Confiance et sécurité

Pourquoi un établissement peut confier à EaseAcademia ses dossiers et les données de ses élèves, comment ces données sont protégées, comment la plateforme aide l'établissement à respecter la loi nigériane sur la protection des données, et les questions à poser à tout prestataire.

Dernière mise à jour · 19 octobre 2026

En bref

Un établissement détient certaines des informations les plus sensibles que l'on puisse conserver sur un enfant : notes de santé, signalements de protection de l'enfance, adresses, numéros de téléphone de la famille, frais dus et résultats d'examens. Les parents les confient parce qu'ils font confiance à l'établissement. Lorsque l'établissement fonctionne sur EaseAcademia, une partie de cette confiance nous revient.

Ce guide explique comment cette confiance se mérite. Il s'adresse aux promoteurs, aux chefs d'établissement et aux délégués à la protection des données, ainsi qu'au responsable informatique ou à l'administrateur à qui l'établissement demande d'examiner un prestataire. Chaque affirmation sur EaseAcademia décrit le produit tel qu'il fonctionne aujourd'hui. Lorsqu'une protection a une limite, la limite est indiquée, et ce que nous ne revendiquons pas encore fait l'objet d'une section à part.

- **L'établissement reste maître de ses données.** L'établissement est le responsable du traitement et EaseAcademia son sous-traitant. Les données servent à faire fonctionner l'établissement, et à rien d'autre. Elles ne sont jamais vendues, et les données des enfants ne servent jamais à la publicité ni au profilage.
- **Chaque porte est fermée au départ.** Toute action est refusée sauf si le rôle de la personne l'autorise, et les dossiers de chaque établissement sont tenus à l'écart de ceux des autres.
- **Les écrits les plus sensibles sont chiffrés deux fois.** Tout est chiffré en transit et au repos, et 167 champs sensibles, des notes de l'infirmerie aux dossiers de protection de l'enfance, bénéficient en plus de leur propre couche de chiffrement.
- **Rien ne se passe sans laisser de trace.** Les actions, et les tentatives refusées, sont inscrites dans un journal d'audit scellé que l'établissement peut consulter.
- **La loi est intégrée.** Les mesures qu'attend la loi nigériane sur la protection des données font partie du produit, et les obligations propres d'EaseAcademia figurent dans un avenant relatif au traitement des données publié.

Ce qu'un établissement nous confie

Toutes les données scolaires ne présentent pas le même risque. Une liste de classe compte ; une note sur le traitement d'un enfant ou un signalement de protection de l'enfance compte bien davantage. EaseAcademia protège l'ensemble, et ajoute des couches à mesure que la sensibilité augmente.

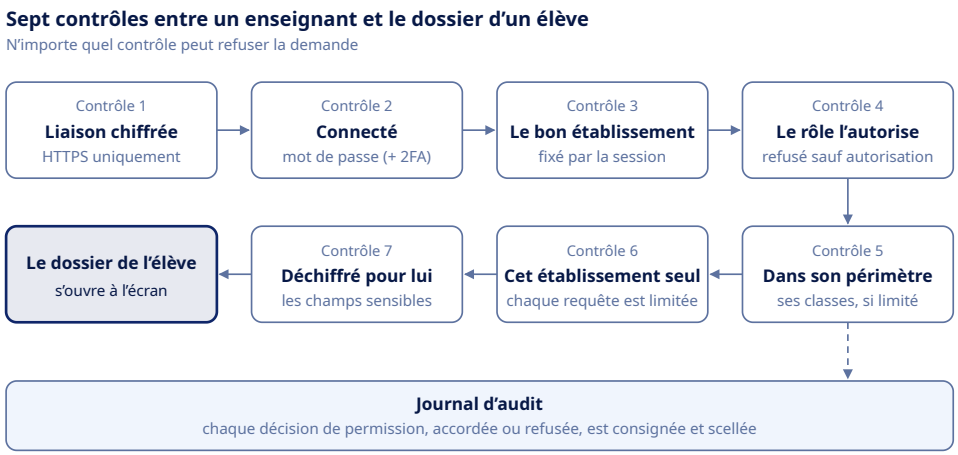
De quoi il s’agit	Exemples	Comment c’est protégé
Dossiers courants	Noms, classes, emplois du temps, présences, notes	Chiffrés en transit et au repos, visibles seulement par les rôles qui en ont besoin, chaque modification enregistrée
Coordonnées et famille	Téléphones et adresses e-mail des responsables légaux, adresses du domicile, notes sur une famille	Tout ce qui précède, et les adresses et les notes sont chiffrées champ par champ
Argent	Factures de frais, paiements, remboursements, crédit prépayé de l’établissement	Tout ce qui précède ; les données de carte sont traitées par Paystack et jamais conservées par EaseAcademia, et chaque avis de paiement est vérifié par sa signature
Données personnelles sensibles	Passages à l’infirmerie et médicaments, protection de l’enfance et discipline, réclamations et procédures disciplinaires du personnel, notes de recrutement	Tout ce qui précède, et chaque champ est chiffré séparément avant d’être enregistré
Fichiers	Bulletins, documents d’admission, photos, pièces jointes des messages	Chiffrés dans le stockage, jamais publics, ouverts uniquement par des liens qui expirent

Les principes derrière chaque mesure

1. **Refuser sauf autorisation.** L’accès part de zéro et s’accorde rôle par rôle. Une erreur dans la configuration d’un rôle reste sans danger : il manque un écran à quelqu’un, plutôt que de lui en montrer un qu’il ne devrait pas voir.
2. **Supposer que n’importe quelle couche peut céder.** La connexion, les permissions, le cloisonnement entre établissements, le chiffrement et le journal d’audit sont des défenses distinctes. En franchir une n’ouvre pas les autres.
3. **Refuser de fonctionner sans sécurité.** Le service en production ne démarre pas sans sa clé de chiffrement, ses secrets de signature, des cookies de connexion sécurisés et un stockage de fichiers chiffré. Une erreur de configuration arrête le service au lieu de l’affaiblir en silence.
4. **Vérifier automatiquement, à chaque modification.** Les protections ont leurs propres contrôles automatisés, qui s’exécutent avant qu’une modification n’atteigne un établissement.
5. **Dire clairement ce que nous ne faisons pas.** Un document de confiance qui n’énumère que des points forts relève du marketing. Celui-ci énumère aussi ses limites.

Sept contrôles entre une personne et un dossier

Lorsqu’un enseignant ouvre le dossier d’un élève, la demande franchit chacun de ces contrôles à tour de rôle. N’importe lequel peut la refuser.



Le parcours d'une demande. Un contrôle qui échoue l'arrête sur place ; chaque décision de permission, accordée ou refusée, est inscrite au journal d'audit.

Les sections suivantes reprennent chaque couche, avec assez de détail pour être vérifiées.

La connexion

La plupart des violations commencent par la porte d'entrée : c'est donc là que se concentre le plus de soin.

- **Les mots de passe ne sont jamais conservés.** Seule une empreinte Argon2id à sens unique est gardée : EaseAcademia peut aider à réinitialiser un mot de passe, mais ne peut jamais le lire. Un mot de passe compte au moins huit caractères, dont une majuscule, une minuscule, un chiffre et un symbole. Le changer exige l'actuel, et le réutiliser est refusé.
- **Les tentatives répétées bloquent le compte.** Cinq mauvais mots de passe en quinze minutes bloquent le compte pendant quinze minutes. Le blocage est conservé avec le compte, si bien qu'un redémarrage de serveur ne l'efface pas, et le titulaire du compte est prévenu dans l'application et par e-mail.
- **La double authentification est disponible.** Le personnel, les administrateurs et les parents peuvent ajouter une application d'authentification, qui produit un code à six chiffres renouvelé toutes les trente secondes, avec dix codes de secours à usage unique en cas de téléphone perdu. Il n'existe volontairement aucun code par SMS ou par e-mail : tous deux sont plus faibles que le mot de passe qu'ils sont censés renforcer. Les élèves et les anciens élèves se connectent sans second facteur.
- **Un établissement peut l'imposer à son personnel.** Dès qu'un établissement active l'obligation, chaque membre du personnel (toute personne qui y détient un rôle autre qu'élève, ancien élève ou parent) doit configurer une application d'authentification. L'établissement choisit un délai de grâce : aucun, ou trois, sept, quatorze ou trente jours, et une personne arrivée plus tard bénéficie du même délai à compter de son arrivée. Le personnel est prévenu dans l'application et par e-mail, puis relancé la veille de l'échéance. Passé ce délai, seul l'écran de configuration s'ouvre encore pour lui, et tant que l'établissement l'impose, il ne peut pas la désactiver. Seul un compte qui utilise déjà la double authentification peut modifier ce réglage.
- **Un téléphone perdu n'est pas une impasse.** Si un membre du personnel a perdu à la fois son téléphone et ses codes de secours, l'établissement peut réinitialiser son second facteur, en indiquant un motif. Seul le propriétaire peut réinitialiser un administrateur, personne dans l'établissement ne peut réinitialiser le propriétaire, et l'établissement ne peut pas réinitialiser un compte que la personne utilise aussi dans un autre

établissement. Chaque réinitialisation est inscrite au journal d'audit et signalée par e-mail au titulaire du compte.

- **Les sessions sont de courte durée.** Le laissez-passer qui autorise chaque demande dure quinze minutes. Il est renouvelé grâce à un jeton remplacé à chaque utilisation, conservé de notre côté uniquement sous forme d'empreinte, et révocable à tout moment. Ce jeton se trouve dans un cookie que les scripts de la page ne peuvent pas lire, ne circule qu'en HTTPS et n'est envoyé qu'au service de connexion. Les demandes de renouvellement venant de tout autre site sont refusées.
- **Les liens de réinitialisation sont à usage unique.** Un lien de réinitialisation n'est conservé que sous forme d'empreinte, ne sert qu'une fois et expire au bout d'une heure. Son utilisation déconnecte le compte sur tous les appareils.
- **Les ordinateurs partagés sont couverts.** Un ordinateur du secrétariat laissé sans surveillance se déconnecte au bout de dix minutes, après un avertissement d'une minute, et demande toutes les heures si la personne est toujours là. La déconnexion efface de l'appareil les pages en cache et les brouillons de formulaires enregistrés.
- **Ceux qui partent perdent vite l'accès.** Désactiver un membre du personnel coupe son accès en quinze minutes au plus, et changer son adresse e-mail professionnelle le déconnecte partout.

Ce que chacun peut atteindre

La connexion répond à la question « qui est-ce ? ». Tout ce qui suit répond à « à quoi peut-il toucher ? ».

- **Chaque action est contrôlée.** Chaque action dans les portails de l'établissement est confrontée aux rôles de la personne avant de s'exécuter. Si rien ne l'autorise, elle est refusée, et le refus est enregistré.
- **Les rôles suivent les vrais métiers.** Les établissements partent de rôles prêts à l'emploi et peuvent créer les leurs, comme responsable des examens ou responsable de l'internat, dans un éditeur de rôles qui se lit comme des phrases simples. Les permissions se règlent par module et par action, et une permission pour un module que l'établissement n'a pas activé ne peut pas être accordée du tout.
- **Le périmètre peut être limité.** Un rôle peut être limité à certaines classes ou à certains départements. Un professeur principal ou un professeur de matière qui tente d'ouvrir une classe qu'il n'enseigne pas est refoulé.
- **Chaque portail est distinct.** Une même personne peut être membre du personnel et parent. Chaque portail a son propre ensemble d'actions, si bien qu'agir en tant que parent ne débloque jamais ce que cette personne peut faire en tant que membre du personnel.
- **Les changements s'appliquent aussitôt.** Lorsqu'un rôle ou un module change, les écrans ouverts sont mis à jour en quelques secondes. Chaque changement d'attribution des rôles est enregistré, et déclenche une alerte de sécurité.

Tenir les établissements à l'écart les uns des autres

Une seule plateforme sert de nombreux établissements : le cloisonnement le plus important est donc celui qui les sépare.

- L'établissement auquel appartient une demande est tiré de la session signée de la personne, et non de quoi que ce soit que son navigateur puisse choisir. Une demande qui désigne un autre établissement est refusée.
- La couche de données ajoute l'établissement à chaque requête qu'elle exécute, et refuse d'exécuter une requête d'établissement qui n'en désigne aucun.

- Notre propre administration de la plateforme est un monde à part, avec sa propre connexion, son propre cookie et ses propres permissions. Ce n'est pas une version renforcée d'un compte d'établissement, et aucun compte d'établissement ne peut y être élevé.

Un chiffrement à trois niveaux



Le chiffrement champ par champ : la note est lisible à l'infirmerie, et illisible pour tout ce qui regarde les données enregistrées.

- **En transit.** Tout le trafic entre les appareils des utilisateurs et la plateforme passe par HTTPS.
- **Au repos.** La base de données et le stockage de fichiers sont chiffrés au repos. Chaque fichier est chiffré au moment où il est écrit, et cette exigence est signée dans l'autorisation de chaque envoi, si bien qu'un navigateur ne peut pas s'en dispenser. Le service en production ne démarre pas si le chiffrement des fichiers est désactivé.
- **Champ par champ.** En plus, 167 champs sensibles répartis sur 79 types de dossiers sont chiffrés en AES-256-GCM avant d'être enregistrés : notes médicales et de l'infirmerie, dossiers de protection de l'enfance et de discipline, réclamations, procédures disciplinaires et évaluations du personnel, notes de recrutement, notes et adresses des familles, pièces d'admission et de transfert, sujets et réponses d'examens, et secrets de double authentification. Chaque saisie reçoit sa propre valeur aléatoire, chacune est scellée au champ auquel elle appartient pour ne pas pouvoir être déplacée vers un autre, et la clé est conservée hors de la base de données. Les clés peuvent être remplacées sans interrompre le service.
- **Le compromis assumé.** Un texte chiffré ne peut être ni recherché ni trié. Plutôt que de chiffrer un champ et de casser en silence la recherche qui en dépend, une courte liste de treize champs reste volontairement consultable par recherche, comme le texte des messages et les motifs de congé du personnel, et chacun est consigné avec sa raison dans la même liste qui pilote le chiffrement. Un contrôle automatisé bloque toute modification dans laquelle cette liste et le code ne concordent pas.
- **Les fichiers ne sont jamais publics.** Chaque fichier s'ouvre par un lien signé qui expire : en une heure pour la plupart des fichiers, en un jour pour les pièces jointes des messages, et en sept jours pour les photos de profil et les logos d'établissement, afin que les pages se chargent vite.

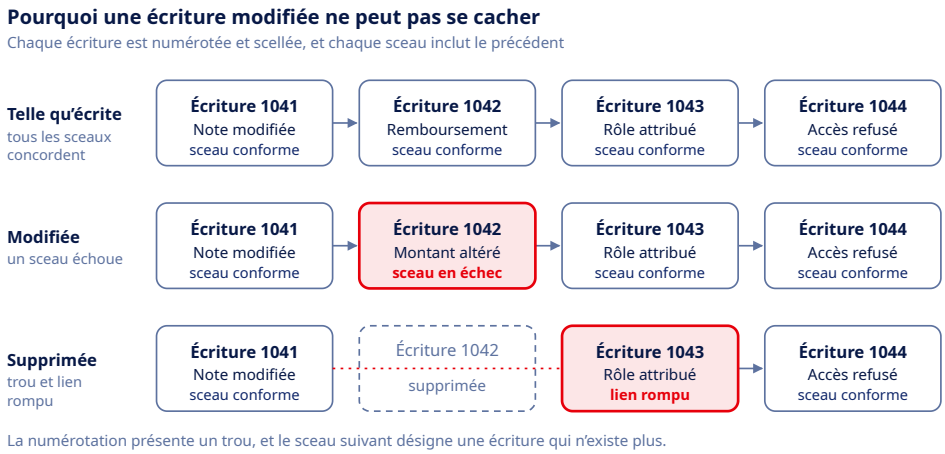
L'argent

- Les parents saisissent leurs données de carte chez Paystack, le prestataire de paiement, et elles n'atteignent jamais les serveurs d'EaseAcademia.

- Chaque avis de paiement de Paystack est vérifié par une signature cryptographique avant d'être pris en compte : personne ne peut simuler un paiement en appelant directement la plateforme.
- Le crédit prépayé de l'établissement est tenu dans un registre où chaque écriture est signée et liée à la précédente, si bien qu'un solde modifié à la main ne se vérifie pas.

Un registre qu'on ne peut pas modifier en douce

La prévention n'est jamais complète : la plateforme est donc conçue pour répondre à la question qui suit tout incident. Qui a fait quoi, quand, et quelqu'un a-t-il été refoulé ?



Les sceaux du journal d'audit : une écriture modifiée ne correspond plus à son propre sceau, et une écriture supprimée laisse un trou et un lien rompu.

- **Écrit là où la décision est prise.** L'écriture d'audit est créée au même endroit que celui qui accorde ou refuse une demande : le journal comprend donc les tentatives refoulées, souvent les écritures dont une enquête a le plus besoin.
- **Qui, tel qu'il était alors.** L'auteur de chaque action est consigné tel qu'il était au moment des faits, si bien que le journal reste compréhensible après un changement de rôle ou un départ.
- **Scellé et chaîné.** Chaque trace d'une action d'une personne, et chaque tentative refusée ou en échec, est numérotée dans l'ordre et scellée par une signature à clé qui inclut le sceau précédent. Chaque jour, un condensé de la chaîne est aussi écrit dans le stockage de fichiers, à l'écart de la base de données.
- **À votre disposition.** Les administrateurs d'un établissement peuvent rechercher dans leur propre journal par personne, par action, par dossier et par date, et l'exporter sous forme de tableur ou de données.

Repérer ce qui ne va pas

- L'activité est résumée chaque minute en mesures par établissement et par type d'action, et des alarmes se déclenchent lorsqu'une mesure franchit le seuil qui lui est fixé.
- Des alertes de sécurité sont émises pour les connexions suspectes, les tentatives répétées, les changements d'attribution des rôles, les réinitialisations de double authentification, les exports du journal d'audit et les activités inhabituelles.

- Lorsqu'un compte est bloqué après des échecs répétés, ou que sa double authentification est réinitialisée, le titulaire du compte en est informé dans l'application et par e-mail.
- Les cookies de connexion, les jetons de session et les en-têtes de sécurité sont masqués dans les journaux de requêtes de la plateforme, si bien qu'un journal ne peut jamais servir à prendre le contrôle d'une session.

Quand notre équipe doit regarder

Parfois, la seule façon de répondre à une demande d'assistance est de voir ce que voit l'établissement. Dans ce cas :

- la session est **en lecture seule** : rien ne peut être créé, modifié ni supprimé ;
- elle couvre **un seul établissement**, et exige un **motif déclaré** et une **nouvelle vérification de double authentification** pour commencer ;
- elle **prend fin d'elle-même**, au bout de vingt minutes par défaut et d'une heure au plus ;
- elle est **enregistrée**, avec le nombre d'actions effectuées, dans le journal d'audit propre à la plateforme.

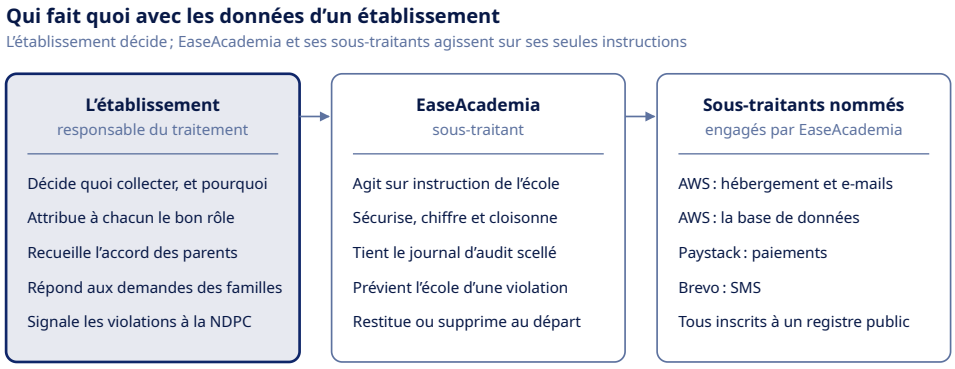
Comment le logiciel est construit

La plupart des défaillances de sécurité sont des erreurs ordinaires, pas des attaques. Les contrôles qui comptent s'exécutent donc automatiquement à chaque modification, et ceux qui protègent les données bloquent la modification au lieu de se contenter d'un avertissement.

- Chaque modification est analysée à la recherche de secrets oubliés dans le code, et de failles connues de gravité élevée dans les logiciels dont dépend la plateforme, y compris ceux qui viennent d'être ajoutés.
- Des contrôles automatisés vérifient que la liste de chiffrement et le code concordent, que les rôles limités le restent et que la base de données peut être construite à partir de rien, en plus de plus de 600 fichiers de tests automatisés et de 25 parcours scolaires complets répétés de bout en bout.
- Les réglages par défaut sont choisis pour rester sûrs quand quelqu'un oublie : le refus plutôt que la permission, et un service qui ne démarre pas plutôt qu'un service qui démarre affaibli.

Qui fait quoi avec les données d'un établissement

La loi sur la protection des données confie l'essentiel des obligations à l'établissement, parce que c'est lui qui décide de ce qui est collecté et pourquoi. EaseAcademia assume sa propre part par écrit, et engage à son tour les entreprises sur lesquelles il s'appuie.



Une responsabilité partagée : l'établissement décide, EaseAcademia agit sur ses instructions, et chaque sous-traitant ultérieur est nommé et engagé par écrit.

Le registre complet des sous-traitants ultérieurs, avec ce que chacun traite et où, fait partie de l'avenant relatif au traitement des données. La plateforme est hébergée chez ces prestataires internationaux reconnus, hors du Nigeria, et l'avenant engage EaseAcademia à appliquer des garanties appropriées à ce transfert.

La NDPA, le NDPR et la GAID en termes simples

Quelles règles s'appliquent aujourd'hui

Les premières règles nigérianes de protection des données étaient le **règlement nigérian de 2019 sur la protection des données (Nigeria Data Protection Regulation, NDPR)**. Elles ont été suivies d'une loi de l'Assemblée nationale, la **loi de 2023 sur la protection des données (Nigeria Data Protection Act, NDPA)**, qui a créé la **Commission nigériane de protection des données (NDPC)** chargée de la faire respecter. En mars 2025, la Commission a publié la **directive générale d'application et de mise en œuvre (General Application and Implementation Directive, GAID)**, qui précise comment la loi s'applique en pratique. Depuis l'entrée en vigueur de la GAID, le 19 septembre 2025, le NDPR et son cadre de mise en œuvre de 2020 ne s'appliquent plus.

Ainsi, lorsqu'on demande si un établissement est « conforme au NDPR », la question porte aujourd'hui sur la NDPA et la GAID. Elles s'appliquent à tout établissement qui conserve des informations personnelles sur des élèves, des parents ou du personnel, quel que soit le logiciel utilisé, et que ses dossiers soient sur papier ou en ligne.

Ce que la loi demande à un établissement

L'établissement est le **responsable du traitement** : ces obligations sont donc les siennes. Concrètement, un établissement doit :

- ne collecter que les informations dont il a besoin, dans un but clair et sur une base légale, et ne pas les garder plus longtemps que ce but ne l'exige ;
- obtenir le consentement d'un parent ou d'un responsable légal lorsque les informations d'un enfant l'exigent, par des moyens adaptés pour vérifier l'âge et le consentement. Selon l'article 31 de la loi, un enfant est toute personne de moins de 18 ans ;
- faire preuve d'un soin particulier avec les données personnelles sensibles, comme les informations de santé ;

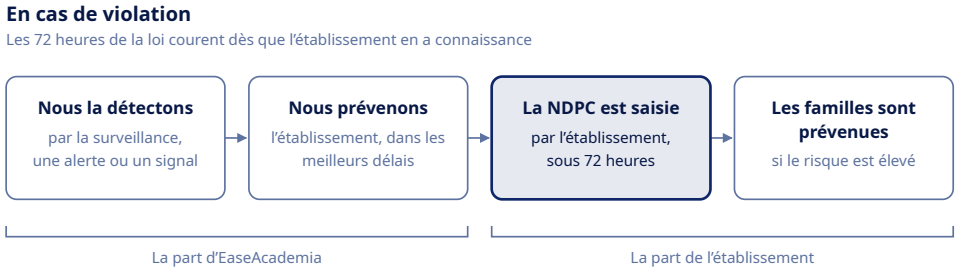
- garder toutes les données personnelles en sécurité, avec des mesures techniques et organisationnelles adaptées ;
- permettre aux élèves, aux parents et au personnel de consulter, corriger, supprimer ou obtenir une copie des informations qui les concernent, et de s'opposer à leur utilisation, lorsqu'ils le demandent ;
- signaler une violation de données personnelles à la Commission dans les 72 heures après en avoir pris connaissance, et prévenir directement les personnes concernées lorsque le risque pour elles est élevé (article 40) ;
- s'assurer que toute entreprise qui traite ces informations pour son compte est tenue par écrit de les protéger, et que les informations envoyées à l'étranger restent correctement protégées.

Enregistrement, DPO et sanctions

Un responsable du traitement qui traite les données personnelles de plus de 200 personnes en six mois est considéré comme un **responsable du traitement d'importance majeure**, selon les lignes directrices de 2024 de la Commission relatives à l'article 44. En comptant les élèves, les parents et le personnel, la plupart des établissements dépassent ce chiffre. Les responsables d'importance majeure doivent s'enregistrer auprès de la Commission, désigner un **délégué à la protection des données (DPO)** et déposer des déclarations d'audit de conformité.

Selon l'article 48, un responsable d'importance majeure encourt une amende pouvant atteindre 10 millions de nairas ou 2 % de son chiffre d'affaires annuel brut de l'exercice précédent, le montant le plus élevé étant retenu. Pour les autres responsables, le montant est de 2 millions de nairas ou 2 %, le plus élevé étant retenu.

La Commission s'intéresse à l'éducation. En février 2026, elle a adressé des avis de mise en conformité à 649 établissements d'enseignement supérieur, leur demandant sous 21 jours leurs déclarations d'audit, les coordonnées de leur DPO, leur enregistrement et un résumé de leurs mesures techniques et organisationnelles. Lorsqu'on demande ce résumé à un établissement, ce guide et la page sécurité décrivent la part de la réponse qui revient à la plateforme.



En cas de violation : EaseAcademia prévient l'établissement dans les meilleurs délais, pour qu'il puisse tenir son propre délai de 72 heures.

Comment EaseAcademia aide pour chaque obligation

Aucun logiciel ne rend un établissement conforme à lui seul. Ce qu'EaseAcademia apporte, ce sont les mesures que la loi attend, déjà construites, ainsi que ses propres engagements par écrit. La colonne de droite reste du ressort de l'établissement, quel que soit son prestataire.

Ce que la loi attend	Ce qu'EaseAcademia apporte	Ce qui reste à l'établissement
Ne collecter que le nécessaire	Les champs facultatifs restent facultatifs, et les modules qu'un établissement n'a pas activés ne collectent rien	Décider quoi collecter et pourquoi, et en informer les familles dans une notice de confidentialité
Le consentement pour les données des enfants	Des formulaires de consentement envoyés aux parents dans leur portail, chaque réponse étant enregistrée avec son auteur et sa date	Décider quand le consentement est nécessaire et ce que dit chaque formulaire
La sécurité	Tout ce que décrit ce guide	Attribuer les rôles avec soin, retirer rapidement ceux qui partent, et imposer la double authentification au personnel
L'accès et les copies	Les parents, les élèves et le personnel consultent leurs propres dossiers dans leurs portails ; les dossiers financiers et le journal d'audit s'exportent depuis l'application ; une copie complète des données de l'établissement est fournie sur demande	Répondre à chaque demande dans les délais
La rectification	Le personnel peut demander la modification de son profil et contester des inscriptions de son dossier professionnel ; le secrétariat corrige directement les dossiers des élèves et des familles	Examiner chaque demande et faire la correction
La suppression et la conservation	Les administrateurs peuvent supprimer des dossiers ; les coordonnées des anciens élèves sont effacées automatiquement au bout de sept ans, ou aussitôt s'ils le demandent ; les brouillons d'admission abandonnés sont effacés	Fixer la durée de conservation de chaque type de dossier
La responsabilité	Le journal d'audit scellé, consultable et exportable	Le passer en revue, et déposer les déclarations d'audit de conformité de l'établissement
Le signalement des violations	Des alertes de sécurité et une surveillance, et l'engagement écrit de prévenir l'établissement dans les meilleurs délais	Saisir la Commission sous 72 heures, et prévenir les personnes concernées
Un accord écrit avec le sous-traitant	Un avenant relatif au traitement des données publié ; un exemplaire contresigné est disponible sur demande	En conserver un exemplaire signé
Les transferts à l'étranger	Des prestataires internationaux nommés, avec des garanties appropriées prévues par l'avenant	Indiquer dans la notice de confidentialité que les données sont hébergées à l'étranger
L'enregistrement et le DPO	Ce guide, l'avenant et le registre des sous-traitants, prêts pour les déclarations de l'établissement	S'enregistrer auprès de la Commission si nécessaire, et désigner un DPO

Cette section est un résumé en termes simples, pas un avis juridique. Faites-vous conseiller sur les obligations propres à votre établissement au titre de la loi et de la GAID.

Pourquoi c’est plus solide que les pratiques courantes

Une grande partie des données personnelles détenues aujourd’hui par les établissements ne se trouve pas dans un système dédié et protégé. Elle se trouve dans les outils qui étaient à portée de main quand l’établissement était petit.

Pratique courante	Le risque	Sur EaseAcademia
Un seul mot de passe administrateur partagé pour le logiciel de l’établissement	Personne ne sait qui a fait quoi, et ceux qui partent gardent le mot de passe	Chacun se connecte en son nom, l’établissement peut imposer la double authentification à tout son personnel, et un compte désactivé cesse de fonctionner en quinze minutes au plus
Listes d’élèves et registres de frais dans des tableurs sur des ordinateurs personnels et des clés USB	Un appareil perdu, c’est un registre perdu, et personne ne sait combien de copies existent	Un seul dossier, chiffré au repos, avec des fichiers ouverts par des liens qui expirent
Questions de classe et de frais gérées dans des groupes WhatsApp	Les informations des enfants et les numéros des parents restent sur des téléphones personnels, hors du contrôle de l’établissement	Les messages et les annonces passent par la plateforme, uniquement vers les personnes que chaque rôle autorise
Un serveur dans le bureau de l’établissement	Vol, coupures de courant et mises à jour de sécurité oubliées	Une infrastructure cloud gérée par des professionnels, avec la base de données et les fichiers chiffrés au repos
Un logiciel où chaque membre du personnel voit tout	Un professeur principal peut ouvrir le livre des frais ; un intendant peut modifier une note	Toute action est refusée sauf si un rôle l’autorise, et les rôles peuvent être limités à certaines classes
Aucune trace des modifications	Un litige sur une note modifiée reste sans réponse	Un journal d’audit scellé de chaque modification et de chaque tentative refusée
Notes de santé et de protection de l’enfance enregistrées en clair	Une seule copie divulguée de la base de données expose les notes les plus sensibles de l’établissement	Ces notes sont chiffrées champ par champ, avec la clé conservée hors de la base de données
Aucun accord écrit avec le prestataire	Au titre de la NDPA, l’établissement porte seul le risque de son prestataire	Un avenant relatif au traitement des données publié et un registre public des sous-traitants ultérieurs

Questions à poser à tout prestataire, nous compris

Question	La réponse d’EaseAcademia
Qui maîtrise les données ?	L’établissement. EaseAcademia est son sous-traitant, selon un avenant relatif au traitement des données publié.
Vendez-vous les données, ou les utilisez-vous pour la publicité ?	Non. Ni ce site ni les portails ne contiennent de traceurs publicitaires ou de mesure d’audience.
Comment les mots de passe sont-ils conservés ?	Sous forme d’empreintes Argon2id à sens unique. Personne chez EaseAcademia ne peut lire un mot de passe.

Question	La réponse d'EaseAcademia
Pouvons-nous imposer la double authentification ?	Oui, à chaque membre du personnel, avec une application d'authentification, dix codes de secours et un délai de grâce fixé par l'établissement. Les parents peuvent l'activer pour eux-mêmes. Il n'existe aucun code par SMS ou par e-mail.
Qu'est-ce qui est chiffré au-delà du disque ?	167 champs sensibles répartis sur 79 types de dossiers, chacun chiffré séparément en AES-256-GCM.
Puis-je voir qui a modifié une note, et qui a été refoulé ?	Oui. Les deux figurent dans le journal d'audit de l'établissement, qu'il peut consulter et exporter.
Votre personnel peut-il voir nos données ?	Uniquement par une session d'assistance en lecture seule, limitée à un établissement, qui exige un motif déclaré et une nouvelle vérification de double authentification, prend fin en une heure au plus et est enregistrée.
Qui d'autre traite nos données ?	AWS, Paystack et Brevo, chacun nommé avec ce qu'il traite dans un registre public.
Pouvons-nous emporter nos données ?	Les dossiers financiers et le journal d'audit s'exportent depuis l'application, et une copie complète des données de l'établissement est fournie sur demande. Lorsqu'un établissement part, il choisit si ses données lui sont restituées ou supprimées.

Ce que nous ne revendiquons pas encore

Un document de confiance ne vaut d'être lu que s'il est honnête sur ses limites. Voici ce qu'un examinateur attentif pourrait demander et qu'EaseAcademia ne propose pas encore :

- **Des certifications.** EaseAcademia ne détient pas de certification ISO 27001 ni SOC 2.
- **Un test d'intrusion indépendant.** Il n'existe pas de rapport de test d'intrusion réalisé par un tiers à partager.
- **Des garanties de service.** Il n'existe pas de garantie publiée de disponibilité ni de délai de rétablissement.
- **Une double authentification obligatoire pour les parents.** Un établissement peut imposer la double authentification à son personnel, mais pour les parents elle reste un choix personnel.
- **L'export complet en libre-service.** Une copie complète des données d'un établissement se demande à l'assistance ; ce n'est pas un bouton dans l'application.
- **Des durées de conservation fixées par l'établissement.** Un établissement ne peut pas encore fixer ses propres délais de suppression automatique ; les dossiers sont supprimés par ses administrateurs ou sur demande.

Lorsque l'un de ces points changera, ce guide le dira.

Signaler un problème

- **Une faille de sécurité :** écrivez à security@easeacademia.com avec les détails et les étapes pour la reproduire. Les recherches de bonne foi qui respectent la vie privée des personnes sont les bienvenues, et nous demandons un délai raisonnable pour corriger un problème avant qu'il ne soit rendu public.
- **Une question ou une demande sur la protection des données :** écrivez à dpo@easeacademia.com ou à privacy@easeacademia.com. Les demandes portant sur le dossier d'un élève ou d'un parent sont transmises à l'établissement, puisque c'est lui le responsable du traitement.

- **Pour tout le reste :** utilisez « Signaler un problème », présent sur chaque écran, ou écrivez à support@easeacademia.com.

La page sécurité, la politique de confidentialité et l'avenant relatif au traitement des données donnent le détail formel qui sous-tend ce guide.

La version la plus récente de ce document se trouve toujours à l'adresse https://easeacademia.com/fr/resources/trust-and-security.