Education International
Internationale de l'Education
Internacional de la Educación

http://www.ei-ie.org

RÉGION EUROPÉENNE - CSEE

Présidente
Christine BLOWER

Vice-Président(e)s
Odile CORDELIER
Andreas KELLER
Trudy KERPERIEN
Dorte LANGE
Galina MERKULOVA
Branimir STRUKELJ

5, Bd du Roi Albert II, 9e
1210 Bruxelles, Belgique
Tél : +32 2 224 06 91/92
Fax : +32 2 224 06 94
secretariat@csee-etuce.org
http://www.csee-etuce.org

Directrice européenne
Susan Flocken

Trésorier
Mike JENNINGS

Lignes directrices du CSEE concernant le nouveau Règlement général de l'UE en matière de protection des données (RGPD)

Adoptées par le Bureau du CSEE LE 29 mai 2018

Le nouveau Règlement général en matière de protection des données (RGPD) entre en vigueur le 25 mai 2018 au niveau national. Cette nouvelle disposition aura une incidence sur la protection des données et la confidentialité des informations personnelles des étudiant(e)s, des enseignant(e)s et des syndicalistes, comme mentionné dans la Déclaration du CSEE relative au Plan d'action 2020 de l'UE en matière d'éducation numérique.

Position générale du CSEE concernant le nouveau RGPD

La protection des données, la confidentialité des informations personnelles et la cybersécurité dans les écoles et les syndicats sont des éléments fondamentaux. Enseignant(e)s, écoles et syndicalistes doivent considérer l'introduction du RGPD comme un moyen d'améliorer leur façon de gérer les données personnelles. Le nouveau RGPD doit respecter les systèmes de protection des données existants et uniquement être utilisé à titre complémentaire pour renforcer la sécurité, si nécessaire.

L'adaptation du RGPD engendre en effet une charge administrative et technique. Les enseignant(e)s et leurs syndicats doivent donc être impliqués dans la mise en œuvre du RGPD au niveau national, en particulier pour éviter que de nouvelles exigences et charges de travail ne pèsent sur les enseignant(e)s lors de l'application de politiques conformes en matière de protection des données ou que cette nouvelle responsabilité ne leur soit déléguée. Les employeurs de l'éducation ont la responsabilité de garantir que leurs établissements scolaires soient conformes au RGPD et bénéficient des fonds publics nécessaires, en particulier pour l'achat, l'adaptation et l'installation de logiciels et de matériel pour le transfert de l'information. Si le nouveau RGPD va de pair avec davantage de responsabilités, ce dernier ne doit pas pour autant engendrer des sanctions plus lourdes ou des exigences fastidieuses pour démontrer la conformité aux nouvelles normes en matière de protection des données, tant dans les processus automatiques que manuels.

Lignes directrices du CSEE pour assurer la conformité au nouveau RGPD[1] et minimiser les risques inhérents à la gestion de la protection des données dans les écoles et les syndicats

1. Désigner un responsable du traitement des données (ex. une autorité compétente) chargé de tenir un registre de tous les processus de traitement des données placés sous la responsabilité de l'entité et désigner un **sous-traitant** (ex. direction d'établissement scolaire) chargé de tenir un registre de tous les traitements de données effectués au nom du responsable du traitement.

2. Garantir que le **responsable du traitement** (« data controller ») **et le sous-traitant** (« data processor ») s'acquittent de leur obligation de nommer **un délégué à la protection des données (DPD)**. Par ailleurs les écoles et les syndicats doivent garantir que les prestataires

[1] Pour de plus amples informations, veuillez consulter le Guide pratique du RGPD pour les syndicalistes (mars 2018).

tiers autorisés à traiter leurs données soient conformes au RGPD et veiller à conclure des contrats juridiquement contraignants avec toute entreprise chargée de traiter leurs informations à caractère personnel.

3. Le DPD doit veiller à **garantir un niveau de sécurité suffisant en utilisant les moyens techniques et organisationnels appropriés** tels que la « pseudonymisation » et le cryptage des données personnelles. Il doit en outre assurer la confidentialité, l'intégrité, la disponibilité et la résilience des systèmes et services de traitement ; la restauration rapide de l'accès aux données personnelles en cas de problème technique ou physique ; ainsi qu'un processus d'évaluation régulière et un contrôle de l'efficacité des mesures techniques et organisationnelles pour garantir la sécurité du traitement.

4. La mise en place de mesures adéquates pour garantir le **principe du traitement licite des données** est au cœur du nouveau RGPD. Cela signifie que les données à caractère personnel doivent être :
a) traitées de manière licite, loyale et transparente au regard de la personne concernée ;
b) collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités ;
c) adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées ;
d) exactes et, si nécessaire,

1. tenues à jour, (les données à caractère personnel qui sont inexactes doivent être effacées ou rectifiées sans tarder ;
2. conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées ;
3. traitées de façon à garantir une sécurité appropriée des données à caractère personnel.

5. Développer une approche permettant de se mettre en conformité avec la condition selon laquelle **un consentement explicite devra être obtenu** dans tous les cas où le traitement des informations personnelles ne fait plus partie de l'administration ordinaire des écoles, en particulier lorsque des tiers interviennent dans la gestion des données. Un consentement explicite des parents (ou des élèves eux/elles-mêmes en fonction de l'âge et de la situation) est obligatoire en cas d'utilisation des données personnelles (de leurs enfants) en dehors de la gestion habituelle de l'école. La personne concernée doit consentir au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques afin de pouvoir protéger ses intérêts légitimes. Ce consentement doit être considéré comme un « acte libre, clair et affirmatif » - si cocher une case peut s'avérer une méthode de consentement efficace, les cases pré-cochées ne le sont pas. Le consentement doit être donné dans le cadre d'une déclaration écrite « qui la distingue clairement des autres questions, sous une forme compréhensible, aisément accessible et formulée en des termes clairs et simples ».

6. Les catégories particulières de données à caractère personnel (particulièrement sensibles) comprennent l'appartenance syndicale et celles qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne. Le traitement est plus strict dans le cadre des activités légitimes ou à des fins syndicales. Dans ces deux cas, des mesures de sécurité doivent être mises en place et le traitement doit se rapporter exclusivement aux membres et aux anciens membres de l'organisation ou aux personnes entretenant des contacts réguliers avec cette dernière et avec ses finalités. Les données à caractère

personnel ne peuvent pas être communiquées en dehors de cette organisation sans le consentement des personnes concernées. Un consentement explicite doit être donné pour autoriser le traitement des données. Le traitement et la sauvegarde des intérêts vitaux de la personne concernée est nécessaire aux fins de l'exécution des obligations et de l'exercice des droits propres en matière de droit du travail et de sécurité sociale.

7. Le DPD a l'obligation **de communiquer les informations** aux personnes qui demandent leurs données personnelles et de faciliter l'exercice des droits de la personne concernée. Ceci implique le **droit d'accès** (gratuit et à des intervalles raisonnables, afin de vérifier la licéité du traitement), le **droit de rectification** (sans délai) et le **droit à l'oubli ou le droit d'obtenir l'effacement des données sans délai** (si les données à caractère personnel ne sont plus nécessaires aux fins pour lesquelles elles ont été collectées, en cas de retrait du consentement, en cas de traitement illicite, en cas d'absence de motif de traitement légitime prévalant et au cas où les informations ont été collectées par des sociétés d'informations/services en ligne durant l'enfance) .

8. Mettre en place des mesures permettant de garantir les autres droits de la personne concernée, tel que le **droit de limiter le traitement par le DPD** (en cas d'objection au traitement, de doute concernant son exactitude, en cas de traitement illicite et si la personne concernée refuse que les données soient effacées) ; le **droit à la portabilité des données** (en cas de traitement automatique autorisé par le consentement d'une personne ou l'exécution d'un contrat, une personne a le droit de recevoir ses données de la part du DPD sous un format structuré, ordinaire et lisible sur un appareil et a le droit de les transmettre à un autre DPD sans opposition du premier) ; et le **droit d'objection** au traitement des données à tout moment.

9. En pratique, **les systèmes électroniques et moyens manuels recommandés pour garantir la protection des données** sont les suivants :
a) Entreposer les dossiers papier dans un lieu fermé durant la nuit
b) Conserver les documents à l'abri du regard des visiteurs
c) Conserver les ordinateurs dans un lieu fermé
d) Garantir que tous les ordinateurs et équipements TIC soient protégés par mot de passe
e) Procéder régulièrement à la mise à jour des logiciels et antivirus afin d'éviter toute perte de données
f) Crypter les documents contenant des catégories de données spéciales, comme les informations concernant l'appartenance syndicale
g) Eviter l'utilisation régulière de disques flash pour l'enseignement ou le stockage de documents

10. Lors de l'**envoi d'e-mails** (ex. à plusieurs destinataires en les identifiant en tant que membres ou non membres), il est recommandé d'utiliser le champ CCI (copie carbone invisible) pour dresser la liste de leurs adresses et se l'envoyer à soi-même. Ainsi, votre propre adresse e-mail est la seule adresse visible.

11. **Enseigner la protection des données et la confidentialité des informations personnelles dans les écoles** est également devenu important au cours de ces dernières années[2]. Afin de permettre aux enseignant(e)s d'enseigner efficacement la notion de protection des données à caractère personnel à leurs élèves, de les sensibiliser et d'améliorer leurs compétences dans ce domaine, il est indispensable de prévoir des ressources pédagogiques appropriées. **Les autorités de protection des données (APD)**

[2] Dr Gloria González Fuster et Dr Dariusz Kloza (éd.) "The European Handbook for Teaching Privacy and Data Protection at Schools", 2016, Vrije Universiteit Brussel. Law Science Technology & Society (LSTS) EAP.

nationales devraient préparer du matériel pédagogique en consultation avec les syndicats de l'enseignement, en prenant en compte les différentes stratégies des écoles et les besoins de formation des enseignant(e)s.