Bac à sable « EdTech »

Les recommandations de la CNIL aux lauréats

À noter

Ce document constitue une **synthèse des principales recommandations** formulées au porteur de projet lors de son accompagnement « bac à sable ». Ces recommandations, applicables à la date de rédaction du document, s'appuient sur les informations communiquées par le porteur de projet et ses échanges avec la CNIL.

Elles sont publiées pour en faire **bénéficier les acteurs du secteur de l'éducation** et **aider les innovateurs** à développer leur solution **sur des projets similaires**.

Juin 2023

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

Table des matières

Le projet « Daylindo » : développer un portfolio de compétences des apprenants

La CNIL a accompagné la société Daylindo de juin 2022 à janvier 2023 sur le développement d'une plateforme permettant de faciliter les transmissions d'informations relatives aux formations suivies et aux compétences acquises dans le milieu professionnel, en proposant notamment un **portfolio de compétences**.

Ce portfolio a vocation à permettre de suivre, tracer et évaluer les compétences acquises par les salariés tout au long de leur vie au sein de l'entreprise.

Il permet plus spécifiquement d'instaurer un **dialogue entre l'apprenant et les différents acteurs intervenant dans sa formation pour suivre sa montée en compétence**.

L'enjeu était double :

- développer un dispositif permettant de **tracer l'acquisition de compétences** dans un contexte professionnel marqué par une pluralité d'acteurs (formateurs pédagogiques et/ou opérationnels, apprenants).
- proposer des **solutions adaptées aux contraintes diverses ;** le dispositif ayant vocation à être utilisé dans des secteurs d'activité caractérisés par une obsolescence des compétences plus ou moins rapide.

Les équipes de la CNIL ont donc accompagné la déléguée à la protection des données de Daylindo sur ces aspects.

Les trois questions suivantes ont été traitées lors de l'accompagnement « bac à sable ».

1. La minimisation des données : comment limiter l'enregistrement des données par les différentes parties prenantes ?

La plateforme Daylindo permet de traiter deux catégories de données pour établir la preuve de l'acquisition des compétences :

- celles permettant de justifier de la bonne réalisation des divers exercices et évaluations des situations de travail, **téléchargées par les apprenants** ;
- celles relatives aux parcours de formation suivis, à l'évaluation et à l'acquisition des compétences, **enregistrées par les formateurs**.

Concernant les données téléchargées par les apprenants pour justifier de la bonne réalisation des exercices

Le téléchargement de documents par les apprenants comporte deux risques principaux : le traitement de données relatives à des tiers (images, vidéos, etc.) ou révélant un éventuel secret (professionnel, industriel, etc) ainsi que le téléchargement de documents non-pertinents par erreur.

Pour limiter ces risques, la CNIL a recommandé à Daylindo de :

- permettre **la visualisation,** avant le téléchargement sur la plateforme, du document ayant vocation à faire office de preuve afin que l'apprenant **confirme son choix de téléchargement** et que tout risque d'erreur soit écarté ;
- insérer un **message « pop-up** » rappelant qu'aucune tierce personne ne doit être visible sur les images téléchargées et qu'aucune information couverte par un secret ne doit être révélée ;
- mener une **réflexion autour de la minimisation des données par secteurs d'activités**. Certaines formations ou parcours ne nécessitant pas le téléchargement de vidéos,

d'images, de sons ou de zones de commentaires libres pour évaluer les compétences, cette option pourrait être écartée par Daylindo et/ou l'entreprise cliente.

Concernant les données enregistrées par les formateurs

La définition des données pertinentes pour évaluer la montée en compétence, c'est-à-dire celles relatives aux parcours suivis par les apprenants et aux modalités d'évaluation, revient aux **référents pédagogiques et/ou opérationnels** au nom de la **liberté pédagogique**.

La nature des données peut également varier selon la formation suivie et le secteur d'activité.

Il a été recommandé à Daylindo et aux entreprises clientes de **sensibiliser les référents sur** la nécessité de se montrer prudents lors de l'utilisation de la plateforme et de la conception des parcours, de manière à enregistrer uniquement les données nécessaires à l'évaluation des compétences.

Cette sensibilisation pourrait être réalisée au moyen d'une **charte ou d'une notice informative** portée à la connaissance des référents dès leurs premières connexions.

2. La conciliation du principe de conservation limitée des données avec l'obsolescence des compétences

Pour le projet *Daylindo,* la définition de la durée de conservation nécessite de prendre en compte la question de **l'obsolescence des compétences**.

Il a été recommandé pour ce projet de définir les durées de conservation au regard de **la durée de validité de la compétence**, résultant tant de la nature de la compétence acquise que du secteur d'activité concerné.

Cette démarche nécessitant des échanges avec les acteurs sectoriels, il a été recommandé à *Daylindo* de retenir les durées de conservation suivantes jusqu'à ce que des durées sectorielles soient définies :

- pour les formations considérées comme « techniques » (apprentissage d'un geste par exemple) : une **durée de conservation courte de deux ans en base active** des données relatives à l'acquisition d'une compétence **à compter de la date de son acquisition de la compétence**. Cette durée correspond à la durée de vie d'une compétence technique définie par l'Organisation de coopération et de développement économique (OCDE) ;
- pour les autres formations (relatives au savoir-être par exemple) : **une durée de conservation plus longue pourrait être retenue** (par exemple, cinq ans à compter de la date de l'acquisition de la compétence par exemple) ;
- à l'expiration de ces durées, il pourrait être proposé à l'apprenant une **réévaluation de la compétence** pour évaluer la pertinence d'une conservation prolongée des données, particulièrement si la compétence n'a pas été exploitée dans le cadre de l'activité professionnelle du salarié.

3. Les personnes habilitées à accéder aux données des apprenants

La solution *Daylindo* cloisonne actuellement les données personnelles de différentes manières :

- par la définition d'environnements laissée à la main de l'entreprise cliente de la solution ;
- par la création de différentes catégories d'utilisateurs selon qu'ils soient apprenants, formateurs ou représentants de l'organisme client de la solution.

La CNIL a recommandé à *Daylindo* de limiter davantage les **données accessibles aux formateurs**. Deux modalités sont envisageables :

- **restreindre l'accès des formateurs aux seules données relatives aux apprenants qu'ils suivent** ;
- permettre aux formateurs d'accéder **aux données des apprenants qu'ils suivent mais également aux données agrégées** (qui ne permettent plus l'identification des personnes) **d'autres apprenants**, pour analyser les différentes trajectoires selon les formations suivies par exemple.

Concernant les **données accessibles aux apprenants**, il a été proposé de restreindre leur accès aux seules données les concernant. Leurs informations seront accessibles à d'autres apprenants uniquement si les apprenants concernés ont consenti à un tel accès.

Le projet de « Klassroom » : développer une solution de communication notamment dans le cadre scolaire

La CNIL a accompagné la société *Klassroom* de fin juin 2022 à juin 2023 sur leur projet « Klassly ».

Ce projet consiste à développer une **solution de communication entre les parents et les enseignants du premier degré**. Cette application se présente comme une alternative aux espaces numériques de travail (ENT).

La solution « Klassly » offre aux enseignants différents **outils** :

- cahier de liaison numérique ;
- cahier de vie des activités réalisées en classe ;
- gestion des absences et des retards ;
- registre des appels ;
- communication des travaux et devoirs ;
- échanges avec les parents (conservations privées ou collectives) ;
- sondage permettant de préparer certaines activités de la classe.

« Klassly » propose aussi des **prestations annexes** telles que la gestion des activités périscolaires, l'organisation des activités de loisirs ou encore l'édition d'un livre-photos de l'année scolaire.

Les équipes de la CNIL ont accompagné la déléguée à la protection des données et les collaborateurs de la société Klassroom sur certains aspects juridiques et techniques de la démarche de mise en conformité.

L'accompagnement a notamment porté sur **l'identification du régime de responsabilité de traitement** applicable à la gestion des activités scolaires ainsi qu'à la création et la gestion des comptes utilisateurs. Il a également eu pour objet de préciser **les modalités de réutilisation des photographies des élèves** réalisées à l'occasion des activités scolaires.

Lors de l'accompagnement « bac à sable », **l'architecture technique** de cette solution a également été analysée avec la société et ses sous-traitants. À la suite de ces discussions, la CNIL a émis des recommandations techniques concernant notamment l'authentification des utilisateurs, la journalisation des accès et opérations, la gestion des incidents ainsi que la gestion des cookies et autres traceurs.

Les trois questions suivantes ont été plus spécifiquement traitées lors de l'accompagnement « bac à sable ».

1. Gestion des activités scolaires par la solution « Klassly » : qui est responsable de traitement ?

Différents acteurs peuvent décider d'utiliser la solution « Klassly » :

- la commune ;
- l'enseignant ;
- l'école représentée par son directeur.

Selon le cas de figure, le schéma de responsabilité de traitement diffère.

Hypothèse n°1 : la commune fait, elle-même, le choix d'utiliser la solution « Klassly »

Lorsque la commune[1] fait le choix d'acquérir pour les écoles/les enseignants des outils alternatifs aux espaces numériques de travail (ENT), elle passe les contrats nécessaires à leur acquisition.

Au plan opérationnel, **la commune peut procéder à la sélection de l'outil numérique qu'elle identifie comme répondant le mieux aux besoins particuliers des enseignants ou des écoles**, en prenant en compte ses finalités, la nature des données personnelles collectées, la durée de conservation, les mesures de sécurité mises en place, *etc.* À ce titre, **la commune dispose de la qualité de « responsable de traitement ».**

Le ministère de l'Éducation nationale détermine les obligations encadrant le fonctionnement et les attendus du service public de l'enseignement : il fixe les finalités attendues des applications nécessaires à atteindre ses objectifs, notamment en matière de communication avec les parents (art. D. 111-4 du code de l'éducation) ou encore de tenue du registre des appels (art. R. 131-5 du code de l'éducation). À cet égard, il **participe à la détermination des finalités du traitement. Il dispose également de la qualité de responsable de traitement.**

Conclusion

La commune n'est pas l'unique responsable de traitement. Son choix est guidé par les grands principes fixés par le ministère de l'Éducation nationale ou les directives transmises par ses représentants. **La commune et le ministère sont responsables conjoints de traitement.**

La société Klassroom a la qualité de sous-traitant.

Hypothèse n° 2 : l'enseignant ou l'école, représentée par son directeur, fait le choix de procéder à l'utilisation de l'application « Klassly » (sans intervention de la commune)

En pratique, les enseignants peuvent parfois acquérir la solution « Klassly » avec leurs fonds personnels, en souscrivant à l'offre « freemium » de Klassroom, ou en utilisant des fonds de la coopérative scolaire.

Dans ce cas, le ministère a la qualité de responsable de traitement au sens du RGPD, même si c'est l'enseignant ou l'école qui a acquis la solution.

En effet, en principe, tout traitement de données personnelles effectué par des agents ou des employés dans le cadre des activités d'une organisation est réputé avoir lieu sous le contrôle de celle-ci.

Les établissements du premier degré n'ayant pas de personnalité juridique, et par ailleurs, les enseignants et directeurs agissant en tant qu'agents de l'administration de l'Éducation nationale, le ministère de l'Éducation nationale doit être considéré comme le seul responsable de traitement.

Conclusion

En cas d'acquisition de la solution « Klassly » par l'enseignant ou l'école, **le ministère de l'Éducation nationale est responsable du traitement constitué.**

La société Klassroom a la qualité de sous-traitant.

[1] La commune a la charge des écoles publiques maternelles et élémentaires.

2. Création et gestion de comptes utilisateurs sur la solution « Klassly » : qui est responsable de ce traitement ?

La solution « Klassly » se présente comme une **plateforme d'accès à différents services**, notamment :

- « classe Éducation nationale » pour gérer les activités scolaires ;
- « classe activités périscolaires » pour organiser l'activité des accueils de loisirs municipaux ;
- « classe activités de loisirs » pour les activités privées proposées par les associations en dehors de l'école (association sportive, club d'échecs, cours de dessins, etc.) ;
- édition d'un livre de photos de l'année scolaire.

L'accès à ces différents services implique la création d'un compte utilisateur par les parents souhaitant y recourir.

Même si les données traitées sont, pour certaines, identiques, il convient de distinguer :

- **le traitement constitué aux fins de déployer et de gérer les services proposés** (par exemple, celui dont le ministère et, le cas échéant, la commune sont responsables pour la gestion des activités scolaires) ;
- **le traitement constitué aux fins de « créer et gérer le profil utilisateur »**.

Ce dernier a pour objet de disposer des données permettant d'identifier les utilisateurs. Il s'agit de leur permettre d'accéder au panel des services proposés par la société Klassroom, via un compte utilisateur unique.

De ce point de vue, seule la société Klassroom identifie les finalités de la gestion des comptes utilisateurs sans autre intervention. **Elle détermine les moyens essentiels du traitement** : catégories de données traitées, durée de conservation, destinataires, etc.

Ni le ministère de l'Éducation nationale, ni les communes n'interviennent dans la gestion des profils et des abonnements nécessaires à l'accès à l'ensemble des services proposés par la société Klassroom.

Conclusion

La société Klassroom est **l'unique responsable du traitement « création et gestion des comptes utilisateurs ».**

Elle doit garantir le respect des exigences du RGPD et de la loi Informatique et Libertés.

3. Les photographies des élèves : la société Klassroom peut-elle réutiliser les données collectées à l'occasion de la création d'une classe « Éducation nationale » ?

Si les parents le souhaitent, les photographies prises en classe et intégrées dans le cahier de vie mis en ligne, via l'application « Klassly », peuvent être imprimées sous la forme d'un livre-photos.

En tant que **sous-traitante du ministère de l'Éducation nationale, la société Klassroom ne peut réutiliser les données issues de la classe qu'à la condition d'obtenir l'autorisation du ministère.**

Avant de délivrer cette autorisation, **le ministère doit réaliser un test de compatibilité**[2].

Par ailleurs, **en réutilisant les données, la société Klassroom devient responsable du nouveau traitement, celui créé aux fins d'éditer le livre-photos.** Elle est responsable de sa **conformité à l'ensemble des exigences du RGPD**.

Pour tout savoir sur la réutilisation des données par un sous-traitant, nous vous invitons à consulter la fiche dédiée sur le site de la CNIL.

Conclusion

Si les parents le souhaitent, la réutilisation des photographies des élèves prises en classe pour en faire un livre-photos est possible, sous réserve de respecter certaines conditions.

[2] Klassroom ne pourra réutiliser les données personnelles pour son propre compte que si cette réutilisation est compatible avec le traitement initial.

Le projet « DATA » : constitution d'un entrepôt de traces d'apprentissages des apprenants en vue de leur publication et de leur analyse

France Université Numérique (FUN) est un **groupement d'intérêt public** issu d'une initiative ministérielle et regroupant plus de quarante membres parmi lesquels l'Etat, les principaux établissements d'enseignement supérieur mais également des organismes de recherche, ainsi que d'autres structures publiques. Ce GIP a vocation à fédérer les projets de cours en ligne des universités et écoles françaises.

FUN est l'opérateur de la plateforme « FUN MOOC », un site web de cours en ligne ouverts à tous, sur laquelle le parcours des apprenants conduit à l'enregistrement de « traces d'apprentissages » (voir ci-dessous).

Son projet, nommé « *DATA* », a pour objectif **de constituer un entrepôt de traces d'apprentissage des apprenants et de les valoriser par des analyses**, par la restitution des données ou de résultats agrégés aux apprenants et aux équipes pédagogiques, ainsi que par leur diffusion.

En constituant un entrepôt à partir de ces données en vue de leur analyse, **le porteur de projet cherche à améliorer la transparence envers les apprenants, à favoriser l'individualisation de leur parcours et à répondre aux besoins de la recherche pour l'amélioration des pratiques pédagogiques**.

FUN envisage de :

- créer un tableau de bord permettant à l'apprenant de visualiser sa progression au sein du parcours dans lequel il est inscrit, et d'exporter ses données ;
- créer un tableau de bord permettant aux enseignants de disposer d'indicateurs globalisés et individualisés sur leurs formations ;
- partager des jeux de données pseudonymisés à des chercheurs identifiés ;

  publier des jeux de données anonymisés.

Suivi de mai à décembre 2022 par une équipe d'agents de la CNIL, FUN a soulevé trois questions prioritaires pour permettre la mise en œuvre de ce projet dans le respect de la protection des données personnelles.

Les équipes de la CNIL ont aidé FUN notamment en ce qui concerne **les mesures et vérifications à mettre en œuvre afin d'anonymiser les données**. Elles ont aussi formulé des **recommandations pour l'ouverture des données**, ou mise en *open data*.

1. Quelle démarche adopter pour considérer que les données d'apprentissage issues de la plateforme de FUN sont anonymes ?

Lors de leur utilisation de la plateforme FUN MOOC, les actions des apprenants (ex. : visionnage de vidéos, les clics sur les contenus proposés et les réponses aux tests) génèrent des données appelées **« traces d'apprentissage »**.

Ces données décrivent précisément le parcours des apprenants et peuvent être révélatrices de leur progression, des difficultés rencontrées ou encore des thématiques des cours qui les intéressent. **Elles constituent donc des données personnelles**, et leur traitement doit être conforme à la règlementation en vigueur.

En constituant un entrepôt de traces d'apprentissage, FUN souhaite répondre à plusieurs objectifs, parmi lesquels **l'ouverture des données ou *open data***, initiée par la stratégie nationale en la matière prévue par la loi pour une République numérique.

Le porteur de projet a donc interrogé la CNIL sur la démarche à adopter pour considérer que les traces d'apprentissage pouvaient être anonymes au sens de l'avis du G29 sur les techniques d'anonymisation[3] en vue de leur ouverture en données ouvertes (*open data*).

Pour mener à bien cette analyse, la CNIL a formulé plusieurs recommandations et conseils au porteur de projet.

- **Mener une sélection des données dont le partage est strictement nécessaire** en application du principe de minimisation et afin de réduire les risques de réidentification.

  La granularité des données et le nombre de catégories de données sont des facteurs pouvant accroître la possibilité d'une réidentification ; exclure certaines données du partage telles que les caractéristiques personnelles de l'apprenant (âge, sexe, lieu de résidence, etc.) permet donc de réduire le risque de réidentification. De plus, **l'utilisation du format « xAPI »**[4] pour toutes les données a été encouragé : l'utilisation de ce format unique est une pratique saine en ce qu'elle permet de limiter les données aux seules catégories choisies.

- **Le risque de réidentification doit être évalué en tenant compte de l'ensemble des données disponibles à un potentiel attaquant**.

  Le risque de corrélation entre les données anonymisées et d'autres données, disponibles par ailleurs sur la plateforme FUN MOOC ou via d'autres sources, doit être pris en compte. FUN a donc été encouragé à **limiter l'accès aux données tierces** pouvant faciliter une réidentification, tel que le pseudonyme des apprenants qui permet de visualiser leur activité sur les forums de discussion, par exemple.

- **Déterminer de manière exhaustive et précise les résultats attendus** des analyses sur les données anonymisées.

  Tout procédé d'anonymisation entraîne une perte d'information, ou d'« utilité » des données, mais cette perte peut être modérée en déterminant **les caractéristiques statistiques** que l'on souhaite conserver après l'anonymisation.

  Il est ainsi recommandé de **sélectionner un procédé d'anonymisation spécifique au besoin** des destinataires des données anonymisées afin d'éviter une perte d'« utilité » trop importante avec un procédé d'anonymisation généraliste.

  A titre d'exemple, un enseignant pourrait identifier les passages les plus complexes de son cours en disposant du pourcentage d'apprenants ayant cliqué sur « pause » sur le passage du cours en question plutôt qu'en disposant de l'ensemble des actions des apprenants anonymisé par un procédé généraliste comme la confidentialité différentielle[5].

- **Les méthodes d'anonymisation choisies doivent correspondre à l'état de l'art** et tenir compte des attaques les plus courantes mais également des risques émergents.

  À cet égard, il a été recommandé de **solliciter la communauté scientifique** afin d'évaluer l'efficacité de différentes méthodes d'anonymisation et de soumettre les données ainsi anonymisées à des attaques fictives. FUN a été encouragé à recourir à des données synthétiques[6] autant que possible dans le cadre d'expérimentations.

---

[3] Lignes directrices sur la transparence au sens du RGPD, groupe de travail « article 29 », cnil.fr

[4] Voir plus d'informations sur xapi.fr

[5] Procédé d'anonymisation pouvant être atteint par plusieurs mécanismes et impliquant notamment l'introduction d'aléa dans les données traitées.

[6] Données générées par des méthodes mathématiques, représentatives des données réelles mais non personnelles - https://linc.cnil.fr/donnees-synthetiques-dis-papa-comment-fait-les-donnees-12.

2. Quelles sont les points de vigilance dans le cadre de la publication de données ?

L'ambition de FUN d'ouvrir ses données au grand public a été l'occasion pour la CNIL de rappeler son positionnement sur ce sujet. De manière constante, la CNIL est favorable aux principes d'ouverture, de partage et de réutilisation de données tout en considérant que la protection de ces dernières est la condition nécessaire pour que ces traitements soient acceptables socialement et soutenables éthiquement.

FUN prévoit l'ouverture des données collectées sur sa plateforme de MOOC, après leur anonymisation, sans restriction d'accès, notamment dans l'objectif d'alimenter la recherche scientifique dans le domaine des outils d'analyse de données au service de l'apprentissage (*learning analytics*[7]).

- La CNIL a recommandé qu'un **suivi sur le long terme** soit réalisé afin de prendre en compte **l'évolution des attaques de réidentification** sur les données anonymisées. FUN a été invité à fournir un **point de contact** afin de recevoir tout signalement concernant la possibilité d'une réidentification découverte par la communauté.

- Il a aussi été recommandé à FUN d'utiliser des techniques de partage des **données adaptées aux objectifs visés et aux risques liés aux traitements**.
  La CNIL a notamment considéré que le partage des données sur la plateforme data.gouv.fr opérée par la Direction Interministérielle du Numérique était adapté au niveau de sécurité visé. Elle a invité FUN à privilégier l'accès aux données **par voie d'API** sur le long terme selon ses recommandations[8]. Provisoirement, un accès par téléchargement d'un fichier unique a semblé adapté, avant que le procédé d'anonymisation des données ne soit automatisé.

- **L'encadrement de l'accès et de la réutilisation des données par une licence présente l'intérêt pour le réutilisateur de faciliter la lecture de ses droits et obligations**. L'utilisation d'une licence par FUN, en tant que groupement d'intérêt public, est régi par le code des relations entre le public et l'administration, qui fournit une liste des licences pouvant être utilisées[9].

- Dans la mesure où les données publiées par FUN seront anonymes, **les personnes devront en amont être informées du traitement d'anonymisation de leur données** (l'anonymisation en elle-même est un traitement soumis à la règlementation « informatique et libertés »). Pour une plus grande transparence, la CNIL a également recommandé d'informer les personnes concernées de la forme que revêtiront leurs données anonymisées qui seront publiées (cf. question n°3).

- Bien que l'accompagnement « bac à sable » n'ait pas porté sur ce point, il est rappelé que la réutilisation de données à des fins statiques est possible sans effectuer un test de compatibilité[10], au sens de l'article 6-4 du RGPD. En effet, une telle réutilisation à des fins statistiques est, par principe, considérée comme compatible avec la finalité initiale.

---

[7] Il s'agit de la discipline consacrée à la mesure, la collecte, l'analyse et la présentation de rapports basés sur des données des apprenants en contexte d'apprentissage dans le but de comprendre et d'optimiser l'apprentissage et le contexte.

[8] « Délibération n° 2023-050 du 25 mai 2023 portant adoption d'une recommandation technique relative à l'utilisation des interfaces de programmation applicatives (API) pour le partage sécurisé de données à caractère personnel », Légifrance

[9] « Licences de réutilisation », data.gouv.fr

[10] L'organisme ou la personne ne peut réutiliser des données personnelles pour son propre compte que si cette réutilisation est compatible avec le traitement initial.

3. Comment informer les apprenants et les équipes pédagogiques du traitement de leurs données ?

Dans le cadre de son projet « DATA », FUN opère différents traitements de données personnelles : collecte des données des équipes pédagogiques (notamment pour l'inscription), collecte et analyse des données des apprenants, partage de données d'apprentissage pseudonymisées avec des chercheurs, etc.

La règlementation impose d'informer les personnes du traitement de leur données personnelles pour leur permettre de connaître la raison de la collecte, de comprendre les traitements réalisés et d'assurer la maîtrise de leurs données, en facilitant l'exercice de leurs droits. Pour le projet « DATA », l'information contribue également à instaurer une **relation de confiance** avec les apprenants.

Que doit contenir l'information fournie aux personnes ?

Pour la plateforme FUN MOOC, **la CNIL a détaillé à FUN le contenu de l'information à fournir** aux équipes pédagogiques proposant les formations et aux apprenants.

Il a notamment été recommandé à FUN de préciser :

- dans le cas de *l'open data*, **la liste des destinataires** (par exemple les personnes physiques ou morales ayant accepté la licence de réutilisation des données publiées par FUN), obtenue en permettant aux destinataires de s'identifier ou d'indiquer à quelle catégorie d'organisme ils appartiennent ;
- la durée de conservation des données par FUN ainsi que **les durées recommandées aux réutilisateurs dans la licence de réutilisation**.

Sous quel format présenter l'information aux personnes ?

- Il est possible de prévoir une **information en deux étapes**. Un premier niveau peut être prévu sur une page web comportant les informations principales, puis un deuxième niveau d'information accessible depuis cette même page via un lien renvoyant vers une notice complète, telles des CGU[11].
- Il est recommandé que ce deuxième niveau permette d'accéder facilement à **l'intégralité des informations à un endroit unique ou dans un même document**.
- La CNIL a vivement encouragé l'intention de FUN de **publier leur analyse d'impact relative à la protection des données** dans la mesure où elle est de nature à contribuer à améliorer la confiance entre les parties prenantes.

Pour aider FUN à identifier la forme de l'information la plus adaptée dans le cas du projet « DATA », **un atelier sur le design de l'information animé par le Laboratoire d'Innovation Numérique de la CNIL (LINC) a été organisé** : les conclusions de cet atelier ont permis de compléter et illustrer les recommandations fournis par la CNIL.

[11] RGPD : exemples de mentions d'information, cnil.fr

Le projet « MyToutatice » : fournir un « *cloud* personnel » pour les élèves connectés à leur espace numérique de travail

La CNIL a accompagné l'académie de Rennes de fin juin 2022 à février 2023 sur leur projet « MyToutatice ».

Ce projet vise à fournir un **Espace Numérique Personnel** (ENP) aux élèves et aux agents de l'académie de Rennes, tout au long de leur scolarité ou de leur carrière, afin de leur redonner **la maitrise de leurs données personnelles** et de les accompagner dans cette démarche de réappropriation, de protection et de sécurité de leurs données.

Conçue comme un « **cartable numérique personnel** », la solution « MyToutatice » permet de récupérer et stocker les contenus dispersés dans diverses applications (Espace Numérique de Travail – ENT, Pronote, Pix, etc.) grâce à des applications choisies par l'académie.

Le dispositif s'appuie actuellement sur une solution en source ouverte (*open source)*.

La CNIL a accompagné la déléguée à la protection des données, la cheffe de projet et l'officier de sécurité des systèmes d'information **sur différents aspects juridiques, sur la démarche de conformité et les outils nécessaires pour y parvenir**.

L'accompagnement a notamment porté sur l'identification des bases légales adéquates pour les différents usages qui pourront être faits de l'ENP (par les agents dans le cadre de leurs missions, et les élèves dans le cadre de leur scolarité).

Les équipes de la CNIL et celles de l'académie ont également travaillé autour de l'information, notamment lors d'un atelier sur le design de l'information pour identifier comment présenter une information claire et facilement accessible aux différentes catégories de personnes concernées.

Les trois questions suivantes ont été traitées lors de l'accompagnement « bac à sable ».

1. La licéité d'un traitement « Espace Numérique Personnel » déployé en milieu scolaire

La première étape pour l'académie de Rennes a été de déterminer **des finalités explicites et légitimes** au traitement « MyToutatice ».

Au regard des différents usages qui pouvaient être faits de l'ENP par chaque catégorie de personne concernée (par les agents dans le cadre de leurs missions, et les élèves dans le cadre de leur scolarité), plusieurs finalités peuvent être retenues.

Dans un second temps, la CNIL et le porteur de projet ont identifié **la ou les bases légales** au regard des finalités et du contexte du traitement.

- **Pour les opérations de traitement qui poursuivent des finalités « scolaires »** (par ex. : suivi des travaux scolaires pour les professeurs) : la base légale de la « **mission d'intérêt public** » a été considérée comme la plus appropriée pour fonder, au moins en partie, le traitement « MyToutatice ».
- **Pour les opérations de traitement qui ne rempliraient pas les critères requis pour reposer sur cette dernière base légale**, il a été convenu que ces traitements pourraient être fondées sur le **consentement** des personnes concernées.

Cela concerne, par exemple, les opérations de traitement réalisées dans le cadre de l'ENP « agents » qui s'inscriraient davantage dans une perspective de « gestion de carrière » ou les opérations réalisées dans le cadre de l'ENP « élèves » qui découlent de certaines fonctionnalités (application « photos » ; certains connecteurs facultatifs tels que « Tracemob »).

L'académie de Rennes a été invitée à être vigilante sur les **modalités de recueil du consentement** – et l'information afférente – qui diffèrent selon la catégorie de personnes concernées (adulte ; enfant de plus ou moins de 15 ans).

Au regard de l'objet du traitement « MyToutatice », il a été recommandé **d'associer**, dans tous les cas, **les mineurs de moins de 15 ans à la démarche du consentement**. En effet, l'ENP « MyToutatice » constitue un espace mis à disposition du mineur et qui a vocation à être utilisé comme un « cartable personnel » ; l'absence d'association du mineur à l'ouverture d'un espace qui lui est dédié serait donc contraire à l'esprit du projet. Il vise, parmi les mineurs de moins de 15 ans, des personnes scolarisées au collège – lesquelles apparaissent pouvoir consentir de manière éclairée au traitement de leurs données (moyennant des modalités de collecte et une information adaptée).

2. La mise en place d'une information adaptée aux différentes catégories de personnes concernées

La CNIL et l'académie ont travaillé autour de l'information, notamment lors d'un **atelier sur le design de l'information**, pour identifier comment fournir une information claire et facilement accessible aux différentes catégories de personnes concernées (élèves, agents, professeurs) – futurs utilisateurs d'un *cloud* personnel « MyToutatice ».

Sur le plan de la **méthode**, il a été recommandé au porteur de projet, :

- de préparer, dans un premier temps, des mentions d'information à portée générale – qui pourront être mises à la disposition des agents ;
- puis d'adapter ces informations aux mineurs, en vue de la délivrance de mentions spécialement destinées à ces derniers.

Recommandations sur le contenu, la forme et l'accessibilité de l'information

La CNIL a notamment recommandé à l'académie de Rennes :

- de décrire en des **termes simples** le dispositif (applications installées, applications proposées mais non obligatoires, etc.) ;
- de distinguer clairement le traitement « Espace Numérique Personnel » (ENP) du traitement « Espace Numérique de Travail » (ENT) ;
- **d'éviter d'utiliser des termes trop juridiques**, techniques ou spécialisés (notamment au regard du public concerné) ;
- de distinguer les conditions générales d'utilisation (CGU) des mentions d'information[12] ;
- de privilégier la **forme active** et de procéder à des illustrations (exemples, cas concrets) ;
- de prévoir **plusieurs niveaux d'information** avec, au-delà des mentions écrites, une information orale des personnes concernées (par ex. : lors des échanges « parents-professeurs ») ;
- de fournir les mentions d'information lors de **la création du compte** ;
- dans la mesure du possible, d'associer les personnes concernées au travail d'adaptation du design du dispositif ;
- de se rapprocher du sous-traitant pour l'adaptation de certaines fonctionnalités du dispositif.

[12] Lignes directrices du CEPD sur la transparence au sens du RGPD : les informations des personnes concernées sur le traitement de leurs données « *devraient être clairement différenciées des autres informations non liées à la vie privée telles que des clauses contractuelles ou des modalités d'utilisation générale* » (p. 7).

Information et sensibilisation des mineurs

Lorsqu'un responsable de traitement cible des mineurs, l'information doit être formulée « *en des termes clairs et simples que l'enfant peut aisément comprendre* »[13].

Il a ainsi été recommandé à l'académie de Rennes :

- de prévoir des mentions d'information **adaptées à différentes tranches d'âge**, et plus généralement au degré de maturité des élèves concernés (par ex. : rédaction de deux versions des mentions d'information, pour les moins de 13 ans et pour les 13 ans et plus ; ou mentions spécifiques aux collégiens et mentions adaptées pour les lycéens) ;
- d'envisager un point de **sensibilisation générale** des élèves à la protection des données ;
- d'employer des formulations adaptées et simplifiées permettant à l'élève de **comprendre que l'information lui est adressée**.

Il a également été conclu qu'il était nécessaire de renforcer l'information des mineurs par le **design** en concevant des interfaces transparentes et simples.

3. Les modalités d'accès aux données et aux contenus des élèves

Le développement d'un espace numérique personnel à destination de collégiens et lycéens a soulevé la question de l'articulation entre :

- la logique du projet – qui est de fournir un cartable **personnel** aux élèves, permettant de stocker différents contenus (dont des données personnelles) ;
- le **besoin, identifié par l'académie, d'accéder** à certains contenus de l'élève.

L'objectif pour la CNIL et l'académie était de délimiter **dans quelles circonstances il serait possible d'accéder aux données de l'élève**, au regard de la règlementation relative à la protection des données personnelles et dans le respect de la logique de « cartable numérique personnel ».

Dans le cadre de cet accompagnement, **3 hypothèses** ont été envisagées.

Hypothèse n°1 : l'exercice du droit d'accès par la personne concernée – en particulier par un élève mineur

En France, ce sont les parents (représentants légaux) qui devraient exercer, en principe, les droits du mineur jusqu'à sa majorité. Toutefois, la CNIL recommande que **les mineurs puissent exercer directement leurs droits sur leurs données personnelles**.

La CNIL a formulé les **recommandations** suivantes concernant l'exercice du droit d'accès par un élève mineur :

- l'élève mineur (collégien) devrait – par principe – être reconnu comme capable d'exercer son droit d'accès (puisque celui-ci lui appartient) ;
- une réponse favorable doit, par conséquent, pouvoir être apportée par le recteur d'académie à l'élève mineur qui effectuerait une demande de droit d'accès ;
- néanmoins, cette capacité d'agir de manière autonome est sans préjudice pour les parents d'exercer ce droit au nom de leur enfant et de l'accompagnement dans leur démarche ;
- pour faciliter l'exercice effectif des droits de l'élève mineur sur ses données, toutes les mesures doivent être prises par l'académie pour expliquer, de façon claire et compréhensible, la démarche et les voies de recours accessibles.

[13] Considérant 58 du RGPD ; voir aussi l'article 12.

Hypothèse n°2 : l'accès par un « destinataire » de données – personne qui reçoit communication de données

Conformément à la logique de « cartable personnel » et aux finalités du traitement, la CNIL a retenu que les seuls destinataires des données du traitement devraient être le sous-traitant (pour les données transmises lors des phases d'authentification et de création) et la DSII de l'académie.

Sur ce point, la CNIL a formulé les **recommandations** suivantes :

- délimiter, au sein de l'AIPD et des fiches « registre », les destinataires et les données auxquelles ces derniers ont accès (la DSII de l'académie et le sous-traitant ne devraient être destinataires que des seules données transmises lors de la phase d'authentification et de création du compte) ;
- informer les personnes concernées, notamment lorsque celles-ci exercent leur droit d'accès, que ces données ont été ou seront communiquées à des destinataires.

Hypothèse n°3 : les tiers autorisés par la loi

Les hypothèses dans lesquelles l'académie de Rennes pourrait recevoir une demande de communication de données d'un tiers autorisé concernent essentiellement **des enquêtes juridictionnelles** (par ex. : réquisition dans le cadre d'une enquête de fournir des informations suite à un partage d'un contenu illicite, injurieux ou diffamatoire à partir de l'ENP).

La CNIL a indiqué que si un contenu inapproprié venait à être signalé à un professeur ou à l'administration, l'académie ne serait pas légitime à accéder à l'ENP de l'élève ou de l'agent afin de vérifier la nature des contenus stockés et partagés. Seul un tiers autorisé pourra obtenir communication des données sur réquisition judiciaire suite à un éventuel dépôt de plainte.

A cet égard, la CNIL a renvoyé le porteur de projet vers le guide pratique « Tiers autorisé » et le recueil des principales procédures.