continuité pédagogique.

1.2. Présentation du KIT SSI pour les ENT

Le Kit SSI pour les ENT est un ensemble de guides pratiques qui recouvrent les domaines suivants :

- La gouvernance de la sécurité des systèmes d'information
- La sous-traitance
- La mise en œuvre des téléservices
- La gestion des incidents

Il a pour objectifs :

- d'outiller les porteurs de projets ENT dans la mise en œuvre de la politique de sécurité tout au long du cycle de vie des ENT. En particulier, les guides prescrivent un ensemble de recommandations pour répondre à la réglementation et aux principes de la gestion de risque, aussi bien en phase de déploiement, d'utilisation ou d'évolution de l'ENT ;
- de fournir un cadre commun de références aux acteurs, partenaires et sous-traitants en rappelant en particulier les règles auxquelles se conforme l'Éducation nationale ;
- de répondre de façon simple et non ambiguë aux différentes situations et problèmes qui peuvent se poser aux responsables et acteurs des ENT.

Dans la continuité des guides proposés par l'ANSSI, en particulier le guide à destination de collectivités territoriales, ce kit SSI vise de façon plus générale à :

- *donner confiance aux usagers dans l'utilisation des services numériques;*
- *garantir la sécurité des données à caractère personnel conformément à la réglementation;*
- *appuyer la transformation numérique des administrations de l'État ;*
- *renforcer la sécurité des acteurs critiques pour l'État.*

1.3.Présentation du guide gestion des incidents

Le présent guide couvre le domaine de la gestion des incidents depuis l'élaboration de l'appel d'offre jusqu'à l'exploitation de l'ENT. Il est conçu comme un ensemble de recommandations ou règles qui rappellent les exigences réglementaires en particulier dans le champ de la protection des données à caractère personnel, ainsi que l'organisation, le rôle et missions des différents acteurs et leur articulation.

Pour cela le guide précise :

- Les objectifs détaillés de la gestion des incidents dans le cadre des ENT ;
- Le périmètre et les contraintes ;
- Les acteurs avec leur rôle et missions
- Un ensemble de recommandations qui constitue le corpus des règles applicables.

2. Objectifs détaillés

2.1. Objectifs détaillés du guide

Les objectifs sont détaillés ci-après avec un n° d'occurrence qui ne présume ni de l'importance ni de l'ordonnancement de l'objectif.

Objectif n°1 : définir dès en amont dans les appels d'offre les pré requis nécessaires à une gestion des incidents respectant les bonnes pratiques, les obligations réglementaires et les exigences que pourraient avoir les autorités de contrôle que sont la CNIL ou l'ANSSI en cas d'incident.

Objectif n°2 : préciser l'organisation préalable qui doit exister en matière de gestion des incidents, conformément à la réglementation, à l'organisation de l'État en région, et au principe de libre administration des collectivités territoriales.

Objectif n° 3 : rappeler le rôle et les missions de différents acteurs dans le contexte d'une gestion d'incidents ainsi que les champs réglementaires auxquelles ils se rapportent.

Objectif n° 4 : rappeler les obligations réglementaires en matière de notification d'incident, d'information des personnes et de collaboration entre les acteurs.

Objectif n° 5 : définir les règles générales en matière de gestion des incidents (déclaration à l'autorité de contrôle, devoirs des acteurs, communication, mesures conservatoires).

Objectif n°6 : expliciter l'articulation des différents acteurs en termes d'échanges ou d'obtention d'information.

Objectif n° 7 : capitaliser sur les incidents.

2.2. Ce qu'est ce guide

Ce guide fournit dans le contexte particulier de la gestion des incidents au sein des ENT un ensemble de recommandations à destination des acteurs. Ces recommandations qui ont une valeur de prescription pour les acteurs de l'Éducation nationale et de référence pour les collectivités territoriales, fixent également les obligations des sous-traitants et les exigences attendues pour ces derniers.

Ces recommandations précisent sous forme de règles ce que peuvent faire les acteurs pour répondre, anticiper, gérer un incident dans le respect de la réglementation et des bonnes pratiques.

2.3. Ce que n'est pas ce guide

Ce guide n'est pas un catalogue de mesures techniques ou organisationnelles qui s'imposeraient à chacun des acteurs. Il ne se substitue en rien aux procédures ou processus mis en œuvre par les académies ou par les collectivités territoriales dans le cadre du principe de libre administration des collectivités territoriales.

Par exemple, en cas de violation de données à caractère personnel au sein d'un établissement, le guide précise des règles en matière de notification de l'incident. Il indique que le chef d'établissement, en sa qualité de responsable de traitement, est également responsable de notification qui doit se faire dans les 72 heures où l'incident a été détecté. Le guide précise qu'en pratique le chef d'établissement déclare l'incident au DPD qui en assurera la notification à la CNIL.

De façon générale dans la mesure ou les DCP sont des DCP élèves ou d'enseignants , le DPD sollicité sera le DPD de l'académie. Dans les cas où la violation de DCP affecterait des personnes relevant de l'autorité des collectivités territoriales, le DPD sollicité sera celui de la collectivité.

Par contre, le guide ne fournit aucune procédure qui expliciterait l'organisation ou les procédures qui relèvent des acteurs de terrain même s'il rappelle la nécessité de leur existence.

3. Contexte

3.1. Périmètre

Le périmètre de la gestion des incidents couvre l'ensemble des ENT du 1er et 2ème degré de l'enseignement scolaire.

Les utilisateurs ou ayant droits de l'ENT sont :

- Les élèves de l'établissement scolaire ;
- Les parents d'élèves ou responsables légaux ;
- Les enseignants ;
- Le personnel de la vie scolaire ;
- Le personnel de direction ;
- Les administrateurs de l'ENT ;
- D'autres personnes dûment autorisées comme du personnel informatique de l'académie, de la collectivité territoriale ou du sous-traitant.

Le document est applicable quelle que soit la configuration de l'organisation pour opérer l'ENT qui peut être de la responsabilité :

- D'une collectivité territoriale ;
- D'un établissement public de coopération communale ;
- D'une académie ou région académique ;
- D'un groupement d'intérêt public ;
- D'un éditeur ou tout autre prestataire privé.

Pour les établissements d'enseignements relevant d'une double tutelle (agricole, militaire, maritime…), la répartition des responsabilités entre collectivités et administration de l'état reste inchangée. Les implications de la double tutelle feront l'objet de précisions ultérieures mentionnées dans les conventions.

Le guide aborde les domaines suivants de la gestion des incidents que sont

- Les prérequis dans les appels d'offre et en termes d'organisation ;
- La mise en œuvre de mesures conservatoires ;
- La notification des incidents et la communication en direction des usagers ou utilisateurs ;

- L'activation et la collaboration des chaînes d'alertes ;
- La communication et l'exploitation des logs ;
- La prise de décision ;
- Le dépôt de plainte.

3.2. Événements redoutés

Voici une liste non exhaustive d'événements redoutés correspondant à autant d'incidents de sécurité pris en compte dans le guide :

Nature	Événement redoutés
Indisponibilité ou déni de service	Indisponibilité de l'ENT pour une durée supérieure à un délai maximal acceptable ayant un impact sur les enseignements, les élèves, les parents ou les enseignants. Ces incidents portent atteinte aux enseignements, impact sur l'organisation, altération de l'image de marque.
	Indisponibilité partielle de l'ENT sur une des valeurs métiers de l'ENT
	Altération de la qualité de service en raison d'un déni de service
Contenu illicite ou choquant	Défiguration de l'ENT de l'établissement ou du portail du porteur d'ENT (contenu illicite, choquant, …) avec un impact social ou médiatique
	Dépôt de contenu illicite, choquant ou non conforme à la charte établissement
Présence d'un zéro day	Vulnérabilité critique sans correctif pouvant porter atteinte à la confidentialité ou à l'intégrité des données contenues dans l'ENT.
Violation de données à caractère personnel	Cyberattaque provoquant une divulgation massive de données élèves et enseignants.
	Altération ou divulgation limitées de données à caractère d'incident
Usurpation d'identité	Vol de login et mot de passe d'un chef d'établissement par une personne malveillante afin de porter atteinte à l'ENT.
	Vol de login et mot de passe pour modifier les notes avec un impact sur la vie scolaire
	Vol de login et mot de passe d'un élève ou d'un enseignant pour envoyer pour déposer des contenus choquants ou envoyez des insultes, messages diffamatoires ou calomnieux
	Compromission du compte de l'administrateur de l'ENT entraînant la compromission totale de l'ENT

Nature	Événement redoutés
Détournement d'usage	Détournement d'usage pour localiser un ou des élèves de l'ENT
	Détournement d'usage pour envoyer des messages contraires à la charte
Défaillance du sous-traitant	Disparition de l'éditeur ou rupture du contrat avec l'éditeur
	Compromission de toute ou partie de l'infrastructure du sous-traitant
	Non-respect des dispositions contractuelles entraînant une potentielle violation des DCP

4. Acteurs : rôle de chaque acteur et actions attendues

4.1. Chef d'établissement

Action(s) à mener	Responsabilité(s)
Déclarer la suspicion d'incident au RSSI ou au DPD (académie ou région académique).	Satisfaction à une obligation légale (Art. 33 RGPD)
Notifier aux intéressés (notamment dans le cas de fuites de données dans lesquelles est identifié un risque élevé pour les usagers)	Satisfaction à une obligation légale (Art. 33.3 RGPD)
Prendre la décision des mesures conservatoires.	Satisfaction à une obligation légale (Art. 34 RGPD) Protection des élèves ou usagers.
Gérer un incident à portée locale	Responsabilité du chef d'établissement (L421-3, R421-10 du CE).
Si incident initié depuis le SI de l'établissement : procédure disciplinaire et/ou dépôt de plainte Déposer une plainte (si impact sur le SI ou sur les usagers de son établissement)	Protection de l'établissement contre les préjudices subis. Responsabilité du chef d'établissement (L421-3, R421-10 du CE).
Communiquer aux intéressés	Communication en gestion d'incidents ou de crise (bonnes pratiques, gestion des risques).

Tableau 1 : Actions attendues du chef d'établissement

4.2. Porteur de projet ENT

Action(s) à mener	Responsabilité(s)
S'assurer que les éléments indispensables à la gestion des incidents sont dans l'appel d'offre et dans le marché.	Relation contractuelle avec le fournisseur de service au regard des recommandations de l'ANSSI (clauses SSI, RGS, PSSIE (Politique de Sécurité des Systèmes d'Information de l'Etat))
S'assurer de la collaboration entre les chaînes d'alertes et chaînes décisionnelles.	PSSIE
Coordonner les actions de réponses aux incidents avec l'ensemble des parties prenantes.	PSSIE

Tableau 2 : Actions attendues du porteur de projet

4.3. Collectivité de rattachement

Action(s) à mener	Responsabilité(s)
Décider des investissements en termes de gestion des incidents.	Compétences des régions (L-214-6 du CE) Compétences des départements (L213-2 du CE)
Valider les décisions	AQSSI collectivité territoriale
Contribuer à l'information du chef d'établissement afin qu'il puisse remplir ses responsabilités. Notifier le RSSI de l'académie de l'incident	Article 4-4 alinéa 4 du décret 2022-513 du 8 avril 2022 relatif à la sécurité numérique du système d'information et de communication de l'Etat et de ses établissements publics
Notifier l'autorité de contrôle	Art. 33 RGPD Kit de conventionnement « Informatique et Libertés » dans le cadre du déploiement d'un ENT

Tableau 3 : Actions attendues de la collectivité de rattachement

4.4. Autorité académique

L'autorité d'homologation académique est compétente lorsqu'elle est porteur de projet.

Elle invite les collectivités territoriales à la commission d'homologation qu'elle met en œuvre.

Lorsque la collectivité territoriale est le porteur de projet, il lui appartient d'homologuer l'ENT.

Dans tous les cas, l'entité responsable de l'homologation communique aux autres entités les résultats de l'homologation. (Cf. guide du kit SSI retaif aux Téléservices.)

Action(s) à mener	Responsabilité(s)
Valider les décisions	Autorité qualifiée pour la sécurité des systèmes d'information (AQSSI, Circulaire n° 2012-046 du 12-3-2012)
Alerter si besoin la chaîne SSI nationale	PSSIE
Mettre en place une gestion d'incident de l'amont jusqu'à l'aval intégrant en particulier les retours d'expérience	Décret n° 2022-513 du 8 avril 2022
Notifier l'autorité de contrôle	Art. 33 RGPD Kit de conventionnement « Informatique et Libertés » dans le cadre du déploiement d'un ENT

Tableau 4 : Actions attendues de l'autorité académique

4.5. DSI de l'académie

Action(s) à mener	Responsabilité(s)
Apporter son expertise sur l'ensemble de cycle de vie de la gestion des incidents.	Organisation et coordination de la gouvernance du système d'information et du numérique en relation les collectivités territoriales
Apporter un appui opérationnel dans la gestion de la réponse à l'incident.	Apport de l'expertise et des moyens de la DSI pour la réponse à l'incident ou à la crise, pour son périmètre de responsabilité

Tableau 5 : Actions attendues du DSI

4.6. RSSI de l'académie

Action(s) à mener	Responsabilité(s)
Apporter son expertise en amont sur l'intégration de la gestion des incidents dans les appels d'offre.	Circulaire n° 2012-046 du 12-3-2012
Garantir l'opérationnalité de la chaîne d'alerte.	Circulaire n° 2012-046 du 12-3-2012
Favoriser la communication de l'information entre parties prenantes opérationnelles.	Circulaire n° 2012-046 du 12-3-2012
Rappeler les règles en termes de recueil et de communication des journaux d'évènements aux parties prenantes et à l'autorité judiciaire.	Circulaire n° 2012-046 du 12-3-2012
Travailler en coordination avec les DPD (académie et CT).	Satisfaction à une obligation légale (Art. 32 RGPD)

Tableau 6 : Actions attendues du RSSI

4.7. DPD de l'académie

Action(s) à mener	Responsabilité(s)
Relayer les signalements à la chaîne d'alerte.	(Art.37,38,39 RGPD) Redevabilité ou « accountability » du RGDP (registre des violations)
Déclarer pour le responsable de traitement la violation de données à la CNIL[1].	Facilitation entre les responsables de traitement et la CNIL (rôle du DPD – guide CNIL)
Conseiller le responsable de traitement.	Conseil et accompagnement de l'organisme (rôle du DPD – guide CNIL)

[1] Il appartient au responsable de traitement de notifier la violation de DCP. Pour cela, il s'appuie sur le DPD qui réalisera en pratique la notification.

Action(s) à mener	Responsabilité(s)
Conseiller son autorité.	Conseil et accompagnement de l'organisme (rôle du DPD, guide CNIL)
Se coordonner avec son homologue (académique ou CT).	Redevabilité ou « accountability » du RGDP (registre des violations)
Travailler en coordination avec la chaîne d'alerte.	Redevabilité ou « accountability » du RGDP (registre des violations)

Tableau 7 : Actions attendues du DPD

4.8. DANE / DRANE

Action(s) à mener	Responsabilité(s)
Relayer les signalements à la chaîne d'alerte SSI académique. Indiquer l'impact de l'incident à l'ensemble des bénéficiaires du service.	Note de service n° 2014-098 du 25-8-2014 Satisfaction à une obligation légale
Accompagner les usagers impactés.	Pilotage de la mise en œuvre dans l'académie du service public du numérique éducatif
Sensibiliser les enseignants, le personnel administratif et le personnel de direction.	Pilotage de la mise en œuvre dans l'académie du service public du numérique éducatif

Tableau 8 : Actions attendues du DANE / DRANE

4.9. Sous-traitant (opérateur de l'ENT ou de l'un de ses composants)

Action(s) à mener	Responsabilité(s)
Notifier au responsable de traitement	Obligation du sous-traitant (RGPD 33.2)
Conduire les investigations sous le contrôle ou la demande du porteur de projet.	Obligation du sous-traitant

Action(s) à mener	Responsabilité(s)
Collaborer avec le Prestataire de Réponse aux Incidents de Sécurité (PRIS), ou les structures académiques, ou les structures des CT chargées des investigations.	Obligation du sous-traitant (RGPD. 28.3.h)
Communiquer à la demande des ayant-droit les journaux d'évènements.	Obligation du sous-traitant
Appliquer les mesures conservatoires décidées, les décisions d'urgence, ou le plan de remédiation.	Obligation du sous-traitant

Tableau 9 : Actions attendues du sous-traitant

5. Recommandations aux acteurs

5.1. Principes

5.1.1. Chaine opérationnelle de la sécurité.

La responsabilité de la gestion des incidents est une responsabilité partagée entre partenaires de la convention qui régit l'espace numérique de travail.

Elle se conforme à l'objectif 32 de la PSSIE qui est de « *partager l'information (alertes, incidents) dans le respect des règles de prudence et mutualiser les opérations de remise en état, de façon à lutter efficacement contre les attaques.* » ainsi qu'aux règles qui en découlent[2].

Pour ce qui relève des responsabilités académiques, le recteur en sa qualité d'AQSSI est responsable de la sécurité des systèmes d'information et par extension, dans le cadre de la responsabilité partagée pour les ENT, responsable de la sécurité des ENT.

- Fonctionnellement, le pilotage ou co-pilotage d'un incident relève de l'IA-DASEN ou de son représentant pour le premier degré, du recteur ou de son représentant pour le second degré.

- Opérationnellement, la chaine est articulée autour du DSI, du DANE, du RSSI et du DPD académique ou de la région académique. Cette chaine s'insère dans la chaine opérationnelle ministérielle.

Côté partenaires, l'organisation relève de la libre administration des collectivités territoriales.

La chaine opérationnelle académique coopère avec la ou les chaines homologues des collectivités territoriales. Les actions de la chaine opérationnelle sont réalisées sans préjudice des obligations découlant du RGPD et du contrôle nécessaire du DPD en cas d'incidents affectant les données à caractère personnel traitées dans l'ENT.

[2] En particulier, règles TI-MOB, TI-QUAL-TRAIT et TI-INC-REM de la PSSIE.

5.1.2. Relations avec les sous-traitants

Les sous-traitants, dont la collaboration pleine et entière est attendue, participent à la gestion des incidents. En sus des obligations qui leur incombent en application du RGPD, des clauses particulières du marché sont établis sur la gestion des incidents[3] et la participation aux instances de pilotage de la sécurité[4].

Ces clauses garantissent notamment :

- La collaboration en termes de conseils et d'assistance pour le traitement d'incident ;
- La communication des journaux de logs ;
- La participation aux réunions de gestion d'incidents ou de crise ;
- La participation aux instances de pilotage.

5.1.3. Relations avec le RGPD

L'espace numérique de travail est un traitement de données à caractère personnel et soumis à ce titre au RGPD.

L'occurrence d'un incident fait l'objet :

- De façon obligatoire, d'une documentation en interne qui précise la nature de l'incident, la catégorie et le nombre de personnes affectées (élèves, parents, enseignants, ...), les impacts, mesures conservatoires, plan de remédiation.
- Le cas échéant, si l'incident constitue un risque pour les personnes concernées, d'une notification à la CNIL.

Pour mémoire, cette notification doit être faite le plus tôt possible, dans un délai n'excédant pas les 72 heures et en cas du dépassement de ce délai, être accompagnée des motifs expliquant le retard.

Ceci implique que le DPD :

- Soit immédiatement consulté lorsqu'une violation de données ou un autre incident ;
- Participe à la réalisation des notifications de violation de données personnelle.

Dans le cas d'une responsabilité partagée, la notification sera faite par l'autorité administrative du porteur de projet sans que cela fasse obstacle à l'information des DPD des autres entités partenaires.

[3] Cf. guide gestion des incidents – Kit SSI
[4] Cf. guide gouvernance – Kit SSI

5.2. Recommandations

R1

Déclarer la suspicion d'incident au RSSI ou au DPD académique

En cas de détection ou de suspicion d'un incident affectant l'ENT de l'établissement, le chef d'établissement déclare l'incident au RSSI de l'académie. Dans le cas d'un incident affectant potentiellement des données à caractère personnel, le chef d'établissement déclare sans délai au DPD de l'académie afin qu'il procède à sa notification.

Pour cela, l'académie ou la région académique tient à jour et met à disposition du chef d'établissement, les coordonnées du personnel en charge de la chaîne d'alerte ou de la protection des données à caractère personnel.

Cette alerte est indépendante de la déclaration dans l'application « faits établissements ». Il est précisé que le DPD doit être « *immédiatement consulté lorsqu'une violation de données ou un autre incident (signalement relevé dans la presse, réclamations, etc.) se produit.* »

i

Pour mémoire, la responsabilité de notifier dans les 72 heures l'autorité de contrôle en cas de violation de DCP relève de la responsabilité du chef d'établissement. Dans la pratique la notification sera faite par le DPD (voir recommandation R12).

R2

Notifier aux intéressés

Dans le cas d'un incident induisant une violation des données à caractère personnel, en coordination avec le DPD académique, le chef d'établissement notifie aux intéressés l'incident les affectant.

Cette notification est réalisée par le chef d'établissement qu'il s'agisse d'un ENT exploité localement dans l'établissement ou d'un ENT opéré par un porteur de projet ou son sous-traitant. Dans le cas d'un ENT opéré par un porteur de projet ou sons sous-traitant, la chaine opérationnelle veillera à une information pleine et entière du chef d'établissement.

i

La notification des incidents aux personnes concernées est obligatoire lorsque l'incident représente un risque élevé. L'appréciation du niveau de risque, en fonction des critères fournis par la CNIL sur site relève du rôle de la chaine opérationnelle dont le DPD est un acteur primordial pour les incidents affectant des DCP.

La notification aux intéressés relève du devoir des services publics et n'est pas une faculté ouverte au sous-traitant. Ce dernier lorsqu'il prend connaissance d'un incident affectant des DCP le notifie au responsable de traitement (cf. Recommandation Rx).

R3

Prendre la décision des mesures conservatoires.

Dans le cas d'un incident affectant spécifiquement son établissement[5], le chef d'établissement prend des mesures conservatoires pouvant aller jusqu'à la suspension d'exploitation de l'espace numérique de travail.

Dans le cas d'un incident affectant tout ou partie d'un ENT opéré par le porteur de projet, ce dernier prend les mesures conservatoires appropriées qui peuvent aller jusqu'à la suspension d'exploitation de l'espace numérique de travail.

Dans le cas d'un incident affectant tout ou partie de l'ENT opéré par le sous-traitant, celui-ci avertit sans délai le porteur de projet en sa qualité de responsable de traitement. Celui-ci envisage avec le sous-traitant les mesures conservatoires appropriées qui peuvent aller jusqu'à la suspension d'exploitation de l'espace numérique de travail et prend la décision de les appliquer.

Si selon le sous-traitant, l'instruction qui lui est donnée constitue une violation des règles en matière de protection des données, il est tenu d'en informer immédiatement son client.
Cette information doit être prise en compte et consignée. Le maintien de l'instruction devra être impérativement motivée.

Note 1 : dans le cas d'un incident affectant tout ou partie de l'ENT opéré par le sous-traitant, la décision par le porteur de projet de maintenir l'exploitation constitue une instruction du client. Si le sous-traitant considère que cette instruction constitue une violation du RGPD, il est légalement tenu d'en informer le porteur de projet. Cette information ne peut pas être ignorée.

Note 2 : les mesures conservatoires ne dispensent nullement d'informer le DPD de l'incident

R4

Gérer un incident à portée locale

Dans le cas d'un incident à portée locale, exemples des cas d'un élève qui a usurpé l'identité d'un autre pour diffuser des propos malveillants ou celui d'un

[5] Que l'ENT soit opéré localement ou par le porteur ou son sous-traitant.

élève qui a usurpé l'identité d'un enseignant pour modifier les notes avec un impact sur la vie scolaire, le chef d'établissement gère localement l'incident.
Ce choix ne fait pas obstacle à la déclaration dans l'application « faits établissements » et de façon plus impérative en cas de violation de DCP ou de suspicion, de signalement au DPD (voir recommandation 1).

En cas de doute, le chef d'établissement s'appuie sur les services académiques ou inter-académiques tels que le proviseur vie scolaire, le service juridique, le RSSI. Il s'appuie également sur le DPD en tant qu'interlocuteur privilégié du responsable de traitement en cas de violation ou suspicion de violation de données à caractère personnel.

R4

Gérer un incident affectant un ensemble d'établissements

Dans le cas d'un incident affectant un ensemble d'établissements, il appartient au porteur de projet :

- De saisir la chaine opérationnelle de son entité ;
- D'informer les autres parties pour coordonner l'action des chaines opérationnelles.

Le porteur de projet veille en particulier à l'application des recommandations :

- R6 pour donner les éléments nécessaires à la communication du chef d'établissement ;
- R9 pour coordonner les actions de réponses à incidents avec l'ensemble des parties prenantes ;
- R11 pour favoriser la communication de l'information entre parties prenantes.

R5

Déposer une plainte

Dans le cadre d'un incident touchant spécifiquement son établissement, le chef d'établissement peut déposer plainte[6].

Toutefois, dans le cas d'une violation de DCP, le chef d'établissement consulte le service juridique et le DPD.

Selon l'impact, il appartiendra au chef d'établissement de « remonter » le dépôt de plainte à l'échelon académique.

Dans le cas d'un ENT opéré dans le cadre d'un partenariat, le dépôt de plainte suite à une atteinte aux données d'élèves, de parents d'élèves ou de personnel

[6] Article 8.2 du décret n°85-924 du 30 août 1985 relatif aux EPLE

de l'éducation nationale relève de l'autorité du recteur et du service juridique inter- académique.

R6

Communiquer aux intéressés

Lors d'un incident, il appartient aux chefs d'établissements de communiquer en direction des intéressés. Pour sa communication, il peut se faire assister du RSSI, du DPD ou du personnel de vie scolaire (PVS) le cas échéant. Dans le cas d'un incident portant sur un ensemble d'incidents, le chef d'établissement communique sur la base des informations communiquées par le porteur de projet (collectivité territoriale, académie).

Cette information peut être prise en charge au niveau académique mais il appartient au chef d'établissement de la relayer.

La communication aux intéressés se distingue de la notification aux intéressés :

- Quand l'incident n'est pas une violation de DCP ;
- Dans le cas où le nombre de personnes concernées par l'incident est plus grand que celui des personnes affectées par la violation de DCP.

Dans ce dernier cas, il est utile d'informer les personnes concernées que leurs données personnelles n'ont pas été affectées, en leur indiquant en particulier que les personnes dont les données ont été affectés ont fait l'objet d'une notification individuelle et que la CNIL a été alerté.

R7

Obtenir les logs

En cas d'incident, le sous-traitant doit communiquer les logs à la demande du RSSI ou des services compétents du porteur de projet.

Dans le cas où l'incident nécessite des investigations complémentaires, ceux-ci ont autorité pour :

- Demander au sous-traitant la communication des logs ;
- Communiquer ou demander à ce que les logs soient communiqués aux autorités judiciaires, auxquelles il ne peut être fait obstacle dans le cadre des investigations qu'elles mènent.

Les clauses de sécurité relatives aux obligations du prestataire doivent spécifier à minima la mise en œuvre des journaux d'enregistrement (logs) :

- Des accès à l'ENT,
- Des communications électroniques conformes à la réglementation,
- Ainsi que des accès aux bases de données.

De plus, ces clauses de sécurité doivent rappeler l'obligation du prestataire en termes de communication des logs à tout tiers désigné par le responsable de traitement.

Le porteur de projet vérifie la présence de telles clauses en s'appuyant sur les services de son RSSI et du DPD.

En plus des clauses réglementaires obligatoires comme les clauses contractuelles type du RGPD ou recommandées comme le CGAG-PI, il est possible de s'appuyer sur :

- Guide de l'externalisation ANSSI §Obligations du prestataire
- Guide du sous-traitant CNIL §4

(cf. Guide sous-traitant)

S'assurer de la collaboration entre les chaînes opérationnelles et décisionnelles.

En amont du traitement des incidents, les partenaires de la convention doivent s'assurer que :

- Les chaines opérationnelles de traitement d'incident et les chaines décisionnelles (ou instances de pilotage) intègrent les ENT dans leur champ d'intervention ;
- Une organisation est mise en œuvre pour coordonner l'action des partenaires et de leurs chaines respectives en cas d'incident ;

Que les présentes recommandations soient portées à la connaissance des chaines opérationnelles et décisionnelles.

Les chaînes opérationnelles des collectivités territoriales coopérent avec la chaîne opérationnelle académique. Les responsabilités académiques sont attribuées au Recteur et celles des collectivités selon leur organisation propre.
Les règles de coordination/partage des responsabilités sont à définir dans les comités définis pour la gouvernance des ENT.

Coordonner les actions de réponses à incidents avec l'ensemble des parties prenantes.

En cas d'incident affectant un ENT regroupant un ensemble d'établissements, il appartient au porteur de projet, une fois qu'il en a été informé :

Sur le plan de l'information :

- D'informer l'ensemble des partenaires, en particulier les chefs d'établissement ;
- De solliciter la chaine opérationnelle ;
- De veiller à la consultation du DPD du porteur de projet.

Sur le plan du respect de la réglementation :

- De s'assurer que les diligences au regard du RGPD ont bien été faites (consignation de l'incident conformément aux recommandation CNIL) ;
- De faire suite ou veiller à ce que soit fait suite à toute demande du DPD.

Sur le plan opérationnel :

- Veiller à la bonne information de la chaine décisionnelle par la chaine opérationnelle ;
- Veiller, le cas échéant, à la coordination avec d'autres structures opérationnelles comme le service communication ou juridique selon l'ampleur de l'incident.

Cf. également recommandation R11.

Le DPD de l'académie ou de la région académique est systématiquement informé lorsque l'incident affecte ou est susceptible d'affecter des données à caractère personnel d'élèves, parents d'élèves ou personnel de l'Éducation nationale.

Valider les décisions

Dans le cas d'un incident affectant un ensemble d'établissements, il appartient à l'entité territoriale en tant que porteur de projet et en liaison avec l'autorité académique, ou à l'autorité académique en tant que porteur de projet avec l'entité territoriale de prendre ou valider les décisions touchant à des mesures conservatoires.

Ces décisions reposent sur les propositions de la chaine opérationnelle. Elles peuvent consister, en particulier, à suspendre tout ou partie des services de l'ENT impliquent l'information de l'ensemble des parties prenantes.

Favoriser la communication de l'information entre parties prenantes

La communication est un facteur clé de la bonne conduite de la gestion d'un incident. Il appartient à tous les acteurs de la gestion des incidents de s'assurer que les autres acteurs de cette gestion en raison de leur fonction ou des dispositions réglementaires en vigueur disposent du même niveau d'information.

Coordination entre partenaires
Le partenaire le premier informé communique en direction des autres partenaires afin d'activer les chaines opérationnelles le cas échéant.
Il est rappelé que le traitement in fine des violations de données à caractère personnel des élèves, parents d'élèves et enseignants relèvent de la responsabilité de l'autorité académique.
En cas d'incident affectant un ensemble d'établissements, la chaine opérationnelle coordonne son action avec la ou les chaines opérationnelles des partenaires.

Coordination entre chaine opérationnelle et DPD
Dans le cadre d'un incident portant sur une violation de données à caractère personnel, la chaine opérationnelle travaille en coordination avec le DPD pour s'assurer qu'aucune mesure prise ne peut contrevenir à des obligations découlant du RGDP.

Cette exigence découle de l'obligation de documentation de l'incident telle qu'elle est prescrite par l'article 33 du RGDP.

L'objet de cette règle est de fluidifier la communication. Une bonne pratique consiste à intégrer le DPD dans la chaine opérationnelle de traitement des incidents et dans l'application de gestion des incidents.

Déclarer la violation de données à la CNIL.

R12

La notification d'un incident relève du responsable de traitement. Selon la CNIL, le DPD « *n'est pas responsable de la conformité de l'organisme (..)ou des notifications de violations de donnée* ».
Dans la pratique, le DPD procédera à la déclaration auprès de la CNIL après validation du responsable de traitement.

Il est rappelé que la déclaration d'incident doit être faite dès que possible, dans la mesure du possible avec un délai n'excédant pas 72h. Dans le cas où ce délai est dépassé la déclaration doit être accompagné d'un motif explicitant la raison du retard.

Ressources :
- Guide des délégués à la protection des données CNIL §4

- Guide du sous-traitant CNIL §4

R13

Conseiller le responsable de traitement

Conformément aux recommandations de la CNIL, le DPD est un acteur clé. En cas de violation de DCP, il conseille le responsable de traitement, en particulier pour documenter les « *faits concernant la violation des données à caractère personnel, ses effets et les mesures prises pour y remédier* » comme en dispose l'article 33 du RGPD. Le cas échéant, le DPD conseille également son autorité administrative,

Dans ce contexte, et conformément à la mission de contrôle de l'effectivité des règles qui lui est dévolue par la réglementation et la CNIL, il peut demander :

- Un audit pour les objets prévus dans le guide CNIL des délégués à la protection des données ;
- La communication des logs pour analyse par les services du RSSI, de la DSI ou d'un tiers mandaté par l'autorité administrative.

Ressources :

- Guide des délégués à la protection des données CNIL §4
- Guide du sous-traitant CNIL

R14

Notifier au responsable de traitement

Dans le cadre d'un incident portant sur une violation de DCP, le sous-traitant doit notifier dès qu'il en a connaissance l'incident au porteur de projet, conformément à l'article 33 alinéa 2 du RGPD. Dans le cas où l'incident affecte un établissement de façon singulière, le responsable de traitement notifie l'incident au chef d'établissement.

Dans le cadre de la convention de partenariat, le porteur de projet en informe les autres responsables de traitement.

L'alinéa 3 de l'article 33 du RGPD s'applique au responsable de traitement qui doit documenter l'incident conformément aux prescriptions de l'article. Dans le cas où le sous-traitant n'est pas capable de fournir tous les éléments, il peut les communiquer de manière échelonnée sans retard supplémentaire.

R15

Appliquer les mesures

Lors d'un incident, le porteur de projet doit avoir le contrôle sur la gestion de celui-ci et être en mesure de faire appliquer les mesures proposées par la chaine opérationnelle et validées par la chaine décisionnelle. Cette faculté doit avoir été prévue dans le marché.

En particulier, en plus de pouvoir accéder à l'environnement et aux logs, le porteur de projet doit pouvoir décider :

- De l'arrêt, de l'isolement, du rétablissement du ou des serveurs ;
- Des conditions de poursuite de l'activité en mode dégradé ;
- De la mise en place de règles de filtrage.

En fonction de l'incident, le porteur de projet peut décider de faire intervenir un prestataire de réponse aux incidents de sécurité qualifiés sur le périmètre de l'ENT opéré par le prestataire. (Voir Recommandation n° 16)

L'autorité du porteur de projet sur la conduite de la gestion des incidents doit avoir été prévue dans l'appel d'offres et le prestataire ne peut s'y opposer sauf s'il estime que les mesures demandées constituent une violation du RGPD.

Conduire les investigations sous le contrôle ou à la demande du porteur de projet.

Lorsque le sous-traitant a détecté ou été informé en premier de l'incident, il le documente pour le compte du porteur de projet conformément à l'article 33 du RGPD. Dans le cas contraire, le porteur de projet avise le sous-traitant.

Dans tous les cas, les investigations sont menées sous le contrôle du porteur de projet chargé de l'application des mesures décidées par la chaine opérationnelle et validée par la chaine décisionnelle.

Les investigations peuvent être menées par le sous-traitant, des ressources internes ou un PRIS.

Dans le cadre des investigations, le porteur de projet peut décider d'une intervention d'un PRIS sur périmètre restreint. Dans ce cas, le sous-traitant participe au bon déroulement de la prestation qui sera exécutée conformément

au §VI du référentiel d'exigences de l'ANSSI relatif aux « prestataires de réponse aux incidents de sécurité »

En particulier, le sous-traitant est associé à :

- L'élaboration des informations de contexte sur l'incident de sécurité communiquées au PRIS ;
- L'établissement de la convention de prestation entre porteur de projet et PRIS (cf. VI.2 du référentiel d'exigences PRIS) ;
- La préparation et l'exécution de la prestation ;
- La restitution et la clôture.

6. Référentiels applicables

Nom	Objet	Ressources/Liens
Décret n° 2022-513 du 8 avril 2022	Relatif à la sécurité numérique du système d'information et de communication de l'Etat et de ses établissements publics	https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000045537693
SDET	Schéma directeur des ENT	https://eduscol.education.fr/1559/schema-directeur-des-ent-sdet-version-en-vigueur
Annexe Opérationnelle	Annexe opérationnelle du SDET	https://eduscol.education.fr/1559/schema-directeur-des-ent-sdet-version-en-vigueur
Kit de conventionnement « Informatique et Libertés »	Kit de conventionnement « Informatique et Libertés » dans le cadre du déploiement d'un ENT	https://eduscol.education.fr/document/9710/download
Recteur délégué de zone	Aspects SSI	Recteur délégué de zone https://www.education.gouv.fr/bo/12/Hebdo15/MENN1206405C.htm
Instruction sur la gouvernance numérique de l'état	Organisation de la sécurité au sein du ministère	(À venir)
Fiche 2 Guide ANSSI collectivités territoriale	Sécurité numérique des collectivités territoriales : l'essentiel de la réglementation	https://www.ssi.gouv.fr/uploads/2020/01/anssi-guide-securite_numerique_collectivites_territoriales-reglementation1.pdf (Fiche 2)
CSIRT régionaux		https://www.ssi.gouv.fr/agence/cybersecurite/france-relance/programme-dincubation-de-csirt/ ARNIA
Guide PRIS ANSSI	Prestataires de réponse aux incidents de sécurité Référentiel d'exigences	https://www.ssi.gouv.fr/uploads/2014/12/pris_referentiel_v2.0.pdf

Politique de Sécurité des Systèmes d'Information de l'Etat (PSSIE)	Règles de protection applicables aux systèmes d'information de l'État	https://www.ssi.gouv.fr/uploads/2014/11/pssie_anssi.pdf