CNIL, fiche « Enseignement du premier et du second degrés : outils collaboratifs en ligne », 24 août 2026

Source : https://www.cnil.fr/fr/enseignement-premier-second-degres-bonnes-pratiques-outils-collaboratifs

Enseignement du premier et du second degrés : les règles et bonnes pratiques pour utiliser les outils collaboratifs en ligne (fiche pratique de la CNIL, 24 août 2026).

Les établissements du premier et du second degrés souhaitant recourir à des outils collaboratifs en ligne doivent se montrer vigilants concernant la protection des données personnelles. La CNIL rappelle les règles à suivre pour la mise en œuvre de ces outils.

L'accélération de la transformation numérique dans l'enseignement conduit à l'utilisation de plus en plus fréquente d'outils collaboratifs en ligne (il peut s'agir d'espaces numériques de travail (ENT) ou d'outils alternatifs aux ENT). Ces outils permettent la mise à disposition de services s'appuyant souvent sur l'informatique en nuage (cloud computing) qui facilitent la collaboration entre les personnels administratifs et enseignants, les élèves et leurs responsables légaux. Ces services impliquent, dans la très grande majorité des cas, des traitements de données personnelles, tels que : le contenu des communications entre les personnels administratifs et enseignants, les élèves et leurs responsables légaux ; les travaux des élèves ; les documents personnels des élèves stockés dans un coffre-fort numérique ; les notes des élèves et les appréciations des enseignants ; etc. Pour pouvoir les utiliser, les responsables de ces traitements doivent s'assurer de leur conformité à la réglementation en matière de protection des données. Ils pourront, pour ce faire, s'appuyer sur les conseils de leur délégué à la protection des données.

L'utilisation des outils collaboratifs en ligne peut impliquer des traitements de données personnelles soumis au RGPD. Le choix d'une base légale adéquate.

La transformation numérique dans l'enseignement a pour objectif de moderniser le service public de l'éducation en développant les usages du numérique dans les établissements scolaires. Depuis la loi du 8 juillet 2013, un service public du numérique éducatif et de l'enseignement à distance accompagne cette évolution. Il a pour missions notamment de : proposer des services numériques pour compléter et enrichir les enseignements ; mettre à disposition des enseignants des ressources pédagogiques, des contenus de formation et des outils de suivi des élèves ; faciliter la communication entre les établissements et les familles. Lorsque l'utilisation d'outils collaboratifs dans un cadre pédagogique entraîne des traitements de données personnelles, le responsable de traitement ne pourra mettre en œuvre ce dispositif qu'après avoir déterminé la base légale de chacun d'entre eux. Si les traitements répondent aux missions de service public des établissements scolaires, qu'ils soient publics ou privés, (et en particulier du service public du numérique éducation (article L.131-2 du code de l'éducation), le responsable du traitement peut s'appuyer sur la base légale de l'exécution d'une mission d'intérêt public. D'une manière générale, le consentement semble difficilement pouvoir être retenu comme base légale pour ces traitements, car pour constituer une base légale valable, le consentement doit notamment être libre, c'est-à-dire ni contraint ni influencé (par exemple par la position d'autorité du responsable de traitement). Les personnes concernées (telles que l'élève, et/ou dans la grande majorité des cas son responsable légal, ou le personnel administratif et enseignant) doivent se voir offrir un choix réel, sans avoir à subir de conséquences négatives en cas de refus.

Attention au(x) traitement(s) de données mis en œuvre par le fournisseur de l'outil collaboratif. Certains traitements sont réalisés par le fournisseur de l'outil collaboratif pour son propre compte. Le responsable de traitement doit s'assurer que l'outil n'a pas recours à des traceurs publicitaires, ces derniers étant en principe interdits, au regard du principe de neutralité du service public de l'éducation, incluant la neutralité commerciale. Si toutefois l'outil collaboratif utilise des dispositifs tels que des traceurs de suivi à des fins d'exploitation publicitaire ou de profilage par exemple, le responsable de

traitement devra désactiver ces fonctionnalités.

L'information des personnes afin d'assurer la transparence. Les personnes concernées (les élèves, leurs responsables légaux et le personnel administratif et enseignant) doivent être informées de tous les traitements de données les concernant mis en œuvre via ces outils collaboratifs en ligne. L'information doit être concise, transparente, compréhensible et aisément accessible (articles 12, 13 et 14 du RGPD) et doit notamment préciser : l'identité et les coordonnées de l'organisme responsable de traitement, ainsi que les coordonnées du délégué à la protection des données, s'il y en a un ; la finalité et la base légale de tous les traitements (voir ci-dessus « le choix d'une base légale adéquate ») ; les destinataires ou les catégories de destinataires des données, ainsi que des précisions sur les transferts envisagés de ces données vers un pays hors Union européenne ; la durée de conservation des données (ou, à défaut, les critères permettant de la déterminer) ; les droits des personnes concernées (les droits d'accès, de rectification, à la limitation, le droit d'opposition, et éventuellement le droit à l'effacement). Cette information doit être adaptée en fonction des personnes concernées. Ainsi, pour les mineurs, l'information doit être simple et pédagogique, adaptée à cette tranche d'âge. À titre d'exemple, les mentions d'information peuvent être écrites en langage clair (normes ISO 24495-1:2023 et ISO 24495-2:2025) ou s'inspirer de la méthode « facile à lire et à comprendre » (FALC) pour les usagers en situation de handicap ou présentant des difficultés de lecture et de compréhension du français. Pour aller plus loin sur les méthodes de conception d'une information adaptée : Les bonnes pratiques de transparence « Données & Design » de la CNIL ; Les ressources de la Direction interministérielle de la transformation publique (DITP) sur le langage clair et les conseils de la CNIL ; Les ressources gouvernementales sur la méthode FALC. L'information doit être facilement disponible, avant la mise en œuvre du traitement de données, par exemple lors de la première connexion du personnel ou de l'élève à l'outil collaboratif en ligne. Elle pourrait également être adressée directement (par courriel notamment) à l'ensemble des personnes concernées, et, en complément, lors de chaque rentrée (par exemple, pour le premier degré, lors de la réunion de rentrée entre le corps éducatif et les responsables légaux). En savoir plus : voir les lignes directrices du CEPD sur la transparence.

L'analyse d'impact relative à la protection des données (AIPD). L'AIPD est un outil important au regard du principe de responsabilisation des organismes responsables de traitements. Elle les aide à mettre en place des traitements de données conformes à la réglementation, et à démontrer cette conformité. Une AIPD est obligatoire pour les traitements de données susceptibles d'engendrer des risques élevés pour les droits et libertés des personnes physiques (article 35 du RGPD). Le Comité européen de la protection des données (CEPD) a publié des lignes directrices, qui identifient les critères à prendre en compte pour évaluer si une AIPD est obligatoire ou non. Ces critères incluent par exemple : un traitement de données relatif à des personnes vulnérables (par exemple mineurs, ou personnel administratif et enseignant lorsque ces derniers sont dans une relation de subordination, etc.) ; un traitement de données à grande échelle (en fonction notamment du nombre de personnes concernées, du volume de données traitées, de la durée ou de la permanence de l'activité de traitement de données, de l'étendue géographique du traitement) ; un traitement incluant des données sensibles (par exemple des données de santé). Si le traitement de données mis en œuvre dans le cadre de l'utilisation de ces outils collaboratifs en ligne répond à au moins deux des critères visés par le CEPD, une AIPD doit être effectuée avant de mettre en place le traitement. Dans la majorité des cas, il est probable qu'une AIPD soit nécessaire. En cas de doute, la CNIL recommande de réaliser une AIPD en s'appuyant par exemple sur l'outil PIA. Il appartient au responsable de traitement de réaliser l'AIPD avant la mise en œuvre du traitement. Le responsable de traitement peut demander conseil au délégué à la protection des données pour l'assister. Il peut également solliciter le fournisseur de l'outil collaboratif afin qu'il l'aide dans la réalisation de l'AIPD en sa qualité de sous-traitant (article 28.3.f du RGPD).

Les garanties présentées par le sous-traitant. Le responsable du traitement est tenu de faire appel « uniquement à des sous-traitants qui présentent des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées » (article 28.1 du RGPD). Le responsable du

traitement est chargé d'évaluer le caractère suffisant des garanties fournies par le sous-traitant et doit être en mesure de démontrer qu'il a pris en considération les éléments prévus par le RGPD. Cela nécessite la communication par le sous-traitant au responsable de traitement de documents pertinents (tels que la politique de protection des données, les conditions générales d'utilisation, la politique de sécurité de l'information, la conformité à un code de conduite RGPD, l'obtention d'une certification RGPD ou d'une certification de sécurité de la famille ISO 27000, etc.). Le CEPD a adopté un avis sur certaines obligations découlant du recours à des sous-traitants et sous-traitants ultérieurs en octobre 2024. Destiné aux autorités de protection des données, ce document peut également aider les responsables de traitement concernant l'étendue des vérifications qui doivent être faites sur la chaîne de sous-traitance. Un contrat doit être conclu entre le responsable de traitement et le sous-traitant. Ce contrat doit prévoir plusieurs mentions obligatoires, telles que l'objet, la durée et la finalité du traitement, ainsi que les obligations des parties, notamment en termes de sécurité des traitements (article 28. 3 du RGPD) et de fin de contrat (notamment s'agissant de la réversibilité et de la suppression des données au terme du contrat). En savoir plus : Le guide à destination des sous-traitants publié par la CNIL ; Clauses contractuelles types entre responsables de traitement et sous-traitant ; La fiche relative à la qualification juridique des parties et les lignes directrices du CEPD concernant les notions de responsable du traitement et de sous-traitant dans le RGPD ; Apporter une attention particulière au choix d'un fournisseur de service cloud (voir le Guide « Sécurité des données personnelles » - fiche n°22 - Cloud : Informatique en nuage).

Encadrement des transferts et protection des données contre les risques d'accès par les États tiers. Le RGPD interdit que des données personnelles soient transférées vers des pays situés en dehors de l'Union européenne en l'absence d'un niveau de protection suffisant et approprié des données. Le chapitre V du RGPD prévoit plusieurs outils juridiques permettant l'encadrement des transferts. Le responsable de traitement doit s'assurer que ces transferts ou le recours à des fournisseurs soumis à des réglementations étrangères soient suffisamment sécurisés, à la fois d'un point de vue juridique et en termes de cybersécurité (mesures techniques supplémentaires). En raison de la vulnérabilité des personnes concernées (personnes mineures) et du fait que ces outils peuvent conduire au traitement d'une quantité considérable de données, dont certaines sont sensibles (à titre d'exemple des données de santé), la CNIL recommande d'assurer une protection des données contre les risques de divulgation à des autorités publiques de pays tiers. À titre d'exemple, le recours à un prestataire bénéficiant de la qualification SecNumCloud de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) permet de garantir la soumission exclusive du prestataire au droit européen. Par ailleurs, conformément à la doctrine technique du numérique pour l'éducation, le décret n° 2025-1165 du 5 décembre 2025 impose aux collèges et lycées publics d'utiliser des outils et services numériques respectant certaines prescriptions techniques de sécurité, d'interopérabilité et de numérique responsable fixées par le ministre.

Textes de référence : Articles 12 du RGPD (Transparence et information des personnes) ; Articles 13 du RGPD (informations à fournir en cas de collecte directe de données) ; Articles 14 du RGPD (informations à fournir en cas de collecte indirecte de données) ; Articles 28 du RGPD (sous-traitant) ; Articles 35 du RGPD (AIPD) ; Chapitre V du RGPD (transfert de données hors UE) ; Lignes directrices sur la transparence au sens du règlement (UE) 2016/679 ; Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est « susceptible d'engendrer un risque élevé » aux fins du règlement (UE) 2016/679 ; Avis 22/2024 relatif à certaines obligations découlant du recours à un ou plusieurs sous-traitant(s) ou sous-traitant(s) ultérieur(s) ; Lignes directrices 07/2020 concernant les notions de responsable du traitement et de sous-traitant dans le RGPD.