

Dossier RGPD et aide à l'AIPD

HSE Signal en milieu scolaire

Version du 11 juillet 2026. Éditeur : DigitHSE (Entrepreneur individuel (EI)). Contact : contact@digithse.fr.

Ce dossier accompagne les établissements qui souhaitent utiliser HSE Signal pour recueillir les signalements de harcèlement. Il aide la personne responsable de la protection des données (DPO ou chef d'établissement) à réaliser son analyse d'impact (AIPD) et présente les réglages recommandés. Il ne remplace pas l'AIPD elle-même : il en fournit la matière.

Qui est responsable de quoi

Au sens du RGPD, l'établissement est **responsable de traitement** : il décide de la finalité (protéger les élèves) et des moyens. DigitHSE est **sous-traitant** : il héberge et fait fonctionner l'outil, uniquement sur instruction de l'établissement, dans le cadre de l'accord de sous-traitance (article 28 du RGPD).

- ✓ L'AIPD est à la charge de l'établissement. Dans le public, elle est pilotée par le DPO de l'académie ; dans le privé, par le chef d'établissement ou son DPO.
- ✓ L'établissement informe les élèves, les familles et les personnels de l'existence du dispositif.
- ✓ DigitHSE fournit les informations techniques nécessaires (ce document) et applique les mesures de sécurité décrites ci-dessous.

Pourquoi une AIPD est nécessaire

Une analyse d'impact est requise (article 35 du RGPD) car le traitement concerne des **personnes vulnérables (des mineurs)** et porte sur un sujet sensible. La réaliser en amont sécurise juridiquement l'établissement et démontre sa bonne foi. Les éléments ci-dessous en couvrent les rubriques principales, selon la méthode de la CNIL.

1. Description du traitement

- ✓ Finalité : permettre à un élève ou un témoin de signaler une situation de harcèlement, afin que l'établissement la traite et protège la victime.
- ✓ Personnes concernées : les élèves (mineurs pour l'essentiel) et, le cas échéant, les personnels.
- ✓ Données recueillies : la description libre de la situation saisie par le déclarant. Le nom et un moyen de contact sont FACULTATIFS le déclarant peut rester totalement anonyme.
- ✓ Aucune donnée de compte n'est demandée au déclarant : le signalement se fait par QR code, sans identifiant ni mot de passe.
- ✓ Destinataires : uniquement les personnes désignées par l'établissement (chef d'établissement, référent harcèlement, CPE...), selon leurs droits d'accès.

- ✓ Hébergement : Union européenne (Allemagne). Aucune donnée n'est vendue ni utilisée à d'autres fins.

2. Base légale et proportionnalité

Le traitement repose sur la **mission d'intérêt public** de l'établissement (article 6.1.e du RGPD) : la protection des élèves et la lutte contre le harcèlement, qui s'inscrivent dans le programme national PHARe. Les données recueillies sont limitées au strict nécessaire : une description des faits, et rien d'autre que le déclarant ne choisit d'ajouter. Le dispositif oriente vers les ressources nationales (3018, 119) plutôt que de se substituer à elles.

3. Mesures de protection déjà en place

Par conception, la plateforme minimise les risques pour les mineurs :

- ✓ Anonymat réel : aucun compte, aucun nom obligatoire. Le déclarant décide seul s'il laisse un contact.
- ✓ Adresse IP jamais conservée : seule une empreinte technique non réversible sert à limiter les abus, puis elle est effacée sous 48 heures.
- ✓ Chiffrement des échanges et cloisonnement strict : les données d'un établissement sont inaccessibles à tout autre.
- ✓ Accès réservé : seules les personnes habilitées par l'établissement consultent les signalements.
- ✓ Photos désactivables pour tout l'établissement (recommandé en milieu scolaire), afin d'éviter toute image d'élève.
- ✓ Conservation maîtrisée : l'établissement fixe la durée et peut demander la suppression à la clôture.

4. Risques résiduels et réponses

- ✓ Signalements abusifs ou canulars : un classement « sans suite » les sort des statistiques, un plafond quotidien et une mise en quarantaine automatique absorbent les rafales, sans jamais bloquer une vraie victime.
- ✓ Ré-identification d'un déclarant anonyme : écartée, car aucune donnée nominative ni IP n'est conservée.
- ✓ Accès non autorisé : limité par le cloisonnement, les droits par rôle et la journalisation des accès anormaux.
- ✓ Sur-signalement depuis un réseau partagé (wifi de l'établissement) : le plafond est réglable pour ne pas gêner l'usage normal.

Réglages recommandés pour un établissement

- ✓ Activer « Ne jamais demander de photo » (Paramètres HSE Signal) : aucun cliché d'élève.
- ✓ Adapter les catégories de signalement au contexte scolaire (par exemple : harcèlement, insultes, mise à l'écart, cyberharcèlement, racket).
- ✓ Désigner un référent qui reçoit les alertes, et limiter l'accès aux seules personnes concernées.
- ✓ Placer les QR dans les lieux discrets (toilettes, couloirs, CDI, cour) pour préserver l'anonymat du geste.
- ✓ Renseigner le numéro d'écoute (3018) pour qu'il s'affiche au déclarant après son signalement.

- ✓ Sur l'écran d'affichage, laisser la cartographie masquée : afficher les numéros utiles (3018, 119) et des messages de prévention plutôt que des statistiques.
- ✓ Informer élèves, familles et personnels, et intégrer ce document à votre AIPD.

Documents liés

Pour aller plus loin : accord de sous-traitance (RGPD), politique de confidentialité et page Sécurité, disponibles sur plateformehse.fr. Une question sur ce dossier ou besoin d'un accompagnement pour votre AIPD ? Écrivez à contact@digithse.fr.