APD
Autorité de protection des données

LA PROTECTION DES DONNÉES **À L'ÉCOLE EN 7 ÉTAPES**

Selon le nouveau Règlement général sur la Protection des données (RGPD) de l'UE

Tables des matières

Qu'est-ce que le Règlement général sur la protection des données (RGPD) ?

Le Règlement général sur la protection des données (RGPD) est un nouveau règlement européen qui fixe des règles que les autorités publiques, les entreprises et toutes les autres organisations doivent respecter lorsqu'elles traitent des données à caractère personnel.

Le RGPD offre aux citoyens une meilleure protection lors du traitement[1] de leurs données à caractère personnel. Cette nouvelle législation est basée sur la législation existante en matière de protection de la vie privée mais renforce un certain nombre de règles, apporte des précisions ou constitue une extension à la législation actuelle. Comme l'écrivait la Commission vie privée, devenue entre-temps l'Autorité de protection des données : « Un vent nouveau est annoncé, pas un ouragan ».

Le nouveau Règlement est entré en vigueur le 25 mai 2018.

Les écoles traitent de nombreuses données à caractère personnel.

Citons par exemple les données des (anciens) élèves et de leurs parents, des enseignants et du personnel d'encadrement. Dans le cadre du traitement de données à caractère personnel, les écoles seront soumises au RGPD.

Quels sont les principaux changements pour les écoles ?

- **Une plus grande responsabilité de celui qui traite les données.**

  L'école devra démontrer elle-même qu'elle traite les données à caractère personnel selon les règles du RGPD.

- Les écoles doivent **désigner un interlocuteur** qui connaît cette législation et qui pourra aider à la mettre en œuvre au sein de l'école.

- L'école doit tenir un **registre des activités de traitement**.

  Un registre des activités de traitement reprend entre autres quelles données à caractère personnel sont traitées par l'école, pour quelles finalités sont-elles utilisées, d'où proviennent ces données et avec qui elles sont partagées.

- La législation prévoit **une obligation de notification** en cas de fuites de données.

  Par exemple, en cas de fuites de données à caractère personnel sensibles, vous êtes obligé, en tant qu'école, de notifier les fuites de données à l'Autorité de protection des données (et éventuellement aux personnes concernées).

- **Un contrôle renforcé**

  En cas de non-respect du RGPD, l'Autorité de protection des données peut imposer des sanctions ainsi que des amendes.

1 Le terme « traitement » recouvre la collecte ou la réclamation, l'enregistrement, l'utilisation et l'échange de données à caractère personnel.

En tant qu'école, comment devez-vous traiter des données à caractère personnel ?

Les principes essentiels auxquels une école doit satisfaire lors du traitement de données à caractère personnel sont les suivants :

- Traitez les données à caractère personnel pour **des finalités déterminées et légitimes**.
  Utilisez les données à caractère personnel uniquement dans ce but.

  Exemple : pour des raisons d'administration des élèves, une école connaît l'adresse du domicile de tous les élèves.
  Ce n'est pas parce qu'une école dispose des données que celles-ci peuvent être transmises à une autre école ou que l'école peut les utiliser pour diffuser une liste d'adresses aux parents.

- **Soyez transparent** lors du traitement des données à caractère personnel.
  Expliquez pourquoi l'école va traiter certaines données à caractère personnel.

- Tout traitement de données à caractère personnel n'est légitime que s'il satisfait à au moins un des fondements légaux.

Les principaux fondements légaux sur lesquels une école peut se baser sont :

- **L'obligation légale** : si la loi l'impose, les données à caractère personnel peuvent être traitées.
  Il s'agit par exemple de données administratives et d'accompagnement de l'élève.
- **Le contrat** : les données à caractère personnel des élèves et des enseignants peuvent être traitées si elles sont nécessaires à l'exécution d'un contrat.
  Par exemple : une photo d'identité d'un élève qui est demandée et qui apparaît sur une carte d'élève afin de lui permettre d'avoir accès à toutes sortes de services proposés par l'école.
- **Le consentement** : le consentement des élèves ou des parents des élèves de moins de 16 ans est nécessaire au traitement de données à caractère personnel pour certaines finalités.
  Par exemple : pour publier des photos d'élèves sur le site Internet de l'école, un consentement sera nécessaire.

- Une école **ne traite pas plus de données à caractère personnel que nécessaire** pour atteindre la finalité déterminée et légitime.
  Par exemple : lors de l'inscription d'un élève, l'école ne doit pas connaître les revenus des parents.

- Les données à caractère personnel traitées par une école **doivent être exactes et pouvoir être corrigées**.
  Par exemple : en cas de déménagement d'un élève, l'école peut adapter l'adresse.

- **Ne conservez pas les données à caractère personnel plus longtemps que nécessaire.**
  Pour certaines données d'élèves, un délai de conservation légal s'applique.
  Respectez le délai de conservation légal des données à caractère personnel.

- En tant qu'école, prenez des mesures appropriées afin de protéger les données à caractère personnel contre les traitements non autorisés.

L'autorité scolaire est responsable du respect de ces principes et doit pouvoir le démontrer.

En tant qu'école, comment s'y prendre ?

Depuis le 25 mai 2018, chaque école doit se conformer au RGPD. Le plan par étapes sert de guide pour mettre en œuvre le nouveau Règlement.

ÉTAPE 1 – Informer et sensibiliser

La sécurité de l'information à l'école est l'affaire de chacun : directeur, enseignants, parents, élèves et apprenants, équipe de nettoyage, concierge, bénévoles, ...

Pendant le processus de conscientisation, assurez-vous que chacun soit au courant de la nouvelle réglementation et veille de manière correcte à la sécurité des données à caractère personnel.

Astuces :

- Ouvrez la discussion autour de la sécurité de l'information et prêtez-y attention lors des moments de concertation : réunions du personnel, association des parents d'élèves, concertation école-centre PMS, ...
- Adaptez si nécessaire les textes suivants : le règlement scolaire, le règlement de travail, la déclaration de confidentialité, le plan de sécurité de l'information, la politique de communication et le plan stratégique en matière d'ICT, ...

ÉTAPE 2 – Désigner un DPO ainsi qu'un point de contact à l'école

- Le RGPD oblige certaines organisations à désigner **un délégué à la protection des données** (« DPO » pour Data Protection Officer). Ce délégué peut être désigné pour plusieurs organisations à condition qu'il soit joignable et disponible pour répondre aux demandes de toutes ces organisations.

  Un délégué à la protection des données veille à ce qu'une organisation satisfasse aux actuelles lois et réglementations en vigueur en matière de vie privée.

- En tant qu'école, désignez **un interlocuteur**.

  Il est par ailleurs important de savoir que l'interlocuteur de l'école n'endosse pas la responsabilité finale du respect du RGPD. Cette responsabilité finale du respect du RGPD incombe à l'autorité scolaire.

ÉTAPE 3 – Tenir un registre des activités de traitement

Le registre doit être établi de manière électronique et tenu à jour.

Respectez le principe de minimisation des données et détruisez les données qui ne sont pas nécessaires ou dont la conservation ne peut être légitimée.

Astuces

- Répertoriez soigneusement les données à caractère personnel qui sont traitées par l'école.

  Posez aussi les questions suivantes :

- Pour quelles finalités l'école utilise-t-elle les données ?
- Où les données sont-elles conservées (PC, papier, supports externes, documents dans le cloud) ?
- Avec quelles parties internes et quelles parties externes les données sont-elles partagées ?
- L'école répond-elle à une obligation légitime pour traiter les données ?
- Combien de temps les données sont-elles conservées ?

  Vérifiez d'abord s'il existe des délais de conservation légaux pour la conservation des données. Si ce n'est pas le cas, appliquez le principe « ne pas conserver plus longtemps que nécessaire », en précisant cette nécessité.

- Qui a accès aux données à caractère personnel ?

  Vérifiez qui précisément a accès aux données à caractère personnel (lire, modifier, supprimer, ...) et comment les données sont protégées. Attention, l'accès peut être aussi bien numérique que physique.

ÉTAPE 4 – Contrats avec des partenaires

Les écoles font souvent appel à des parties externes ou à certains services ICT qui conservent des données à caractère personnel pour elles.

Ainsi, par exemple, les écoles ont recours à des fournisseurs de kits numériques pour des systèmes d'administration et de suivi des élèves, des systèmes d'administration du personnel et du matériel didactique. Le RGPD qualifie ce genre de fournisseurs de «sous-traitants». Les contrats avec ces fournisseurs doivent être réexaminés à la lumière du RGPD.

4.1 – Passez en revue vos contrats de sous-traitance et demandez-vous si vos contrats mentionnent :

1.	Les finalités et la nature du traitement, le type de données, les catégories de personnes concernées et les droits et obligations des deux parties	☐ OUI	☐ NON
2.	Que le fournisseur garantit qu'il ne traitera les données à caractère personnel que sur la base des instructions écrites de l'école et qu'il ne les utilisera pas pour quelque autre finalité (sauf obligation légale explicite)	☐ OUI	☐ NON
3.	Que le fournisseur garantit qu'il prendra les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque	☐ OUI	☐ NON
4.	Que le fournisseur s'engage à ne recrutera aucun autre sous-traitant sans l'autorisation écrite préalable de l'école	☐ OUI	☐ NON
5.	Que le fournisseur garantit que les personnes qu'il a autorisées à traiter les données à caractère personnel (par ex. des techniciens chargés de la gestion du service) se sont engagées à respecter la confidentialité ou sont tenues par une obligation légale de confidentialité appropriée	☐ OUI	☐ NON
6.	Que le fournisseur est d'accord d'aider, dans toute la mesure du possible, l'école à s'acquitter de son obligation de donner suite aux demandes dont les personnes concernées la saisissent en vue d'exercer leurs droits	☐ OUI	☐ NON
7.	Que le fournisseur se déclare disposé, le cas échéant, à aider l'école à garantir le respect de ses obligations en ce qui concerne la sécurité, la notification et/ou la communication d'une fuite de données et l'analyse d'impact relative à la protection des données	☐ OUI	☐ NON
8.	Que les données ne sont pas transmises en dehors de l'Union européenne vers des pays qui n'offrent pas un niveau de protection adéquat ou sans garanties appropriées complémentaires qui seront d'abord convenues avec l'école	☐ OUI	☐ NON
9.	Que le fournisseur garantit qu'au terme de la prestation de services, toutes les données à caractère personnel seront supprimées en toute sécurité ou renvoyées à l'école et que les copies existantes seront détruites	☐ OUI	☐ NON
10.	Que le fournisseur est d'accord de mettre à la disposition de l'école toutes les informations nécessaires pour démontrer le respect de ses obligations et pour permettre la réalisation d'audits, y compris des inspections, par l'école ou par un autre auditeur qu'elle a mandaté, et de contribuer à ces audits.	☐ OUI	☐ NON

Astuces

- Dressez une liste de tous les logiciels au sein de l'école qui collectent des données à caractère personnel.
- N'oubliez pas les applications. Réunissez également les contrats avec les fournisseurs de ces applications.
- Évaluez les contrats actuels et futurs avec des prestataires de services externes et apportez-y les changements nécessaires. Dans ce cadre, tenez compte des mentions listées au point 4.1 de cette brochure.

ÉTAPE 5 – Contrôler si le consentement est nécessaire

Le registre des activités de traitement permet à l'école de contrôler quelles données à caractère personnel requièrent un consentement.

Par exemple : des photos ou des vidéos sur lesquelles des personnes sont reconnaissables sont également des données à caractère personnel. Si l'école veut utiliser les images afin de les placer sur le site Internet de l'établissement, ce n'est possible qu'avec le consentement de la personne qui apparaît à l'image (ou de ses parents).

Astuces

Vérifiez de quelle manière le consentement est demandé et soumettez la procédure à la check-list suivante :

- Utilisez un langage clair, sans petits caractères ;
- Indiquez pourquoi les données sont utilisées et ce qu'il en sera fait ;
- Indiquez aussi de quelle manière les données peuvent être consultées et modifiées ;
- Mentionnez également le droit à l'oubli. Dans certains cas, vous ne pouvez pas supprimer les données d'une personne parce que la loi ne le permet pas. Mentionnez-le aussi dans le texte ;
- Le consentement doit être exprimé par un acte positif.

  Par exemple : si vous comptez régler le consentement via un formulaire électronique, la case ne peut pas être cochée automatiquement.

- Si le consentement n'est pas donné, cela ne peut pas avoir de conséquences négatives pour la personne concernée.

  Par exemple : si des parents ne donnent pas leur consentement pour la publication de photos de leur enfant sur Facebook, cela ne peut pas avoir d'autres conséquences pour l'enfant.

ÉTAPE 6 - Sécurité physique et sécurité de l'infrastructure ICT

Sécurité physique

Il est recommandé que l'école limite l'accès aux espaces où sont situées ou utilisées/traitées des données à caractère personnel aux personnes habilitées. Il en va de même pour les locaux de serveurs contenant des données sécurisées.

Astuce

- Prenez des mesures préventives et évitez ainsi les dommages causés par le feu, les inondations, etc. Par exemple : détection d'incendie appropriée, extincteurs, ...

Sécurité ICT

Une installation, des réseaux et des serveurs IT bien sécurisés sont une condition connexe pour la sécurisation de données.

Des supports de stockage amovibles comme des caméras, des disques durs externes, des CD et des clés USB sont une source potentielle d'infection par des logiciels malveillants (malwares). Les supports de stockage amovibles sont aussi à l'origine de la perte d'informations sensibles dans de nombreuses organisations.

En tant qu'école, prenez dès lors les mesures nécessaires pour prévenir le risque de pertes de données.

Astuces

- Protégez vos appareils contre les menaces telles que les virus et autres malwares.
- Effectuez régulièrement des sauvegardes.
- Évaluez votre politique d'accès.
- Apprenez à votre personnel et à vos élèves comment reconnaître des fichiers infectés, que faire avec de tels fichiers et comment télécharger en toute sécurité.
- Décidez si le personnel et les élèves ont la permission d'utiliser des appareils mobiles ou de télécharger des fichiers sur les équipements scolaires.

  Fixez-en bien les conditions.
- Appliquez strictement les règles de base concernant la sécurisation au moyen de mots de passe et veillez à ce que les élèves et le personnel les respectent rigoureusement.
- Autorisez l'utilisation de dispositifs amovibles uniquement dans le cadre des cours et exigez que les enseignants et les élèves scannent tout support amovible contre les malwares avant utilisation. Apprenez-leur à exécuter une telle procédure avec succès.
- Évitez d'enregistrer des données d'élèves ou de collègues sur des dispositifs amovibles sauf s'il n'est pas possible de faire autrement. Dans ce cas, codez ou cryptez les données à l'aide d'un mot de passe.

Points d'attention supplémentaires concernant les données à caractère personnel

- **Attention au phishing !**

  Le phishing est une fraude en ligne par laquelle le fraudeur amène la victime sur une fausse page Internet. Cela représente l'un des plus grands risques pour la sécurité. Discutez-en avec le personnel de manière à ce que le risque qu'une personne transfère des données sensibles soit limité.

- Ne laissez aucun document sensible sur les imprimantes en libre accès.
- Pour le cryptage d'un accès à des données sensibles, utilisez une authentification à deux facteurs.
- Conservez vos mots de passe dans un endroit sûr.
- Déconnectez-vous toujours des sessions ouvertes

ÉTAPE 7 - Violations de données à caractère personnel et obligation de notification

Une fuite de données est une situation dans laquelle des données à caractère personnel risquent d'être rendues publiques de manière non autorisée, perdues, détruites ou altérées.

Parmi les exemples de fuites de données, citons :

- le vol intentionnel de données par des cybercriminels (hacking, phishing) ;
- la perte ou le vol de supports amovibles (disque dur externe, clé USB, ordinateur portable, ...) ;
- des défaillances techniques. Par exemple : une brèche dans un logiciel ;
- la négligence dans l'emploi ou la communication de mots de passe ;
- l'envoi accidentel d'un e-mail avec divulgation de données à caractère personnel.

TO DO POUR LES ÉCOLES

- Tenez un registre interne des incidents et prévoyez une procédure interne afin de détecter, rapporter, analyser et si nécessaire notifier des violations.
- Vous devez journaliser chaque incident en interne.

Si l'incident peut provoquer toute forme de dommage à la (aux) personne(s) concernée(s), notifiez l'incident à votre délégué à la protection des données qui doit avertir l'Autorité de protection des données dans les 72 heures.

En cas de risque élevé pour les droits et libertés, vous devez également notifier l'incident à la (aux) personne(s) concernée(s) elle(s)-même(s).

Exemple : une notification à l'Autorité de protection des données et aux personnes concernées est nécessaire en cas de vol de données non cryptées contenant des informations médicales des élèves.

Vous voulez en savoir plus sur le RGPD ?

- L'Autorité de protection des données a conçu un vaste portail comportant un dossier thématique sur le RGPD. Vous pouvez aussi y consulter le plan général par étapes : « RGPD - Préparez-vous en 13 étapes ! » https://www.autoriteprotectiondonnees.be/

- Consultez la brochure technique détaillée pour les écoles, spécifiquement pour les directions, les coordinateurs ICT et/ou les points de contact.

- Si vous cherchez des informations et de l'inspiration, le site Internet axé sur l'enseignement de l'Autorité de protection des données, www.jedecide.be constitue un outil utile et une source d'informations, en particulier si vous souhaitez aborder ces thèmes avec les élèves. Le site comporte un volet pour les jeunes ainsi qu'un autre pour les parents et pour l'enseignement.