RÉSOLUTION SUR LES PLATES-FORMES D'APPRENTISSAGE EN LIGNE

40ème Conférence internationale des commissaires à la protection des données et de la vie privée
23 octobre 2018, Bruxelles

CO-AUTEURS :

- Bureau du commissaire à l'information et à la protection de la vie privée de l'Alberta, Canada
- Bureau du commissaire à l'information et à la protection de la vie privée de l'Ontario, Canada
- Commissariat à la protection de la vie privée du Canada
- Office de protection des données à caractère personnel, République tchèque
- Commission nationale de l'Informatique et des Libertés, France

CO-SPONSORS :

- Thüringer Landesbeauftragte für den Datenschutz, Thuringe, Allemagne
- Privacy Commissioner for Personal Data, Hong Kong
- Garante per la protezione dei dati personali, Italie
- Data Protection Registrar, Jersey
- National Privacy Commissioner, Philippines
- Office de protection des données à caractère personnel, Pologne
- Agencia española de protección de datos, Espagne

Le marché mondial des plates-formes d'apprentissage en ligne s'est fortement développé. Il vise à aider les autorités éducatives à proposer de meilleurs services éducatifs et à améliorer les résultats scolaires des enfants et des jeunes. Un nombre croissant d'autorités éducatives utilise actuellement ces plates-formes pour fournir des services éducatifs en classe, et pour avoir une meilleure compréhension des besoins d'apprentissage des élèves.

Certaines de ces plates-formes permettent une analyse des données d'apprentissage (« Learning analytics ») qui peut contribuer fortement aux pratiques d'apprentissage innovantes et efficaces. Dans le meilleur des cas, elles peuvent renforcer et compléter les interactions entre les élèves, les parents et les enseignants au sein de la communauté éducative, tout en aidant les élèves à développer pleinement leurs capacités individuelles. Les plates-formes d'apprentissage en ligne sont néanmoins susceptibles de comporter des risques pour la protection de la vie privée, du fait, notamment, de la collecte, de l'utilisation, de la réutilisation, de la divulgation et du stockage des données des personnes concernées.

Or, les données à caractère personnel des enfants et des jeunes méritent une protection spécifique et ne doivent être traitées que sur un fondement légal suffisant. Les enfants et les jeunes ont droit à la protection de leur vie privée, et doivent pouvoir exercer leurs droits avec le soutien de leurs parents ou tuteurs. Les parents doivent être mis en capacité d'aider leurs enfants à exercer leurs droits, et de participer activement à cet exercice.

Les classes sont devenues des environnements de plus en plus connectés, ce qui peut engendrer des risques pour la protection de la vie privée des enfants. En particulier, ces classes connectées soulèvent des questions en matière de transparence, dans la mesure où les droits relatifs à la protection des données et de la vie privée risquent d'être mis à mal par des pratiques de traitement des données disproportionnées de la part des plates-formes d'apprentissage en ligne, des prises de décision automatiques opaques et par une utilisation abusive de l'analyse de l'apprentissage. En ce qui concerne les enfants et les jeunes, ces pratiques peuvent avoir des

conséquences considérables à long terme au niveau social, économique et professionnel, et ne pas tenir compte de l'évolution de leurs capacités.

Au vu de ce qui précède, et conformément à l'objectif visé d'adopter des résolutions sur des sujets d'intérêt ou de préoccupation communs, la 40ème Conférence internationale des commissaires à la protection des données et de la vie privée (ICDPPC) appelle toutes les parties concernées dans le champ de l'apprentissage en ligne, et en particulier

- les fournisseurs et concepteurs de plates-formes d'apprentissage en ligne, y compris les prestataires dont les services collectent des données sur les élèves ; et
- les autorités éducatives, y compris les ministères de l'éducation, les conseils scolaires, les cadres et personnels éducatifs et les enseignants,

à respecter pleinement les droits des élèves, parents et enseignants («les personnes ») à la protection de leurs données à caractère personnel et à garantir que les données collectées soient uniquement utilisées à des fins éducatives conformément à la législation sur la protection des données.

Les parties sont invitées à prendre les mesures et à suivre les recommandations émises ci-dessous, à chaque stade du développement, de la mise en œuvre et de l'utilisation des plates-formes d'apprentissage en ligne.

1) Il est demandé aux autorités éducatives de :

a) **S'assurer en leur sein qu'elles ont l'autorité et l'expertise nécessaires pour décider de recourir aux services de ces plateformes d'apprentissage.** Les rôles, responsabilités et pouvoirs décisionnels doivent être clairement définis en interne entre les enseignants, les cadres et personnels éducatifs et toute autre autorité éducatives concernée, afin de déterminer qui est responsable et qui détient l'autorité légale lors de la négociation et de la passation de contrats avec des fournisseurs de plates-formes d'apprentissage en ligne. Ces autorités dûment mandatées doivent être en mesure de bien appréhender la

législation relative à la protection des données pour garantir sa prise en compte dans les conditions et dispositions des contrats et des accords conclus avec des tiers.

b) **Établir des politiques et procédures permettant d'évaluer, de valider et d'accompagner l'utilisation des plates-formes d'apprentissage en ligne, et, dans la mesure du possible si cela exigé, réaliser des études d'impact sur la protection des données et de la vie privée.** Ces politiques doivent favoriser le contrôle de chacun sur ses données, préciser les rôles et responsabilités des divers acteurs impliqués, atténuer les risques et promouvoir la responsabilisation de chacun.

c) **Former les enseignants et leur apporter un soutien continu.** Les enseignants doivent recevoir des informations pertinentes, adéquates et à jour concernant la protection des données et les droits des personnes, pour pouvoir utiliser de façon efficace les plates-formes d'apprentissage en ligne. En ayant accès à des ressources, des formations et des ateliers, les enseignants peuvent ainsi bénéficier au maximum des avantages de ces plates-formes, et proposer aux élèves et parents des conseils et une assistance adaptés pour bien les utiliser.

d) **Travailler avec d'autres autorités éducatives et, en coopération avec les autorités nationales de protection des données, convenir de normes communes pour l'utilisation des plates-formes d'apprentissage en ligne.** Cette approche collaborative pour arriver à des pratiques communément admises permet d'accroitre les effets de leviers, l'échange de connaissances, l'élaboration de bonnes pratiques et d'optimiser des ressources, afin d'éviter tout manquement en matière de sécurité et de protection des données lors de la prestation de services de plates-formes d'apprentissage en ligne.

e) Si cela est exigé ou nécessaire, **demander aux personnes leur consentement valide, éclairé et valable.** La base légale du traitement des données des élèves par une plate-forme d'apprentissage en ligne utilisée par un établissement scolaire doit être déterminée par la loi ou par des règles établies par les autorités compétentes, le cas échéant. En l'absence d'une telle base légale, le consentement des parents, le consentement des élèves ou éventuellement des deux, doit être obtenu. La validité de ce

consentement suppose qu'en cas de refus de l'élève, celui-ci ne soit pas désavantagé par rapport aux élèves qui ont donné leur consentement. Le refus ou le retrait du consentement de tout ou partie du traitement des données, devrait, si possible, pouvoir intervenir à tout moment.

f) **Si la législation nationale le permet, définir une politique permettant aux personnes d'accéder à la plate-forme d'apprentissage en ligne depuis leurs appareils électroniques personnels.** Cette politique doit préciser pour quels usages spécifiques la plate-forme peut alors être utilisée ainsi que les conséquences du recours à un équipement personnel, en particulier lors de l'installation de logiciels ou d'applications mobiles.

2) ***Il est demandé aux autorités éducatives, aux fournisseurs et concepteurs de plates-formes d'apprentissage en ligne, conjointement ou indépendamment selon la législation nationale applicable en matière de protection des données, de :***

a) **S'assurer que les plates-formes d'apprentissage en ligne protègent correctement les données à caractère personnel des utilisateurs et satisfont aux normes de protection des données pertinentes.** Quelle que soit la manière dont l'utilisation des plates-formes d'apprentissage en ligne est régie, les dispositions doivent toujours être conformes aux lois et exigences applicables en matière de protection des données.

b) **S'assurer que les finalités pour lesquelles les données à caractère personnel sont collectées, traitées et utilisées, sont légitimes, adaptées au contexte et autorisées par la loi.** Les collectes des données d'élèves doivent toutes être limitées aux données nécessaires à des finalités éducatives. Par défaut, les données ne doivent pas être utilisées à d'autres fins, et en particulier à des fins commerciales ou de marketing. En outre, les données des élèves ne doivent jamais être réutilisées pour d'autres finalités non éducatives, sans le consentement exprès donné librement, s'il existe une législation autorisant cette réutilisation dans ces conditions. Tout traitement ultérieur doit être effectué si possible avec des données désidentifiées, y compris à des fins statistiques et de recherche.

c) **Limiter le volume de données personnelles à traiter.** La collecte, l'utilisation, la conservation et la communication des données, en particulier des données d'élèves, doivent toujours être limitées à ce qui est strictement nécessaire pour répondre aux finalités autorisées. Réduire le risque soulevé par une collecte excessive de données d'élèves doit être un principe fondamental guidant les pratiques de traitement des données des plates-formes d'apprentissage en ligne.

d) **Avant de collecter des données à caractère personnel, informer les personnes des données qui vont être traitées par la plate-forme d'apprentissage en ligne, et des motifs de ce traitement.** Cette information doit être faite en temps utile et de manière claire, concise et adaptée à l'âge des personnes. Des supports visuels graphiques, audio, vidéos ou autres media peuvent être utilisés en plus d'informations textuelles. Il doit être possible d'obtenir facilement une information plus détaillée. L'information doit permettre aux personnes de prendre des décisions éclairées. Par ailleurs, elle doit expliquer les utilisations et communications à des tiers, préciser les risques de préjudice découlant du traitement des données, résumer les protections et garanties mises en place, et mentionner les droits existants et des options ouverts aux personnes.

e) **Dans la mesure du possible, permettre aux personnes d'utiliser la plate-forme d'apprentissage en ligne avec des données désidentifiées.** Afin d'éviter la collecte excessive de données, les personnes doivent pouvoir utiliser les plates-formes d'apprentissage en ligne de manière anonyme ou avec des pseudonymes non identifiants.

f) **Dans la mesure du possible, éviter d'utiliser les données à caractère personnel proprement dites, et en particulier les données relatives aux comportements d'apprentissage, à des fins de prédiction, de profilage ou de prise de décision automatisée.** L'utilisation des données des élèves pour les évaluer de façon subjective ou porter sur eux des appréciations hypothétiques les concernant, peut nuire au développement de leurs capacités. Lorsque les données sont utilisées à des fins d'analyse statistique et de profilage, pour réaliser de telles évaluations, pour prédire un comportement ou dans le cadre d'un processus de prise de décision, les élèves et parents

doivent en être clairement informés. On doit également leur proposer des voies de recours leur permettant de contester, le cas échéant, ces évaluations.

g) **Intégrer et utiliser des outils permettant aux personnes de gérer leurs données à caractère personnel, et d'exercer de façon effective leurs droits, en particulier leur droit d'accès, de rectification, d'effacement ou, le cas échéant, à la portabilité des données.** Ces droits doivent également s'appliquer aux métadonnées, inférence, évaluations et profils, qu'ils concernent des élèves, des parents ou des enseignants.

h) **Définir des durées de conservation pour les différentes catégories de données à caractère personnel, et les respecter.** Les données et métadonnées ne doivent être conservées qu'autant que cela est nécessaire pour satisfaire aux finalités de collecte et d'utilisation prévue. En particulier, les traces d'interactions entre les élèves, parents et enseignants doivent être régulièrement supprimées. À l'expiration de la durée de conservation, un mode de suppression ou de destruction adapté doit être mis en œuvre afin de garantir l'effacement des données en toute sécurité.

3) ***Il est demandé aux fournisseurs et concepteurs de plates-formes d'apprentissage en ligne de :***

a) **Être transparents quant à leurs pratiques de traitement des données vis-à-vis des autorités éducatives et des personnes utilisant les plates-formes d'apprentissage en ligne.** Ces personnes doivent disposer d'un point de contact unique susceptible de répondre aux questions concernant la protection des données de chaque plate-forme d'apprentissage en ligne. Elles doivent avoir le droit de demander toute explication nécessaire à l'entreprise sur ses pratiques en matière de gestion des données et de porter plainte auprès d'une autorité de protection des données si elles ne sont pas satisfaites des explications de l'entreprise ou si elles estiment que les données ont été utilisées à mauvais escient.

b) **Limiter les finalités de collecte de données aux finalités appropriées au contexte éducatif, et préciser, dans les conditions générales de services ou autres contrats juridiques, en quelles circonstances les données à caractère personnel sont susceptibles d'être communiquées.** Les données des élèves ne doivent jamais être utilisées pour d'autres finalités ou réutilisées à des fins non éducatives sans le consentement exprès s'il existe une législation autorisant cette réutilisation.

c) **Être clairs, spécifiques et cohérents dans les conditions générales de services proposées.** Les entreprises doivent éviter d'utiliser des termes comme « finalités éducatives » qui sont trop générales et ne permettent pas aux personnes de comprendre précisément comment leurs données personnelles sont utilisées.

d) **Adopter des technologies renforçant la protection de la vie privée et intégrer les principes de protection des données dès la conception et par défaut.** Les pratiques et technologies permettant de réduire au minimum ou d'éviter la collecte et l'utilisation des données à caractère personnel doivent toujours être préférées, et leur efficacité doit être régulièrement vérifiée et améliorée.

e) **S'assurer que les données à caractère personnel sont conservées dans le respect de la législation nationale sur la protection des données.** Des mesures administratives, physiques et techniques doivent être mises en place pour assurer le traitement licite des données à caractère personnel conformément aux exigences requises, et éviter tout risque lié à un défaut de sécurité.

4) Enfin, il est demandé aux membres de l'ICDPPC de :

a) informer les personnes concernées et les sensibiliser sur les risques en matière de protection des données et sur les responsabilités associées à l'utilisation de plates-formes d'apprentissage en ligne ;

b) utiliser la présente Résolution pour élaborer des lignes directrices aidant les autorités éducatives, les fournisseurs et concepteurs de plates-formes d'apprentissage en ligne à satisfaire à leurs obligations en termes de protection des données et de la vie privée ;

c) promouvoir la présente Résolution et ses recommandations auprès des parties prenantes et décideurs politiques dans leurs juridictions et leurs réseaux ;

d) se concerter avec les organisations internationales et groupes pertinents de la société civile pour promouvoir et donner suite à la présente Résolution ; et

e) coopérer les uns avec les autres, ainsi qu'avec le Groupe de travail international sur l'éducation au numérique, pour partager des ressources, des connaissances et des bonnes pratiques.

La présente Annexe se compose de DEUX PARTIES :

Partie A. Notes complémentaires et explicatives ; et

Partie B. Suggestions visant à aider les membres à mettre en œuvre la présente Résolution

Partie A. Notes complémentaires et explicatives

La Résolution sur les plates-formes d'apprentissage en ligne (la Résolution) s'appuie sur des travaux précédents de groupes de travail de l'ICDPPC, en particulier sur le Working Paper on E-Learning Platforms[1] du Groupe de travail international sur la protection des données dans les télécommunications ; le Rapport sur le ratissage de 2017 du GPEN concernant les services éducatifs en ligne[2] du Global Privacy Enforcement Network ; et le Rapport sur les résultats d'une enquête sur les plates-formes d'apprentissage[3] du Groupe de travail international sur l'éducation au numérique. Ces trois documents démontrent le besoin d'une résolution sur les plates-formes d'apprentissage en ligne.

La Résolution traite de considérations importantes en matière de protection de la vie privée et de sécurité en relation avec les logiciels informatiques, applications mobiles et outils Web spécifiquement fournis aux établissements scolaires, auxquels les élèves, parents et enseignants accèdent via Internet et qu'ils utilisent dans le cadre d'une activité d'enseignement.

Les recommandations sont principalement destinées aux autorités éducatives en tant que responsables du traitement. Ces autorités peuvent élaborer et faire respecter des contrats et des bonnes pratiques permettant aux fournisseurs et concepteurs de plates-formes d'apprentissage

1 « Groupe de Berlin », https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/working-paper/2017/2017-IWGDPT_Working_Paper_E-Learning_Platforms-en.pdf

2 « Rapport sur le ratissage de 2017 du GPEN », https://www.ipc.on.ca/wp-content/uploads/2017/10/gpen-sweep-rpt-fr.pdf.

3 « Rapport du Groupe de travail international sur l'éducation au numérique sur l'enquête », https://icdppc.org/wp-content/uploads/2017/12/DEWG-Rapport-des-canadiens-en-Fran%C3%A7ais_eplateformes_Sept-2017.pdf

en ligne de garantir une utilisation conforme aux législations de protection des données et aux droits relatifs à la protection de la vie privée des personnes concernées. Un certain nombre de recommandations sont également destinées aux fournisseurs et concepteurs de plates-formes d'apprentissage en ligne en tant que sous-traitants, car ils sont en mesure de développer des services respectueux de la protection des données et de la vie privée.

Définitions

Aux fins de la présente Résolution, on entend par :

Plates-formes d'apprentissage en ligne, les outils et supports technologiques en ligne aidant à diffuser les connaissances, à les développer et à favoriser l'interaction entre les enseignants, les élèves et les établissements scolaires. Les plates-formes d'apprentissage en ligne font appel à des dispositifs divers (comme des ordinateurs, des tablettes et des téléphones mobiles), à des traitements de données et à des types d'usages (en classe, en ligne) et à différents acteurs (élèves, enseignants, établissements scolaires, fournisseurs de plates-formes ou d'applications).

Ce terme exclut les tâches de pure gestion scolaire, sans lien avec des apprentissages, et exécutées via des applications administratives mises en œuvre par des autorités éducatives, comme l'affectation et la répartition des enseignants, ou encore la gestion administrative des élèves.

Données à caractère personnel, les données à caractère personnel des élèves, parents et enseignants. Elles comprennent des informations permettant de les identifier, comme leur nom, un numéro d'identification, des données géographiques, biographiques ou médicales, des coordonnées, des modèles de comportements, des dossiers disciplinaires, des besoins éducatifs spécifiques et d'autres informations. Elles font également référence à des identifiants en ligne, ou à un ou plusieurs facteurs spécifiques à l'identité physique, physiologique, génétique, mentale, économique, culturelle ou sociale d'une personne.

Autorités éducatives, les entités établissant les programmes scolaires et définissant les règles ou les cadres de l'enseignement. Les autorités éducatives incluent les ministères de l'éducation, leurs représentants locaux, les conseils scolaires, les établissements scolaires, les cadres et personnels éducatifs et les enseignants.

Analyse de l'apprentissage, la mesure, la collecte, l'analyse et la production de données concernant les élèves et leurs pratiques d'apprentissage, afin de mieux comprendre et d'optimiser cet apprentissage et l'environnement dans lequel il se fait. L'analyse de l'apprentissage inclut les pratiques d'« apprentissage adaptatif », c'est-à-dire d'utilisation de données à caractère personnel pour proposer un apprentissage et une assistance personnalisés.

Recommandations

Les précisions suivantes ont pour objectif d'approfondir les recommandations de la Résolution en donnant davantage d'éléments de contexte, d'explications et des exemples :

1) Il est demandé aux autorités éducatives de :

a) S'assurer qu'elles ont l'autorité et l'expertise nécessaires pour décider de recourir aux services de ces plateformes d'apprentissage.

- Ne pas définir l'autorité responsable et le niveau de responsabilité fait courir des risques inutiles en matière de protection des données, et pourrait conduire à des violations de la vie privée et de sécurité, à des enquêtes et des sanctions. Des autorités éducatives peuvent ne pas être habilitées à collecter, utiliser ou communiquer certains types de données à caractère personnel, ou à autoriser des plates-formes d'apprentissage en ligne à effectuer certaines opérations de traitement de données. Le personnel éducatif peut, pour sa part, ne pas être habilité à contractualiser avec des tiers au nom de son établissement scolaire et de ses élèves.

- Les autorités éducatives doivent :
  - prendre des mesures pour que l'utilisation des plates-formes d'apprentissage en ligne soit conforme aux lois et aux politiques internes en matière de protection des données ;
  - s'assurer que les responsabilités pour décider de recourir à des plates-formes d'apprentissage en ligne sont clairement définies ou déléguées ;
  - définir les limites éventuelles de leur habilitation à utiliser une plate-forme d'apprentissage en ligne ;
  - s'assurer que l'accord conclu avec le fournisseur de plate-forme d'apprentissage en ligne stipule que celui-ci peut uniquement traiter les données des élèves conformément aux instructions de l'établissement scolaire[4] ;
  - dans la mesure du possible, utiliser un contrat écrit ou un accord juridique et prendre des dispositions supplémentaires lors de la cession de licence d'achat « conclue au clic » (« click-wrap licences »)[5], notamment en :
    - s'assurant que l'offre est conforme aux lois et exigences nationales en matière de protection des données ;
    - procédant à une analyse des conditions générales d'utilisation afin de déterminer si le fournisseur a conservé le droit de les modifier sans préavis ; et
    - limitant les personnes habilitées à accepter les conditions générales d'utilisation en matière de protection des données ou à les modifier.[6]
- Lorsque les contrats « conclus au clic » (« click-wrap licences ») ne sont pas conformes aux lois nationales en matière de protection des données et aux exigences de politiques internes, les autorités éducatives ne doivent pas recourir à ces services.

---

4 Document de travail du groupe de Berlin, p. 6.

5 La concession de licence par clic ou la conclusion de contrat au clic nécessite qu'un utilisateur accepte les conditions générales avant d'utiliser le produit ou le service.

6 Pour de plus amples informations à ce sujet, voir Privacy Technical Assistance Center, *Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices*, (« EdTech Paper ») p. 8-10 : https://tech.ed.gov/wp-content/uploads/2014/09/Student-Privacy-and-Online-Educational-Services-February-2014.pdf

b) Établir des politiques et procédures permettant d'évaluer, de valider et d'accompagner l'utilisation des plates-formes d'apprentissage en ligne, et, dans la mesure du possible si c'est exigé, réaliser des études d'impact sur la protection des données et de la vie privée.

- Afin de garantir le respect des lois en matière de protection des données et des exigences de politiques internes applicables, les autorités éducatives doivent prendre des dispositions pour comprendre de quelle façon la plate-forme d'apprentissage en ligne traite les données à caractère personnel et identifier les risques qui peuvent en découler au regard de la protection des données , ainsi que les stratégies permettant de les atténuer. Le manque d'objectifs organisationnels préalables ou de compréhension en matière de traitements de données à caractère personnel par les plates-formes d'apprentissage en ligne peut faire courir des risques non prévus ou non intentionnels en matière de sécurité et de vie privée, comme des violations ou des traitements inappropriés.
- Les autorités éducatives doivent :
  - recourir à des méthodes d'évaluation, d'atténuation des risques et de mise en conformité avec les règles de protection des données avant de recourir à des services de plates-formes d'apprentissage en ligne ;
  - définir des politiques, procédures et normes opérationnelles pour permettre l'utilisation des plates-formes d'apprentissage en ligne ;
  - faire savoir et imposer aux élèves, parents, enseignants et fournisseurs de plates-formes d'apprentissage en ligne l'application des règlements [intérieurs] scolaires ;
  - renforcer le contrôle de chacun sur ses données à caractère personnel, en adoptant des mesures techniques et organisationnelles qui permettent d'exercer les droits d'accès, de rectification et autres droits relatifs à la protection de la vie privée, conformément à la législation et la politique de protection des données applicables ;

- assurer de façon continue un suivi et une mise à jour des mesures techniques et organisationnelles relatives à la sécurité des données ;
- procéder à un inventaire des services éducatifs en ligne actuellement utilisés dans l'établissement ou l'académie, pour permettre de recenser et d'évaluer l'ensemble des données des élèves, parents et enseignants partagées avec des fournisseurs[7].

EXEMPLES de questions pertinentes à se poser lors de l'analyse des plates-formes d'apprentissage en ligne : [8]

- Des informations concernant des élèves, parents ou enseignants seront-elles partagées avec des acteurs autres que l'autorité éducative ?
- Allez-vous partager ces informations avec des sociétés ou des personnes qui ne sont pas des personnels de l'établissement scolaire ? Si c'est le cas, qui aura accès à ces données ?
- Quels types d'informations sont partagés ?
- Les données sont-elles collectées pour des finalités ultérieures?
- Allez-vous demander le consentement des élèves ou des parents pour partager ces informations ?
- Quels sont, selon vous, les risques pour les élèves en cas de partage de ces informations? Pour vous, en tant qu'enseignant? Pour l'établissement scolaire ?

c) Former les enseignants et leur apporter un soutien continu.

[7] EdTech Paper, p. 8. Voir aussi *The Common Sense Privacy Evaluation Initiative* pour des suggestions et exemples relatifs à la réalisation d'évaluations des plates-formes d'apprentissage en ligne : https://www.commonsense.org/education/privacy.

[8] Berkman Klein Center for Internet & Society at Harvard University, *Educational Technology and Student Privacy Checklist* : https:/dlrp.berkman.harvard.edu/node/59.

- Si les enseignants ne sont pas formés aux enjeux en termes de protection des données que soulève l'utilisation des plates-formes d'apprentissage en ligne sur la protection de la vie privée, ils risquent de ne pas avoir les compétences pour sélectionner, déployer, configurer et utiliser les plates-formes. Ainsi, les enseignants peuvent ne pas être en mesure de guider les élèves et parents pour utiliser correctement ces services.
- Les autorités éducatives doivent :
  - fournir aux enseignants une liste de plates-formes d'apprentissage en ligne évaluées et approuvées ;
  - organiser, pour les enseignants, des sessions d'information pour expliquer comment les plate-formes d'apprentissage en ligne traitent les données à caractère personnel, et comment bien les utiliser. Ces informations sont destinées à être utilisées par les parents et les élèves ;
  - assurer un égal accès à des équipements et des ressources à jour, et proposer une formation professionnelle continue adaptée afin de permettre aux enseignants d'apprendre à maîtriser les nouvelles technologies[9] ;
  - sensibiliser les élèves à la protection des données en invitant les enseignants à intégrer le Référentiel de formation des élèves à la protection des données personnelles[10] dans leurs pratiques d'enseignement adaptées par groupes d'âge , notamment en leur donnant des conseils sur les bonnes pratiques, à suivre pour :
    - créer un compte en ligne, un profil utilisateur et poster des contenus en ligne ;
    - régler les paramètres de son compte et ses favoris;
    - gérer les cookies, et particulièrement les cookies et autres traceurs tiers;
    - télécharger et installer des logiciels, particulièrement sur les équipements informatiques personnels ; et
    - supprimer un compte et/ou des contenus en ligne[11]

[9] HabiloMédias, *L'apprentissage connecté : Le personnel enseignant et les technologies en réseau dans la classe*, p. 82 : http://habilomedias.ca/sites/mediasmarts/files/publication-report/full/jcmbiii_apprentissage_connecte.pdf

[10] 38ème ICDPPC, https://icdppc.org/wp-content/uploads/2015/02/FR-6.pdf

[11] Rapport sur le ratissage du GPEN, p. 8 : https://www.ipc.on.ca/wp-content/uploads/2017/10/gpen-sweep-rpt-fr.pdf.

d) Travailler avec d'autres autorités éducatives et, en coopération avec les autorités nationales de protection des données, convenir de normes communes pour l'utilisation des plates-formes d'apprentissage en ligne.

- L’absence de normes élaborées et appliquées de façon commune, peut avoir pour conséquence une application incohérente des droits et obligations individuels en matière de protection des données.
- Les autorités éducatives doivent :
  - faciliter la coopération et le partage des connaissances, des bonnes pratiques et autres ressources, en particulier pour l'utilisation de plates-formes d'apprentissage en ligne pré-évaluées et approuvées ;
  - développer et promouvoir l'utilisation de modèles de clauses contractuelles, de normes d'évaluation, de labels de certification et de codes de conduite.

e) Si cela est exigé ou nécessaire, demander aux personnes leur consentement valide, éclairé et valable.

- Les personnes doivent pouvoir exercer leurs droits à la protection des données, en particulier, en donnant ou refusant leur consentement. Dans le cas d’une utilisation obligatoire de plate-formes d'apprentissage en ligne et si aucune option alternative ou mécanisme de refus n’est proposé, le consentement obtenu ne peut être considéré comme valide, et ne peut servir de base juridique au traitement.
- Dans certains cas, un consentement exprès peut être nécessaire, par exemple lors du traitement de données sensibles, pour des finalités nouvelles ou incompatibles, ou lorsqu'il existe un risque de préjudice important.

- Dans l'environnement éducatif dans lequel les plates-formes d'apprentissage en lignes sont utilisées, il peut exister un déséquilibre de situation entre les élèves et les autorités éducatives. Les utilisateurs d'une plate-forme d'apprentissage en ligne ne se sentent en effet pas toujours libres de ne pas utiliser cette plate-forme, si le choix leur est laissé, car cela peut les désavantager par rapport à leurs pairs. Dans ces cas, le consentement ne peut être considéré comme valide.
- Certaines finalités de traitement peuvent être interdites. Ainsi, certaines collectes, utilisations ou divulgations de données à caractère personnel peuvent avoir des effets discriminatoires ou préjudiciables pour certaines personnes et sont inappropriées.
- Même dans le cas où les autorités éducatives sont habilitées et ont l'autorité nécessaire pour décider de recourir à des services de plates-formes, les personnes concernées doivent avoir le choix de ne pas les utiliser et doivent pouvoir bénéficier de services éducatifs alternatifs.
- Les autorités éducatives doivent :
  - Prendre en compte ces refus ;
  - proposer des méthodes alternatives d'enseignement ne nécessitant pas l'utilisation d'une plate-forme d'apprentissage en ligne.
- Lorsque le consentement des personnes constitue la base légale du traitement des données, les autorités éducatives, les fournisseurs et concepteurs de plates-formes d'apprentissage en ligne doivent :
  - s'assurer qu'un consentement direct, éclairé et spécifique est donné par la personne ;
  - si nécessaire, obtenir le consentement des parents. Lorsque les personnes concernées sont des jeunes en mesure de donner eux-mêmes leur consentement, leur maturité doit être prise en compte, tout comme le contexte ;
  - recueillir le consentement exprès des élèves avant de communiquer des informations personnelles concernant des élèves sur un site public, lorsque cette pratique est autorisée.

Si la législation nationale le permet, définir une politique permettant aux personnes d'accéder à la plate-forme d'apprentissage en ligne depuis leurs appareils électroniques personnels.

- De nombreuses autorités éducatives mettent à la disposition des élèves, parents et enseignants des ordinateurs, tablettes et autres équipements informatiques, ainsi qu'une infrastructure en réseau. Dans certains cas, ceux-ci peuvent utiliser leurs propres appareils personnels pour se connecter à l'infrastructure en réseau de l'établissement scolaire. Cette utilisation d'un équipement personnel n'est pas sans soulever des risques supplémentaires en matière de protection des données et de la vie privée
- Les autorités éducatives doivent limiter ces risques en :
  - s'assurant que leur infrastructure en réseau est régie par des politiques d'utilisation claires et transparentes ;
  - réduisant au minimum et, le cas échéant, en interdisant la collecte des données qui proviennent d'équipements personnels et qui ne concernent pas les activités éducatives.

2) Il est demandé aux autorités éducatives, fournisseurs et concepteurs de plates-formes d'apprentissage en ligne, conjointement ou indépendamment selon la législation nationale applicable en matière de protection des données, de :

a) S'assurer que les plates-formes d'apprentissage en ligne protègent correctement les données à caractère personnel des utilisateurs et satisfont aux normes de protection des données pertinentes.

- Si les données des utilisateurs ne sont pas correctement protégées, cela crée des risques d'atteinte à la confidentialité et à la sécurité, comme par exemple, l'utilisation et la divulgation non-autorisées de données. Par exemple, des données sensibles d'élèves pourraient être révélées en raison de l'utilisation de mécanismes de connexion non sécurisés,

d'une mauvaise configuration de la plate-forme ou d'une erreur humaine ; cela nécessitera alors la mise en place de mesures de sécurité supplémentaires.

- Des accords juridiques peuvent garantir la légalité d'un traitement en prônant un contrôle efficace, la responsabilisation et la conformité. Des dispositions contractuelles doivent renforcer les droits et obligations des personnes en matière de protection des données.
- Les autorités éducatives, les fournisseurs et concepteurs de plates-formes d'apprentissage en ligne doivent :
  - s'assurer que les exigences en matière de protection des données personnelles font partie intégrante de tous les accords juridiques passés avec les plates-formes d'apprentissage en ligne, y compris en ce qui concerne les accords de service négociés et « conclus au clic » (« clip-wrap terms ») ;
  - s'assurer que les accords juridiques décrivent la nature des données à caractère personnel à traiter, les finalités de la collecte, leurs utilisations et les destinataires, le lieu d'hébergement du traitement, les exigences en matière de durée de conservation, ainsi que les droits d'accès et de rectification. Ils doivent également prévoir des garanties administratives, physiques et techniques, ainsi que des exigences en matière de notification de violation de données ;
  - prévoir et exiger l'utilisation d'un mécanisme d'authentification multi-facteurs lors de la connexion à la plate-forme par les administrateurs et les enseignants, afin de prévenir toute utilisation détournée [de données] en cas de vols de mots de passe ;
  - exiger la mise en place et l'application de contrôles d'accès et de politiques de connexion, pour s'assurer que l'accès aux données à caractère personnel est bien géré et contrôlé. L'accès aux données à caractère personnel doit se fonder sur le principe du « besoin d'en connaître » ;

- chiffrer les transmissions de données entre les serveurs et les utilisateurs des plates-formes. A cet effet, il convient d'utiliser la technologie de chiffrement adaptée à la plate-forme concernée[12] ;
- assurer un suivi en continu et une mise à jour des contrôles de sécurité.

- En cas de violation de données, les fournisseurs de plates-formes d'apprentissage en ligne et les autorités éducatives doivent en avertir les établissements scolaires, les élèves ou leurs parents, ainsi que les autorités de protection des données pertinentes, conformément aux exigences nationales en matière de notification de violation de données.

b) S'assurer que les finalités pour lesquelles les données à caractère personnel sont collectées, traitées et utilisées, sont légitimes, adaptées au contexte et autorisées par la loi.

- Limiter l'utilisation des données d'élèves à des fins éducatives, y compris dans le contexte de l'apprentissage des élèves, constitue une mesure de protection des droits des personnes concernées, en particulier des mineurs.

- Ces données ne doivent pas être utilisées pour des finalités commerciales, en particulier la revente de données et la réutilisation pour des finalités de marketing directes ou indirectes.

c) Limiter le volume de données à caractère personnel à traiter.

- Le principe de minimisation des données doit être appliqué en permanence pour limiter le risque de collecte, utilisation et diffusion abusives ou non-autorisées des données à caractère personnel.

[12] Conférence des commissaires allemands à la protection des données, *A Guidebook From the Data Protection Supervisory Authority for Online Learning Platforms in School Classrooms*, p. 22. Traduction en anglais disponible sur : https://www.tlfdi.de/mam/tlfdi/datenschutz/guidebook_from_the_data_protection_supervisory.pdf

- Les autorités éducatives, les fournisseurs et concepteurs de plates-formes d'apprentissage en ligne doivent :
  - évaluer si les données personnelles sont nécessaires et dans quelle mesure elles répondent aux finalités éducatives[13] ;
  - laisser le choix aux élèves et aux parents qui ne souhaitent pas fournir leurs données personnelles sur des plates-formes d'apprentissage en ligne, de refuser cette collecte.

d) Avant de collecter des données à caractère personnel, informer les personnes concernées des données qui vont être traitées par la plate-forme d'apprentissage en ligne, et les motifs de ce traitement.

- Une information insuffisante ou un manque de transparence peut porter atteinte aux principes de licéité et loyauté et empêcher les personnes de prendre des décisions éclairées et donner un consentement valable.
- Les autorités éducatives, les fournisseurs et concepteurs de plates-formes d'apprentissage en ligne doivent :
  - utiliser des notices spécifiques pour communiquer, informer de manière proactive et permettre aux personnes concernées de comprendre comment leurs données personnelles seront traitées ;
  - rédiger ces notices d'information de la manière la plus efficace et la plus adaptée au contexte ;
  - dans la mesure du possible, prévoir une information lors de l'inscription, en engageant un dialogue direct avec les parents et les élèves, en les informant de leurs droits et de la manière dont ils peuvent les exercer ;

[13] Voir les recommandations des sections 3(b) et 3(c) du présent document qui définissent les exigences veillant à ce que les objectifs déclarés soient clairs et adaptés au contexte éducatif.

- lorsque l'information s'adresse aux élèves, leur fournir un accompagnement adapté à leur âge pour leur permettre de bien la comprendre ;
- fournir des informations relatives aux types de données collectées, à leurs finalités d'utilisation et à leurs destinataires potentiels ;
- prévoir une information sur la façon dont les données agrégées et désidentifiées seront utilisées et communiquées ;
- avertir les personnes concernées en cas de modification des pratiques de traitement des données par l'autorité éducative ou la plate-forme d'apprentissage en ligne ;
- fournir les coordonnées de l'autorité nationale de protection des données.

> **Exemple :** La plupart des politiques de confidentialité des sites informent de la présence et de l'utilisation de cookies tiers, sans fournir d'instructions précises ou d'options concrètes pour prévenir leur utilisation ou savoir les gérer. Les cookies tiers peuvent généralement être bloqués sans perte apparente de fonctionnalité. De nombreux enseignants et élèves ne savent peut-être pas comment les bloquer ou les gérer. Les fournisseurs de plates-formes d'apprentissage en ligne doivent fournir des options concrètes pour bloquer ou gérer les cookies, afin que les utilisateurs puissent les utiliser sans être tracés[14].

e) Dans la mesure du possible, permettre aux personnes d'utiliser la plate-forme d'apprentissage en ligne avec des données désidentifiées.

- Une collecte excessive de données à caractère personnel expose à un risque d'utilisation abusive et de violation.

[14] Rapport sur le ratissage du GPEN, p. 5.

- Conformément au principe de minimisation de données, l'identité des personnes tout comme la possibilité de les identifier doivent être réduites au maximum en recourant à une méthode de pseudonymisation.
- Les autorités éducatives, les fournisseurs et concepteurs de plates-formes d'apprentissage en ligne doivent :
  - permettre aux personnes d'utiliser la plate-forme d'apprentissage en ligne sans avoir à créer un compte personnel. Si un identifiant ou compte d'élève est nécessaire, il doit être possible de créer des pseudonymes qui ne révèlent pas les noms ou d'autres données identifiables ;
  - lorsque des données à caractère personnel doivent être collectées par la plate-forme d'apprentissage en ligne, désidentifier ou agréger les données dès que possible ;
  - éviter d'utiliser les identifiants de connexion aux réseaux sociaux, car cela peut entraîner la collecte et la divulgation excessives de profils détaillés et d'autres informations identifiables entre le site de réseau social et la plate-forme d'apprentissage en ligne, et peut limiter la capacité des élèves à empêcher le traçage de leurs activités sur l'ensemble du Web.

Exemple : Les fournisseurs de plates-formes d'apprentissage en ligne doivent conseiller aux enseignants d'utiliser le moins possible de données personnelles lors de la création de profils en attribuant un pseudonyme aux élèves. Ceux-ci peuvent ensuite accéder à leur profil en entrant un code d'accès unique qui leur a été fourni. Ainsi, les élèves n'ont pas à fournir de données personnelles, et peuvent utiliser le service en recourant à un pseudonyme[15].

[15] Rapport sur le ratissage du GPEN, p. 5.

f) Dans la mesure du possible, éviter d'utiliser les données à caractère personnel proprement dites, en particulier les données relatives aux comportements d'apprentissage, à des fins prédictives, de profilage ou de prise de décision automatisée.

- Si les données personnelles peuvent constituer des informations utiles pour orienter positivement une décision en matière d'éducation, le recours à des données personnelles aux seules fins d'analyse prédictive soulève des enjeux importants tant en termes de protection des données qu'en matière éthique.
- Les plates-formes d'apprentissage en ligne adaptent la présentation de leurs ressources pédagogiques en fonction de chaque apprenant, collectent des données sur les capacités et comportements d'apprentissage des élèves, et les évaluent pour améliorer l'efficacité du processus d'apprentissage. L'accumulation de données des élèves à de telles fins n'est pas sans soulever certains risques, même si cela peut paraitre justifié au vu des bénéfices obtenus.
- Les évaluations automatiques, ainsi que la création de profils d'élèves pour un usage autre que l'activité pédagogique concernée, peuvent nuire aux capacités d'évolution des enfants et des jeunes[16]. Les algorithmes utilisés pour les évaluations automatisées peuvent reposer sur des hypothèses erronées qui ne peuvent pas être vérifiées. Par nécessité, ils n'utilisent qu'un nombre limité de données, et ne prennent pas en compte les circonstances et difficultés rencontrées par les élèves. Les profils basés sur des comportements d'apprentissage observés portent atteinte aux droits fondamentaux à la protection des données et à la liberté d'expression.
- Lorsque les données sont utilisées dans le cadre d'évaluations ou de décisions automatisées par la plate-forme qui dépassent les limites de l'exercice pédagogique avec les élèves, ce processus doit être transparent pour les enseignants, les élèves et les parents. Ces derniers

[16] UNICEF, *Children's Online Privacy and Freedom of Expression* : https://www.unicef.org/csr/files/UNICEF_Childrens_Online_Privacy_and_Freedom_of_Expression(1).pdf

doivent toujours avoir le droit de contester cette utilisation, et de contester les évaluations et décisions qui en résultent.

- Les autorités éducatives doivent:
  - s'assurer qu'elles gardent un contrôle total sur les conclusions ou les évaluations concernant les élèves, en particulier, en cas de prise de décision automatisée.
- Les autorités éducatives, les fournisseurs et concepteurs de plates-formes d'apprentissage en ligne doivent :
  - garantir une utilisation transparente des algorithmes et profils pouvant influencer la prise de décision. Tout système de prise de décision automatisée ou fondé sur un autre système des prise de décision, ainsi que la justification des conclusions formulées par les systèmes, doivent être expliqués aux élèves et parents ;
  - dans le cas de décisions individuelles automatisées, donner accès à cette décision et à sa justification. Des procédures spécifiques doivent être mises en place pour donner lieu à une évaluation humaine des décisions dans les cas où des objections seraient émises, des contre-arguments présentés ou dans les cas où ces décisions seraient contestées[17] ;
  - faire expertiser en externe et/ou tester les algorithmes, protocoles, concepts et applications. Des audits publics, ou réalisés par des tiers de confiance, peuvent contribuer à offrir l'assurance que la plate-forme d'apprentissage en ligne ne donnera pas de résultats qui ne seraient pas justes ou seraient discriminatoires[18] ;
  - Lorsque les données relatives aux comportements d'apprentissage sont collectées et utilisées à des fins de prédiction et de profilage, prendre en compte les recommandations figurant dans les résolutions connexes de l'ICDPPC, en particulier la Résolution sur le profilage adoptée par la 35ème ICDPPC[19].

[17] Document de travail du groupe de Berlin, para. 37.
[18] Document de travail du groupe de Berlin, para. 33.
[19] https://icdppc.org/wp-content/uploads/2015/02/Profiling-resolution-FR.pdf

g) Intégrer et utiliser des outils permettant aux personnes de gérer leurs données à caractère personnel, et d'exercer de façon effective les droits relatifs à la protection de leur vie privée, y compris leur droit d'accès, de rectification, d'effacement ou, le cas échéant, à la portabilité des données.

- Les entreprises doivent concevoir leurs services et plates-formes d'apprentissage en ligne de manière à permettre aux élèves, parents ou enseignants de demander éventuellement l'accès, la rectification ou l'effacement des données. Le non-respect de cette obligation crée un risque que les personnes ne puissent pas exercer leurs droits à la protection de leurs données.
- Les autorités éducatives doivent :
  - éviter de conclure des accords avec des plates-formes d'apprentissage en ligne, dans lesquels les données des élèves sont soumises à des traitements en « boite noire » offrant peu de transparence et de contrôle ;
  - lorsque les circonstances le permettent, faciliter l'exercice des droits relatifs à la protection de la vie privée en aidant les personnes concernées ou en agissant en leur nom auprès des plates-formes d'apprentissage en ligne, tout en veillant à ce que ses droits soient respectés et protégés;
  - éduquer les élèves et informer les parents des outils permettant d'exercer leurs droits en matière de protection des données.
- Les fournisseurs de plates-formes d'apprentissage en ligne doivent :
  - intégrer des outils permettant l'exercice effectif des droits d'accès, de rectification et d'effacement ;
  - lorsque les lois relatives à la protection des données donnent aux personnes le droit à la portabilité de leurs données, s'assurer que les données sont mises à disposition dans un format structuré, couramment utilisé et lisible par machine (par exemple, pour prendre en compte le changement d'établissement scolaire d'un élève).

h) définir des durées de conservation pour les différentes catégories de données à caractère personnel, et les respecter.

- Des politiques ou des calendriers de conservation définissent les types de documents ou de données, leurs finalités et leur durée de conservation. Ils permettent d'établir et de documenter les périodes de conservation standard pour les différentes catégories de données, et constituent une aide pour établir les politiques et les procédures d'effacement sécurisées.
- La conservation des données pendant une durée excédant celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées, peut exposer ces données à un risque d'utilisation abusive et de violation. Les élèves et les parents ont le droit d'accéder et de rectifier leurs fichiers pédagogiques et autres données à caractère personnel (y compris des données comportementales) stockés, quelle que soit la personne qui les collecte ou les tient à jour.
- La suppression des données une fois qu'elles ne sont plus nécessaires, réduit le risque qu'elles ne soient plus pertinentes ou exactes, ou deviennent excessives ou obsolètes[20].
- Les autorités éducatives, les fournisseurs et concepteurs de plates-formes d'apprentissage en ligne doivent :
  - diffuser une information concernant les catégories de données collectées, les finalités pour lesquelles elles seront utilisées, l'identité des acteurs participant au traitement, la durée de conservation des données, et les pratiques de sécurité mises en place[21] ;
  - sous réserve d'autres obligations légales, veiller à fournir des explications sur les données traitées par la plate-forme d'apprentissage en ligne ;

[20] Pour connaître d'autres raisons d'adopter une politique de conservation, voir l'organisme britannique Information Commissioner's Office, « Storage Limitation »https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/principles/storage-limitation/

[21] Document de travail du groupe de Berlin, para. 30.

- limiter au minimum la conservation des données générées par leur utilisation, comme les logs de connexion, les évaluations et les profils ;
- ne transmettre des données d'une activité pédagogique à une autre que sous le contrôle plein et entier des enseignants, et de manière transparente pour les enfants et leurs parents. Les données qui ne sont pas transmises doivent être supprimées après une période de conservation raisonnable suivant la fin de l'activité ;
- supprimer les comptes individuels et les données personnelles qui leur sont associées après une période d'inactivité de non-utilisation définie, ou sur demande.

3) Il est demandé aux fournisseurs, concepteurs de plates-formes d'apprentissage en ligne de :

a) Être transparents quant à leurs pratiques de traitement des données vis-à-vis des autorités éducatives et des personnes utilisant les plates-formes d'apprentissage en ligne.

- Les élèves, parents et enseignants ont le droit de savoir quelles données personnelles les concernant sont collectées, comment elles seront utilisées et si elles seront communiquées à d'autres personnes. Si les pratiques de traitement des données de la plate-forme d'apprentissage en ligne ne sont pas totalement transparentes, les autorités éducatives et les personnes risquent de ne pas être en mesure de prendre des décisions éclairées concernant leur participation à la plate-forme.
- Pour garantir une prise de décision éclairée, les fournisseurs et concepteurs de plates-formes d'apprentissage en ligne doivent :
  - mettre à disposition, sous une forme compréhensible, des informations concernant la façon dont ils gèrent les données ;
  - indiquer clairement les pratiques de traitement des données aux autorités éducatives avant de conclure des contrats de services ;

- indiquer clairement les pratiques de traitement des données aux élèves et parents lors de leur inscription au service ;
- aviser de toute modification des conditions de collecte, d'utilisation ou de communication des données. L'information doit clairement expliquer les changements proposés ou mis en œuvre ;
- donner aux autorités éducatives, aux parents et aux élèves un point de contact pouvant répondre aux questions concernant les pratiques de traitement des données de la plate-forme ;
- garantir la pérennité de leurs services pour la durée de l'accord conclu avec l'autorité éducative.

b) Limiter les finalités de collecte de données aux finalités appropriées au contexte éducatif, et préciser, dans les conditions générales de services ou autres contrats juridiques, en quelles circonstances les données à caractère personnel sont susceptibles d'être communiquées.

- Les finalités de collecte, d'utilisation et de communication doivent être adaptées au contexte éducatif pour éviter tout risque de traitement de données inapproprié, non autorisé ou illégal.
- Les fournisseurs et concepteurs de plates-formes d'apprentissage en ligne doivent :
  - traiter uniquement les données à caractère personnel conformément au contexte éducatif dans lequel elles sont fournies ;
  - ne jamais réutiliser ou partager des données concernant l'utilisation de la plate-forme d'apprentissage en ligne par les élèves, pour des finalités incompatibles ou ultérieures ;
  - ne jamais utiliser les données issues de l'utilisation de plates-formes d'apprentissage en ligne à des fins commerciales et marketing.

c) Être clairs, spécifiques et cohérents dans les conditions générales de services proposés.

- Si les conditions générales de services ne sont pas mises à disposition de manière claire et cohérente, les autorités éducatives ne seront pas en mesure de prendre des décisions éclairées lorsqu'elles concluent des accords avec des fournisseurs de plates-formes d'apprentissage en ligne.
- Les fournisseurs et concepteurs de plates-formes d'apprentissage en ligne doivent :
  - définir clairement les finalités pour lesquelles ils vont collecter des données à caractère personnel, et éviter des termes vagues comme « des finalités éducatives » ou « la qualité de l'enseignement » et éviter par là même une collecte excessive de données[22] ;
  - appliquer les recommandations figurant dans le présent document afin de rédiger des conditions générales d'utilisation claires et cohérentes, en particulier l'interdiction d'utiliser les données à certaines finalités, les durées de conservation et les garanties appropriées.

> **Exemple :** Indiquer qu'une collecte de données est nécessaire à des « fins éducatives » est trop général. Indiquer que la collecte est nécessaire pour « améliorer les compétences en lecture en CM2 » ou « améliorer les cours de physique au niveau du collège » indique plus clairement les finalités de la collecte de données.

d) Adopter des technologies renforçant la protection de la vie privée et intégrer les principes de protection des données dès la conception et par défaut.

[22] Pour d'autres exemples de conditions générales claires, voir : U.S. Department of Education's Privacy Technical Assistance Centre, *Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices*: https://studentprivacy.ed.gov/sites/default/files/resource_document/file/TOS_Guidance_Jan%202015_0%20%281%29.pdf.

- Les technologies renforçant la protection de la vie privée (« PET's ») permettent de limiter la collecte et l'utilisation de données personnelles, d'améliorer la transparence du traitement de ces données et de faciliter le respect des règles de protection des données. L'utilisation de ces technologies devrait rendre plus difficile la violation de certaines règles de protection des données et / ou aider à les détecter[23].

- Les fournisseurs et concepteurs de plates-formes d'apprentissage en ligne doivent :

  - limiter le volume de la collecte de données personnelles et utiliser des données désidentifiées conformément aux recommandations 2(b) et 2(e), et aux principes de protection des données dès la conception et par défaut[24] ;

  - prendre en compte la protection des données dans des bases d'archives ou bases temporaires;

  - établir des mesures de sécurité pour veiller à ce que la disponibilité, l'intégrité, la confidentialité, la durabilité et la traçabilité des données à caractère personnel respectent voire même dépassent les normes et pratiques en vigueur ;

  - prendre en compte la Resolution on Privacy by Design adoptée par la 32ème ICDPPC.[25]

e) S'assurer que les données à caractère personnel sont conservées dans le respect de la législation nationale sur la protection des données.

[23] Commission européenne, *Technologies renforçant la protection de la vie privée – Le cadre juridique existant*, MEMO/07/159, mai 2007, http://europa.eu/rapid/press-release_MEMO-07-159_fr.pdf ; Commissariat à la protection de la vie privée du Canada, *Technologies d'amélioration de la confidentialité – Un survol des outils et des techniques*, nov. 2017, https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/recherche/consulter-les-travaux-de-recherche-sur-la-protection-de-la-vie-privee/2017/pet_201711/ ; Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information (ENISA), *Privacy-Enhancing Technologies,* https://www.enisa.europa.eu/topics/data-protection/privacy-enhancing-technologies ; ENISA, *Privacy by Design*, https://www.enisa.europa.eu/topics/data-protection/privacy-by-design.

[24] Voir aussi l'article 25 du *règlement général sur la protection des données* de l'Union européenne, « Protection des données dès la conception et protection des données par défaut », http://www.privacy-regulation.eu/en/article-25-data-protection-by-design-and-by-default-GDPR.htm

[25] https://icdppc.org/wp-content/uploads/2015/02/32-Conference-Israel-resolution-on-Privacy-by-Design.pdf

- Dans de nombreux cas, les données personnelles des plates-formes d'apprentissage en ligne ne sont pas stockées ni traitées dans des systèmes de données sous le contrôle des autorités éducatives. Bon nombre d'entre elles ont plutôt recours à des fournisseurs externes pour stocker et traiter les données des élèves. L'utilisation de plates-formes dématérialisées (dans le cloud) peut soulever de nouveaux risques pour la transparence, la sécurité et la responsabilisation du traitement des données[26].
- Les fournisseurs et concepteurs de plates-formes d'apprentissage en ligne doivent :
  - fournir des garanties administratives, physiques et techniques pour garantir que le traitement de toutes les données est conforme aux exigences applicables en matière de localisation des données ;
  - permettre de réaliser régulièrement des audits par les responsables du traitement, des autorités de protection des données ou d'autres organismes de contrôle mandatés, le cas échéant ;
  - en cas d'utilisation de services dématérialisés (basés dans le cloud), veiller à ce que ceux-ci respectent voire même dépassent les normes et pratiques de protection des données en vigueur en matière de sécurité, d'accès et de responsabilisation[27] ;
  - prendre en compte les résolutions adoptées précédemment dans ces domaines, notamment la Resolution of Cloud Computing adoptée par la 34ème conférence d'ICDPPC[28].

[26] Working Paper on Cloud Computing – Privacy and data protection issues – « Sopot Memorandum » – 51e réunion, 23-24 avril 2012, Sopot (Pologne), p. 1-3.

[27] Contrôleur européen de la protection des données, *Guidelines on the use of cloud computing services by the European institutions and bodies* ; ENISA, « Cloud Security » page ; NIST, *Guidelines on Security and Privacy in Public Cloud Computing* ; ISACA, *IT Control Objectives for Cloud Computing: Controls and Assurance in the Cloud*.

[28] https://icdppc.org/wp-content/uploads/2015/02/Resolution-on-Cloud-Computing.pdf

Partie B. Suggestions visant à aider les membres à mettre en œuvre la présente Résolution

La Résolution, et en particulier ses recommandations, donnent aux autorités de protection des données (APD) une base à laquelle se référer lorsqu'elles sont amenées à traiter des questions relatives aux plates-formes d'apprentissage en ligne et à l'utilisation des données personnelles. Lors de la mise en œuvre de la Résolution au niveau national, les APD sont invitées à prendre en compte les mesures suivantes :

a) Informer les personnes et les sensibiliser sur les risques en matière de protection des données et sur les responsabilités associées à l'utilisation de plates-formes d'apprentissage en ligne

- Les APD sont invitées à publier la Résolution sur leurs sites Web et dans d'autres publications, à la partager et à la communiquer sur des canaux de diffusion, comme les médias sociaux, et à la citer dans leurs travaux concernant l'éducation, les enfants et les jeunes.
- Dans ce cadre, il est suggéré aux APD de préparer des ressources éducatives (ou de tirer parti de ressources préparées par d'autres) et, si possible, d'agir en tant que structure-ressource en pouvant apporter des informations et partager les bonnes pratiques. Elles peuvent, par exemple, organiser des sessions de sensibilisation à la protection des données et mieux faire connaître les mesures pour limiter les risques, exposés dans la présente Résolution. Ces ressources éducatives et actions d'information peuvent venir compléter les efforts engagés par les APD afin de permettre aux enfants et aux jeunes de mieux connaître et exercer leurs droits en matière de protection des données.

b) Utiliser la présente Résolution pour élaborer des lignes directrices aidant les autorités éducatives, les fournisseurs et concepteurs de plates-formes d'apprentissage en ligne à satisfaire à leurs obligations en termes de protection des données et de la vie privée

- Les APD sont invitées à utiliser la présente Résolution comme point de départ pour élaborer des lignes directrices concernant les plates-formes d'apprentissage en ligne et leurs pratiques de traitement des données.
- Les lignes directrices peuvent être spécifiquement adaptées aux lois et aux contextes nationaux pour préciser les attentes et obligations qui incombent aux différents acteurs de l'apprentissage en ligne. Elles doivent orienter les prestataires de services éducatifs pour les inciter à offrir des garanties adéquates de haut niveau pour la collecte, le traitement, la conservation et la communication des données des élèves, parents et enseignants.
- Les lignes directrices permettent également aux APD d'approfondir certains sujets, comme, par exemple, l'utilisation de l'analyse de l'apprentissage. L'analyse de l'apprentissage peut nécessiter la création de nouvelles données personnelles sensibles utilisées pour établir des profils individuels à des fins d'analyse et de prédiction, et elle doit donc se conformer à des règles claires. Les lignes directrices doivent définir les principes directeurs et servir de cadre éthique solide, pour encadrer les pratiques d'analyse d'apprentissage et se conformer aux lois applicable en matière de protection des données.
- De même, dans la mesure du possible, les APD doivent travailler avec toutes les parties prenantes pour définir des codes de bonnes pratiques régissant l'utilisation des plates-formes d'apprentissage en ligne. Ces codes peuvent être un bon moyen d'aborder des questions concernant la rédaction de contrats de services par des fournisseurs de plates-formes d'apprentissage en ligne, en définissant des normes minimales sur les informations devant figurer dans ces contrats.

c) Promouvoir la présente Résolution et ses recommandations auprès des parties prenantes et décideurs politiques dans leurs juridictions et leurs réseaux

- Les APD peuvent jouer un rôle fondamental pour identifier, recenser et mettre à disposition des connaissances et ressources complémentaires. De plus, elles sont bien

placées pour s'assurer que les décideurs politiques et tout autre décideur influent soient parfaitement pleinement informés de ces textes et documents de référence avant de prendre des décisions dans ce domaine.

- Les APD sont invitées à diffuser la Résolution auprès des autorités gouvernementales et éducatives et des décideurs politiques, ainsi qu'auprès du secteur privé concerné, des associations de parents et d'autres parties prenantes pertinentes, afin de favoriser les échanges et influencer les politiques et législations en rapport avec les points importantes soulevés par la présente Résolution.
- La sensibilisation qui sera menée par les APD sur leur territoire national viendra renforcer l'impact de la Résolution et favoriser les échanges nécessaires sur la question des plates-formes d'apprentissage en ligne, des bonnes pratiques en matière de gestion des données et, plus généralement, de traiter des droits à la protection des données dans les classes.
- Par exemple, les APD peuvent s'associer aux autorités éducatives pour aider les parents et enseignants à mieux comprendre les enjeux en termes de données personnelles liés à l'utilisation des plates-formes d'apprentissage en ligne. Cette connaissance du sujet peut également aider dans des contextes non couverts par la présente Résolution (par exemple, l'utilisation d'applications de soutien scolaire en ligne).

d) Se concerter avec les organisations internationales et groupes pertinents de la société civile pour promouvoir et donner suite à la présente Résolution

- Les APD sont invitées à mobiliser leurs contacts utiles dans les réseaux des organisations internationales et structures de la société civile concernées par la protection des données, par les enfants et les jeunes, par l'éducation et l'apprentissage, pour partager avec eux le contenu de la présente Résolution.
- Ces organisations et structures peuvent contribuer à proposer des nouvelles perspectives et expertises pour favoriser le développement de plates-formes d'apprentissage en ligne qui soient plus respectueuses de la vie privée, en réduisant les risques et valorisant leurs

apports. Elles peuvent également aider à créer un effet d'entrainement au plan régional et international pour coordonner les diverses initiatives.

e) Coopérer les uns avec les autres, ainsi qu'avec le Groupe de travail international sur l'éducation au numérique pour partager des ressources, des connaissances et des bonnes pratiques.

- Il est fortement conseillé aux APD de poursuivre la collaboration et le partage de leurs expériences dans le cadre de la mise en œuvre de la présente Résolution et, si des mesures d'exécution en découlent, de partager les résultats de leurs enquêtes.
- Ce partage peut se faire directement entre les APD, ainsi que par l'intermédiaire des différents mécanismes de l'ICDPPC, notamment du Groupe de travail international sur l'éducation au numérique.
- Pour sa part, le Groupe de travail international sur l'éducation au numérique est encouragé à poursuivre ses recherches et ses analyses des pratiques de traitement de données des plates-formes d'apprentissage en ligne, et à tenir à jour un référentiel des lignes directrices et codes de bonnes pratiques élaborés par les membres de l'ICDPPC ou d'autres parties prenantes, qui concernent ou font référence à la présente Résolution.