MINISTÈRE
DE L'ÉDUCATION
NATIONALE
ET DE LA JEUNESSE

Liberté
Égalité
Fraternité

SDET

Schéma Directeur des Espaces numériques de Travail pour l'enseignement scolaire

ENT

Espace numérique de travail

Annexe Opérationnelle - version 2024
Juillet 2024

Table des matières

Table des illustrations

Table des tableaux

1. Introduction

1.1. Organisation du SDET

Le SDET est organisé en trois parties

- un document principal ;
- une annexe opérationnelle ;
- des documents d'accompagnement.

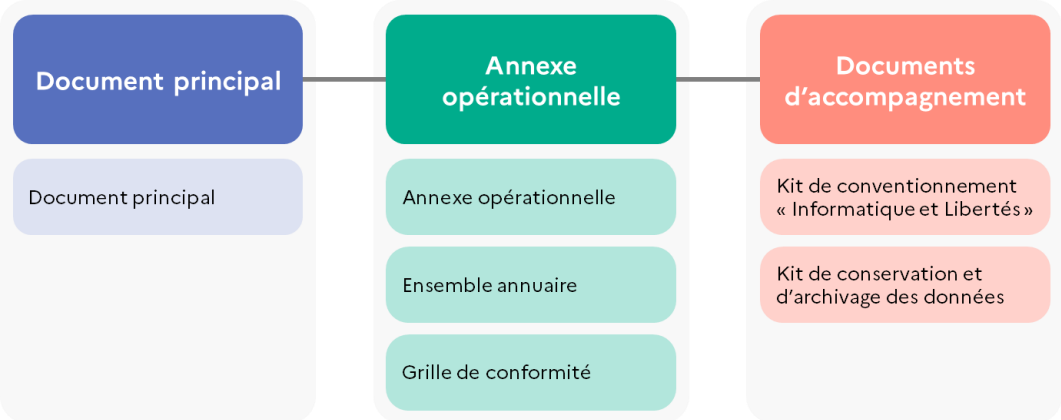

Figure 1 : Organisation du SDET

Pour connaître la version en vigueur du SDET (document principal, annexe opérationnelle, documents d'accompagnement), consulter la page de présentation du SDET[1] sur le site éduscol.

[1] Page de présentation du SDET sur le site éduscol (https://eduscol.education.fr/sdet)

1.2. Organisation de l'annexe opérationnelle

La présente **annexe opérationnelle** complète le document principal avec :

- des éléments opérationnels sur des sujets de mise en œuvre concernant l'authentification-autorisation-SSO[2], et l'annuaire
- des éléments juridiques ;
- une grille de conformité regroupant l'ensemble des principes.

Elle est composée :

- du présent document ;
- de l'ensemble annuaire – « Annexe opérationnelle du SDET - Ensemble annuaire version 2024 » ;
- de la grille de conformité – « Annexe opérationnelle - Grilles de conformité version 2024 ».

1.3. Ensemble annuaire

L'ensemble annuaire est composé des documents suivants :

<u>Communs aux premier et second degrés :</u>

- Spécifications de l'annuaire ENT
- Evolutions des spécifications
- Annexe 2 – Alimentation depuis le SI du MEN et autres SI
- Annexe 6 – Nomenclatures ENT
- Annexe 7 – Bonnes pratiques pour l'exploitation de l'ENT et de l'annuaire ENT.

<u>Pour le premier degré :</u>

- Annexe 1 – Dictionnaire des données ENT (format tableur).

<u>Pour le second degré :</u>

[2] SSO : Single Sign-on (authentification unique)

- Annexe 3 – Caractérisation des personnes et des structures (format tableur) ;
- Annexe 4 – Schéma LDAP et nomenclatures (format tableur) ;
- Annexe 5 – Alimentation depuis le SI du MEN et depuis d'autres SI externes (format tableur) ;

2. Authentification–Autorisation–SSO (AAS)

2.1. Introduction

Ce chapitre de l'annexe opérationnelle du SDET s'inscrit dans le cadre des qualités attendues d'un ENT au titre de la sécurité, particulièrement celles de la sécurité des accès et de la confidentialité des données. Il complète les éléments décrits dans le document principal, service mutualisé de gestion d'identités et d'accès.

À cet effet, il fournit un ensemble de définitions destinées à préciser certains concepts et des principes à respecter afin que tous les acteurs de la communauté éducative de l'école ou de l'établissement scolaire évoluent dans un cadre de confiance autour de deux sujets d'attention principaux :

- La propagation des informations d'identité ;
- L'interfaçage entre l'ENT et les services externes au projet ENT (services Tiers) sans fédération d'identités.

2.1. Fédération d'identités

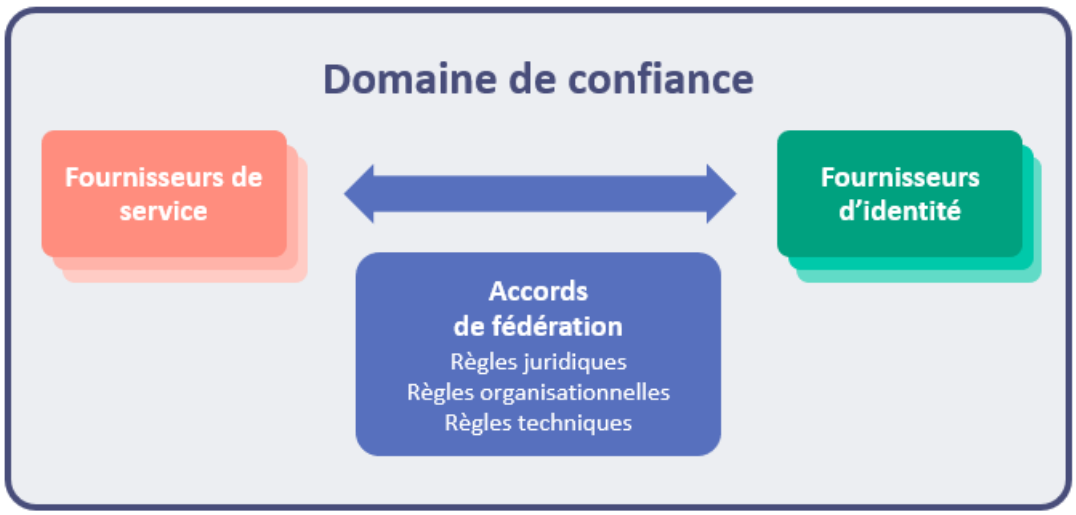

Figure 2 : Concepts clé de la fédération d'identités

La fédération d'identités s'articule autour des concepts clés suivants :

- domaine de confiance ;
- fournisseur d'identité ;
- fournisseur de service ;
- fournisseur d'attributs ;
- accords de fédération.

Les définitions de ces concepts sont désormais inscrites dans le glossaire du corpus documentaire de la doctrine technique du numérique pour l'éducation[3]

[3] https://doctrine-technique-numerique.forge.apps.education.fr/glossaire/

2.2. Propagation des informations d'identité entre l'ENT et les services externes au projet ENT

2.2.1. Généralités

Dans le cadre des projets ENT, la fédération d'identités concerne un ensemble d'acteurs de la sphère éducative qui coopèrent au sein d'un espace de confiance pour notamment gérer des identités, gérer les autorisations des utilisateurs et contrôler leurs accès.

La solution ENT peut être fournisseur de service et/ou fournisseur d'identité. Trois configurations peuvent se présenter :

- ENT fournisseur de service : c'est le cas « nominal » où l'utilisateur authentifié auprès d'un fournisseur d'identité externe souhaite accéder à un service applicatif proposé par l'ENT (ENT fournisseur de service) ; l'ENT reçoit de ce fournisseur d'identité des informations d'identité, sur la base desquelles le contrôle d'accès au service applicatif peut alors s'effectuer ;
- ENT fournisseur d'identité et fournisseur de service : c'est le cas où l'utilisateur authentifié sur l'ENT accède aux services de ce même ENT ; la mise en œuvre des mécanismes de fédération d'identités n'est pas nécessaire ;
- ENT fournisseur d'identité : c'est le cas où l'utilisateur authentifié sur un ENT souhaite accéder à un service applicatif distant (externe au projet l'ENT). Cela nécessite de transmettre des informations d'identité depuis l'ENT vers le fournisseur de service. L'ENT joue ici le rôle de fournisseur d'identité, et éventuellement de fournisseur d'attributs.

Ces cas d'usage sont illustrés sur la Figure 3 selon que l'on positionne la solution ENT en fournisseur de service ou d'identité :

- Le fournisseur de service peut-être un ENT, un autre ENT ou un service externe à l'ENT ;
- Le fournisseur d'identité peut-être un ENT ou un fournisseur d'identité externe à l'ENT.

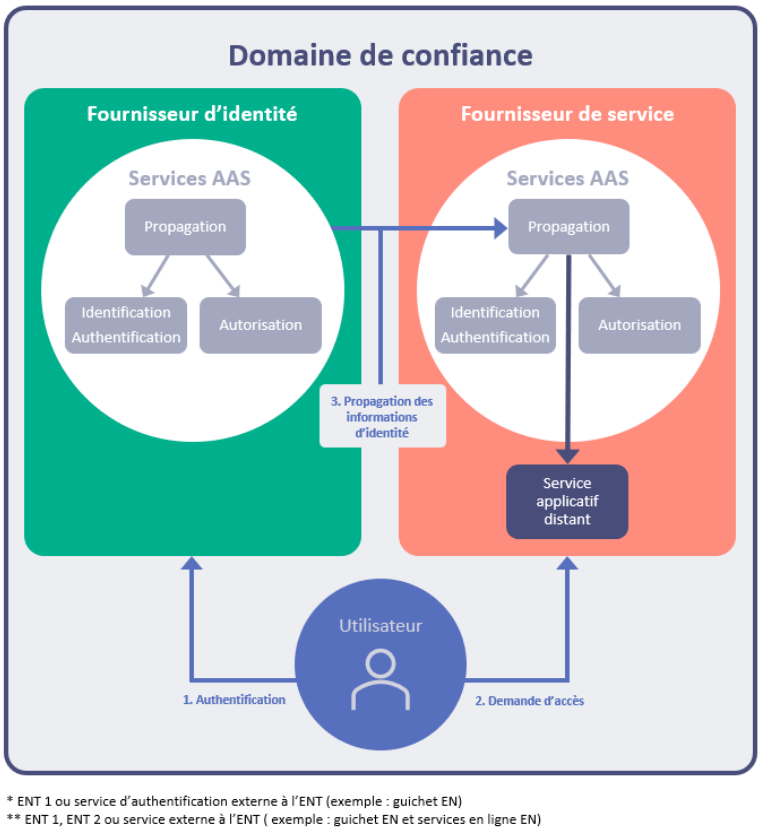

Figure 3 : Propagation des informations d'identité

Le domaine de confiance de la fédération est régi par le cadre général des règles de l'accord de fédération, qui déterminent notamment les engagements des fournisseurs d'identité et des fournisseurs de service.

Des compléments relatifs aux échanges d'informations d'identité sont donnés au chapitre 2.3 « Cas des guichets et des portails de service mis en œuvre par l'Éducation nationale ».

2.2.2. Données partagées

Afin d'assurer le fonctionnement de la fédération, et notamment de réaliser le contrôle des accès des utilisateurs aux services applicatifs, il est nécessaire de définir des données communes à tous les membres de la fédération.

2.2.3. Fonctions proposées

La fonction de **Propagation d'identités** est décrite dans le service mutualisé de gestion d'identités et d'accès du document principal du SDET.

2.2.4. Cinématiques d'accès

Ce chapitre présente les cinématiques d'accès pour différents cas d'usage.

Ces cinématiques ne sont pas exclusives les unes des autres et plusieurs d'entre elles peuvent se présenter au sein d'une même solution ENT, par exemple pour des profils utilisateurs différents.

2.2.4.1. ENT fournisseur de service

Dans les trois cas d'usage ci-après, l'ENT n'est pas fournisseur d'identité mais seulement fournisseur de service.

Il s'agit du cas de figure où l'identification / authentification des utilisateurs de l'ENT est déléguée à un guichet externe : un guichet de l'Éducation nationale pour les personnels de l'Éducation nationale, pour les élèves et leurs responsables, un guichet de la collectivité pour un personnel de collectivité.

Se référer aux principes (AAS-18 et AAS-19) listés dans le chapitre 2.6. Récapitulatif des principes

2.2.4.1.1. Cas d'usage : accès à un service ENT depuis le portail de l'ENT

Ce cas d'usage décrit la cinématique d'accès dans le cas où l'utilisateur accède à l'ENT depuis le portail de l'ENT.

Remarque : ce cas d'usage ne peut pas s'appliquer à tous les utilisateurs de l'ENT : les comptes invités ou les catégories d'utilisateurs n'ayant pas de fournisseur d'identité externe doivent s'authentifier sur l'ENT.

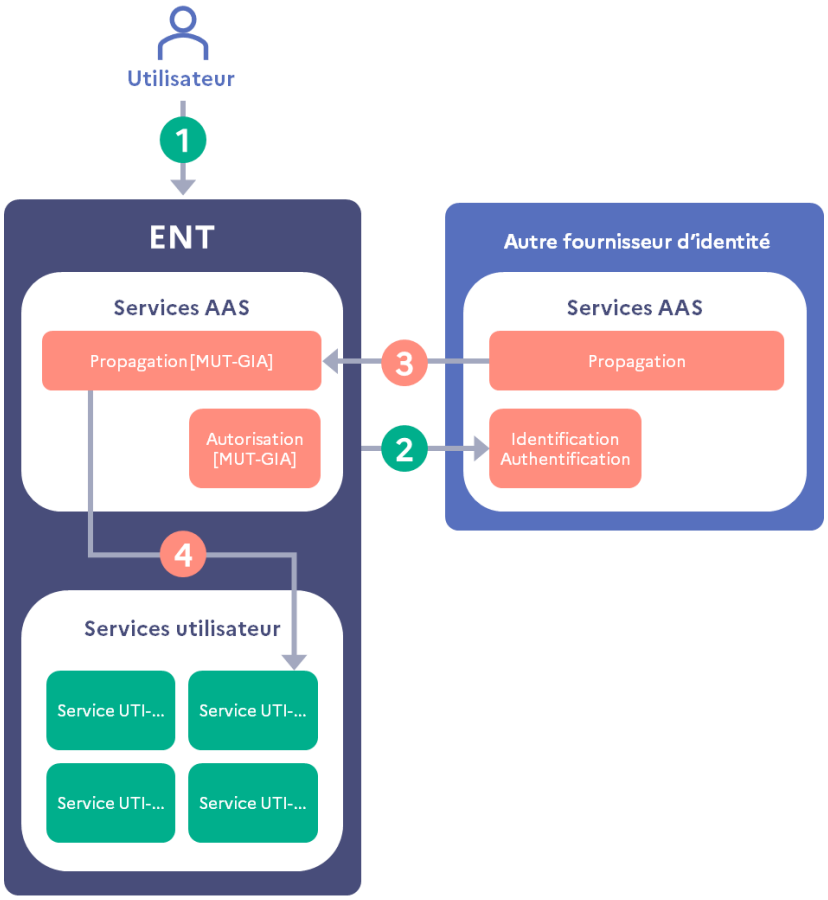

Figure 4 : Authentification déléguée à un fournisseur d'identité externe et accès à un service ENT depuis le portail de l'ENT

La cinématique d'accès indiquée à la Figure 4 est la suivante :

1) L'utilisateur non authentifié accède à l'ENT ;
2) Il indique son profil (élève, parent, enseignant…) sur le service de découverte de l'ENT ; il est redirigé vers le guichet d'authentification externe adéquat auprès duquel il s'authentifie ;
3) Le guichet externe propage les informations d'identités vers l'ENT ;
4) Le service de propagation de l'ENT propage ces informations vers le service applicatif de l'ENT.

L'utilisateur peut alors accéder aux services Utilisateurs de l'ENT auxquels il a droit.

2.2.4.1.2. Cas d'usage : accès à un service externe depuis le portail de l'ENT

Ce cas d'usage décrit la cinématique d'accès lorsque l'utilisateur travaille sur l'ENT et souhaite accéder aux services associés à son fournisseur d'identité (par exemple : ENT proposant un lien vers les services en ligne du ministère en charge de l'Éducation nationale pour les élèves et leurs représentants légaux, ceux-ci ayant été préalablement authentifiés auprès d'un guichet de l'Éducation nationale).

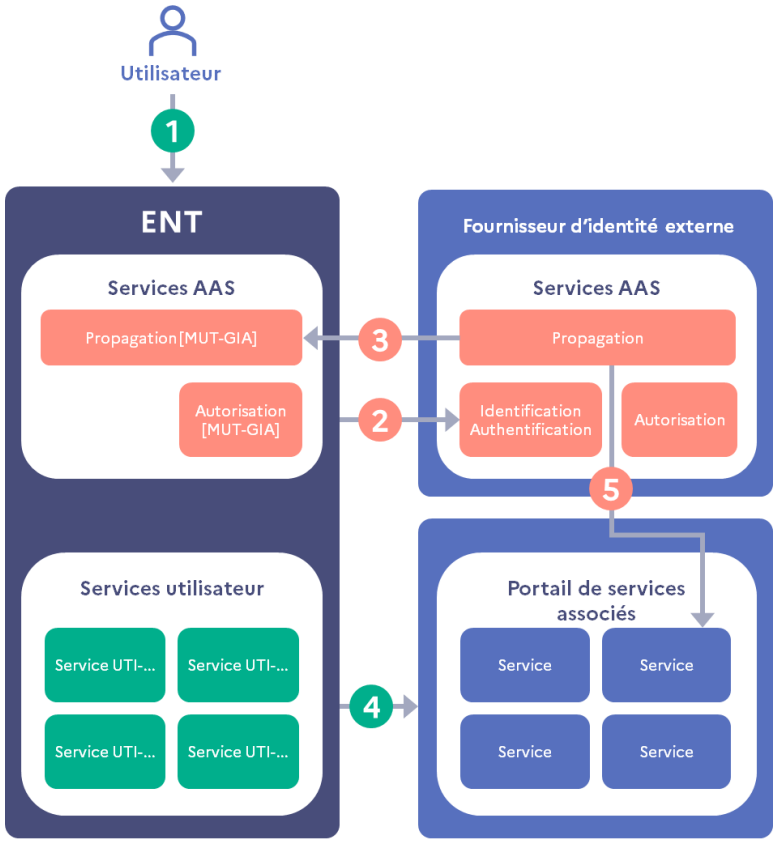

Figure 5 : Authentification déléguée à un fournisseur d'identité externe et accès à un fournisseur de service externe depuis le portail de l'ENT

La cinématique d'accès indiquée à la Figure 5 est la suivante :

1) L'utilisateur non authentifié accède à l'ENT ;
2) Il indique son profil sur le service de découverte de l'ENT ; il est redirigé vers le guichet d'authentification externe auprès duquel il s'authentifie ;
3) Le guichet externe propage les informations d'identités vers l'ENT ;
4) L'utilisateur choisit dans son ENT un lien vers un service associé au guichet externe ; le service de propagation du guichet externe propage les informations d'identité vers le portail de services associé.

L'utilisateur peut alors accéder au service externe, selon ses droits.

2.2.4.1.3. Cas d'usage : accès à un service ENT depuis un portail externe

Ce cas d'usage décrit la cinématique d'accès lorsque l'utilisateur utilise les services associés à son fournisseur d'identité, et souhaite accéder à l'ENT (par exemple : portails académiques ou portails des collectivités proposant un lien vers le portail de l'ENT).

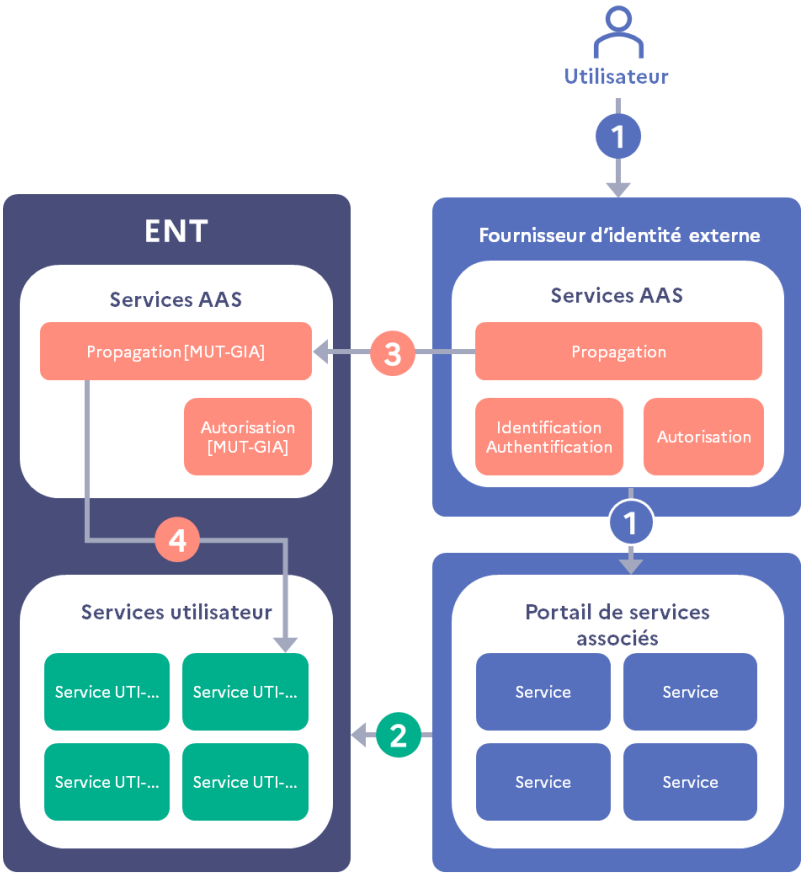

Figure 6 : Authentification déléguée à un fournisseur d'identité externe et accès à un service ENT depuis un portail externe

La cinématique d'accès indiquée à la Figure 6 est la suivante :

1) L'utilisateur non authentifié accède au portail de services associé à son fournisseur d'identité ; il s'authentifie auprès du guichet et a accès aux services proposés sur le portail ;
2) L'utilisateur sélectionne le lien vers le portail de l'ENT ;
3) Le guichet externe propage les informations d'identité vers l'ENT ;
4) Le service de propagation de l'ENT propage ces informations vers le service applicatif de l'ENT.

L'utilisateur peut alors accéder aux services Utilisateurs de l'ENT auxquels il a droit.

2.2.4.2. ENT fournisseur d'identité

Dans le cas d'usage illustré Figure 7, l'ENT est le fournisseur d'identité.

2.2.4.2.1. Cas d'usage : accès à un service externe dans un domaine de confiance depuis le portail de l'ENT

Ce cas d'usage décrit la cinématique d'accès lorsque l'utilisateur, préalablement authentifié sur son ENT et utilisant les services de l'ENT, souhaite accéder à des services externes en mode de fédération d'identités.

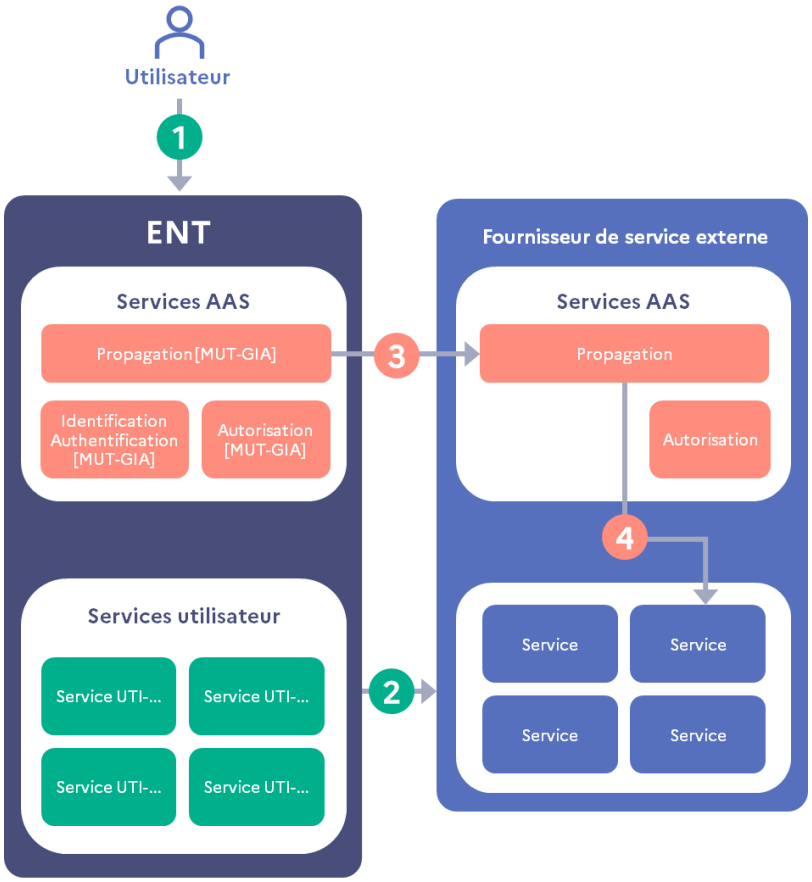

Figure 7 : ENT fournisseur d'identité et accès à un service externe depuis le portail de l'ENT

La cinématique d'accès indiquée à la Figure 7 est la suivante :

1) L'utilisateur s'authentifie sur l'ENT ;
2) L'utilisateur sélectionne le lien vers le service externe ;
3) L'ENT propage les informations d'identité vers le fournisseur de service externe ;
4) L'utilisateur peut alors accéder au service externe.

Se référer aux principes (AAS-20 et AAS-21) listés dans le chapitre 2.6. Récapitulatif des principes

2.3. Cas des guichets et des portails de service mis en œuvre par l'Éducation nationale

Les configurations et cinématiques d'accès évoquées peuvent s'appliquer aux portails de services et aux guichets d'authentification proposés par le ministère :

- Le portail « Scolarité Services » du ministère en charge de l'Éducation nationale ;
- Les autres portails académiques ;
- Les guichets d'authentification académiques Agents pour les personnels de l'Éducation nationale ;
- Le guichet national ÉduConnect pour les élèves et leurs représentants légaux.

Le ministère en charge de l'Éducation nationale et les académies ont pour ambition d'atteindre un niveau d'engagement de service des guichet équivalent à celui exigé des prestataires de la solution ENT.

Ceci suppose :

- La mise en cohérence et une bonne synchronisation des référentiels de données sur lesquels s'appuient les guichets et les annuaires ENT ;
- Une qualité de service équivalente à celle du projet ENT ;
- Des outils de supervision et de suivi de la qualité de service ;
- Une capacité de tests pour la bonne articulation entre chaque projet ENT et le guichet ;
- Le fait que le renforcement des services de l'Éducation nationale ne conduise pas à une redondance ou à une incohérence fonctionnelle entre les bouquets de service ;
- Le maintien de l'ENT comme point d'accès privilégié aux différents services de l'ENT ;
- Le lien entre l'ENT et les services de l'Éducation nationale.

2.3.1. L'authentification

La doctrine technique pour le numérique définit que le guichet d'authentification de l'Éducation nationale pour les agents est **le service socle Guichets-Agents**. Il fournit les services d'identification, d'authentification et de gestion des comptes utilisateurs associés.

De même, **le guichet national ÉduConnect** est le service socle qui fournit les services d'identification, d'authentification et de gestion des comptes utilisateurs associés pour les responsables d'élèves et les élèves.

La solution ENT peut s'articuler en fédération d'identités avec les services en ligne du ministère en charge de l'Éducation nationale et ces deux services socles selon les différentes configurations indiquées au **chapitre 2.2.4 « Cinématiques d'accès »**.

2.3.2. Mise en œuvre

La mise en œuvre du guichet national ÉduConnect est définie dans le document **« Spécifications techniques »**

2.4. Cas du guichet d'authentification de l'enseignement agricole

Le guichet d'authentification de l'enseignement agricole fournit le service d'identification, d'authentification et de gestion des comptes utilisateur pour les agents, les apprenants[4] et les personnes en lien avec les apprenants (« responsables »). Il s'agit du guichet unique pour les trois populations.

Le vecteur d'identité **FrEduVecteur** retourné par le guichet de l'enseignement agricole contient la clé de jointure de la personne (valeur de l'attribut ENTPersonJointure).

2.5. Principes pour l'interfaçage entre l'ENT et les services Tiers sans fédération d'identités

Ce chapitre apporte des principes dans le cadre de l'interfaçage entre la solution ENT et des services applicatifs Tiers (hors services en ligne du ministère en charge de l'Éducation nationale et hors GAR).

[4] Dans l'enseignement agricole, les apprenants comportent les élèves, les apprentis et les adultes en formation continue.

Selon le type d'interface fonctionnelle entre une solution ENT et un service Tiers, plusieurs catégories de services Tiers peuvent être définies. Des principes spécifiques à chaque catégorie sont donnés ci-après.

2.5.1. Présentation des différentes catégories de services Tiers

La définition des catégories de services Tiers repose sur les caractéristiques fonctionnelles de l'interface entre le service Tiers et l'ENT, et notamment les modalités d'authentification et de contrôle d'accès, le type d'informations d'identité transmises et le stockage ou non de ces informations par le service Tiers.

Les services Tiers sont ainsi répartis en cinq catégories, dont les caractéristiques sont présentées dans le tableau ci-après :

Catégorie de services Tiers hors GAR	Conditions d'accès
Catégorie 1	L'accès au service **ne nécessite ni authentification ni contrôle d'accès (accès libre).**
Catégorie 2	L'accès au service nécessite une authentification et un contrôle d'accès basés uniquement sur **l'appartenance de l'utilisateur au projet ENT et/ou à une école ou un établissement scolaire défini et/ou à son profil d'accédant[5].**
Catégorie 3	L'accès au service nécessite une authentification et un contrôle d'accès de l'accédant avec **transmission de données uniques par utilisateur mais non nominatives** (identifiant utilisateur non significatif).
Catégorie 4	L'accès au service s'effectue sur la base **d'informations non nominatives transmises par l'ENT lors de la connexion** et sur la base **d'informations nominatives sur l'accédant, dont dispose au préalable le service Tiers** (« mapping » d'identités réalisé par le service Tiers). **Le processus préalable d'inscription au service applicatif Tiers s'effectue hors ENT.**
Catégorie 5	L'accès au service s'effectue sur la base **d'informations fournies par l'utilisateur lors de la première connexion au service Tiers via l'ENT** (formulaire en ligne…). Lors des connexions suivantes, l'accédant sera reconnu par le service Tiers sur la base d'informations utilisateur transmises par l'ENT (fonctionnement identique à la catégorie 4 : mapping d'identités).

Tableau 1 : Catégories de services Tiers hors périmètre GAR selon les conditions d'accès

2.5.2. Principes fonctionnels

Pour chaque catégorie de services Tiers citée ci-dessus, les éléments suivants seront détaillés :

- La cinématique fonctionnelle ;

[5] Le profil de l'accédant est défini au chapitre **Erreur ! Source du renvoi introuvable.** « **Erreur ! Source du renvoi introuvable.** »

- Les données potentiellement transmises.

En tout état de cause, le principe de proportionnalité défini par la CNIL relatif à la protection des données personnelles doit être respecté : « *seules doivent être enregistrées les informations pertinentes et nécessaires pour leur finalité*. ».

Les données transmises ne peuvent pas être utilisées à d'autres finalités de traitement que celles indispensables à la fourniture du service.

2.5.2.1. Services de catégorie 1

Rappel : l'accès à un service de catégorie 1 ne nécessite ni authentification ni contrôle d'accès (accès libre).

2.5.2.1.1. Cinématique fonctionnelle

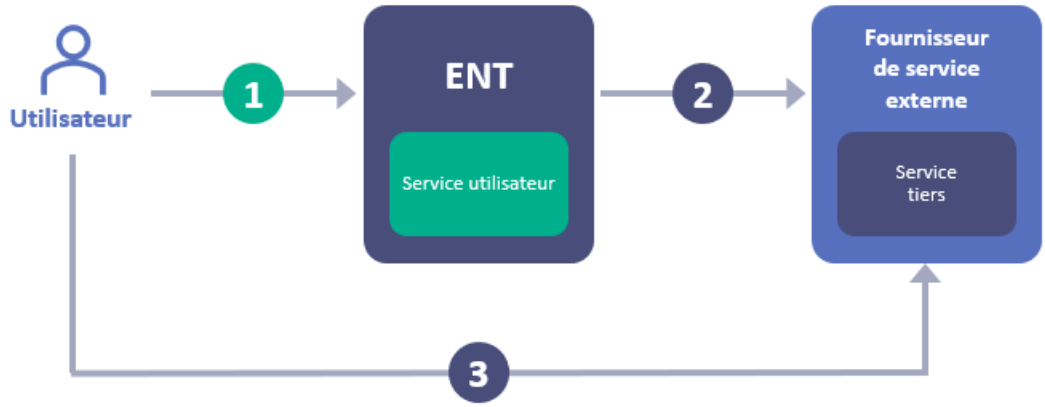

Figure 8 : Cinématique fonctionnelle pour les services de catégorie 1

Comme illustré Figure 8, la cinématique d'accès à un service de la catégorie 1 est la suivante :

1) L'utilisateur s'authentifie auprès de son ENT ou auprès d'un fournisseur d'identité externe à l'aide de son login et de son mot de passe ;
2) L'utilisateur demande l'accès au service via un lien fourni par l'ENT ;
3) L'utilisateur accède de façon anonyme au service Tiers sans qu'aucune information ne soit nécessaire pour le contrôle d'accès au niveau du service Tiers.

2.5.2.1.2. Données transmises

La règle concernant les données transmises est décrite dans le principe directeur AAS-1 (Cf. chapitre 2.6)

2.5.2.1.3. Exemple

Un utilisateur accède à un site internet qu'il a déposé dans ses favoris de l'ENT, par activation du lien.

Aucune donnée n'est envoyée par l'ENT au site externe. L'utilisateur change de sphère de responsabilité et de configuration de travail.

2.5.2.2. Services de catégorie 2

Rappel : l'accès à un service de catégorie 2 nécessite une authentification et un contrôle d'accès basés uniquement sur **l'appartenance de l'utilisateur au projet ENT et/ou à une école ou un établissement scolaire défini et/ou à son profil d'accédant.**

2.5.2.2.1. Cinématique fonctionnelle

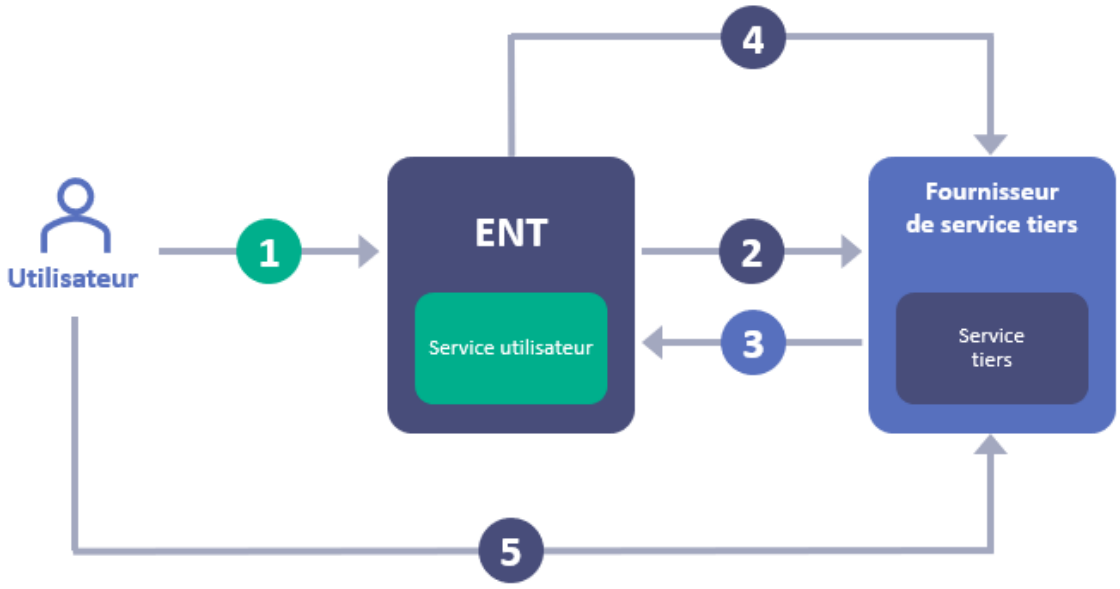

Figure 9 : Cinématique fonctionnelle pour les services de catégorie 2

Comme illustré Figure 9, la cinématique d'accès à un service de la catégorie 2 est la suivante :

1) L'utilisateur s'authentifie auprès de son ENT ou auprès d'un fournisseur d'identité externe à l'aide de son login et de son mot de passe ;
2) L'utilisateur demande l'accès au service via un lien fourni par l'ENT ;
3) Le service Tiers demande à la solution ENT la transmission d'informations sur l'accédant ;
   a) L'identification et le contrôle d'accès sont effectués par le service Tiers sur la base de **l'appartenance de l'utilisateur au projet ENT et/ou à une école ou à un établissement et/ou à son profil d'accédant** ;

b) d'autres attributs non associés à une identité décrits dans le Tableau 2 peuvent être transmis également uniquement s'ils sont indispensables au fonctionnement du service Tiers ;

4) La solution ENT fournit au service Tiers les informations demandées à l'étape précédente ;
5) L'utilisateur accède **de façon anonyme** au service Tiers.

2.5.2.2.2. Données transmises

Les règles concernant les données transmises sont décrites dans les principes AAS-2 à AAS-4 (Cf. chapitre 2.6)

Profil de l'accédant	Attributs 1er degré	Attributs 2nd degré	Nomenclatures BCN correspondantes
National_elv	Niveau de formation	Niveau de formation	N_MEF_STAT_4
National_elv	(N/A)	Filière	N_MEF_STAT_5
National_elv	(N/A)	Niveau de formation du diplôme	N_NIVEAU_FORMATION_DIPLOME
National_elv	(N/A)	Spécialité du diplôme	N_FORMATION_DIPLOME
National_elv	(N/A)	Enseignements	N_MATIERE_ENSEIGNEE
National_elv	Classe	Classe	Pas de nomenclature nationale
National_elv	Groupe(s)	Groupe(s)	Pas de nomenclature nationale
National_ens	Spécialité de poste	Discipline de poste	N_DISCIPLINE_POSTE / N_SPECIALITE_POSTE
National_ens	(N/A)	Matières enseignées	N_MATIERE_ENSEIGNEE
National_ens	Classe(s)	Classe(s)	Pas de nomenclature nationale
National_ens	Groupe(s)	Groupe(s)	Pas de nomenclature nationale
National_tut	Aucun	Aucun	(N/A)
National_dir	(N/A)	Service	N/A
National_eta	(N/A)	Service	N/A
National_aca	(N/A)	Service	N/A
National_col	(N/A)	Service	N/A

Tableau 2 : Autres attributs non associés à une identité pouvant être transmis pour les services de catégorie 2 et 3

Des traitements doivent être réalisés par les solutions ENT afin de ne transmettre que les données relatives à l'établissement à partir duquel le service Tiers est appelé.

2.5.2.3. Services de catégorie 3

Rappel : L'accès à un service de catégorie 3 nécessite une authentification et un contrôle d'accès de l'accédant avec **transmission de données uniques par utilisateur mais non nominatives** (identifiant utilisateur non significatif).

2.5.2.3.1. Cinématique fonctionnelle

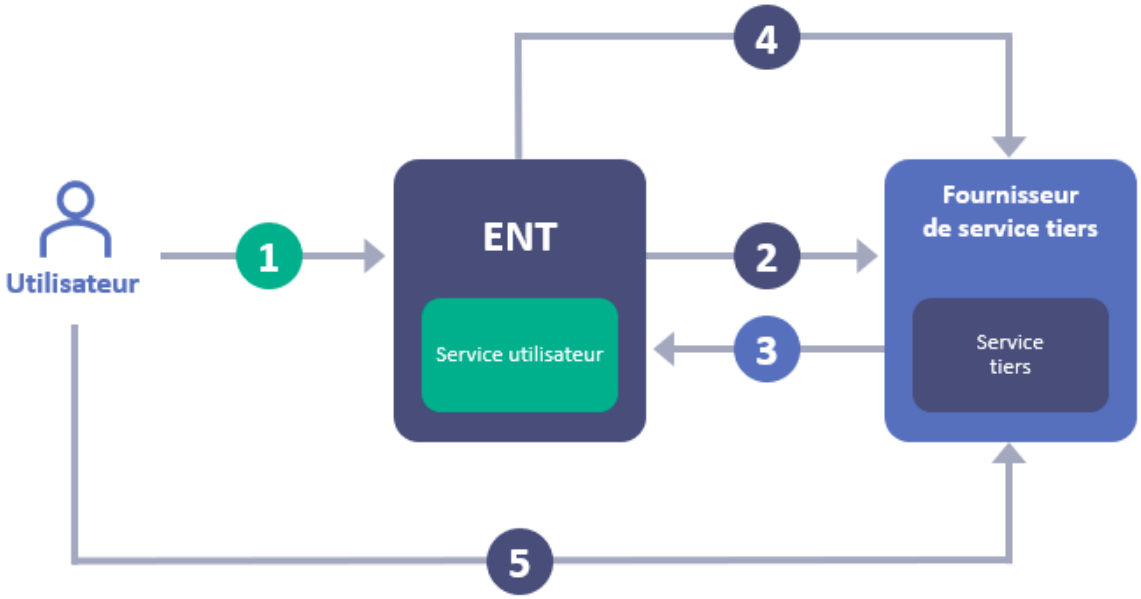

Figure 10 : Cinématique fonctionnelle pour les services de catégorie 3

Comme illustré Figure 10, la cinématique d'accès à un service de la catégorie 3 est la suivante :

1) L'utilisateur s'authentifie auprès de son ENT ou auprès d'un fournisseur d'identité externe à l'aide de son login et de son mot de passe ;
2) L'utilisateur demande l'accès au service via un lien fourni par l'ENT ;
3) Le service Tiers demande à la solution ENT la transmission d'informations sur l'accédant ;
   a) **L'authentification et le contrôle d'accès** sont effectués par le service Tiers sur la base d'un **identifiant unique par utilisateur mais non nominatif et éventuellement de l'appartenance de l'utilisateur au projet ENT et/ou à une école ou à un établissement et/ou à son profil d'accédant** ;
   b) d'autres attributs non associés à une identité décrits dans le Tableau 2 peuvent être transmis également uniquement s'ils sont indispensables au fonctionnement du service Tiers ;

4) L'ENT fournit au service Tiers les informations demandées à l'étape précédente ;
5) L'utilisateur accède **de façon anonyme** au service Tiers mais **personnalisée** au vu de l'identifiant utilisateur transmis.

2.5.2.3.2. Données transmises

Les règles concernant les données transmises sont décrites dans les principes AAS-5 à AAS-8 (Cf. chapitre 2.6).

2.5.2.4. Services de catégorie 4

Rappel : l'accès à un service de catégorie 4 s'effectue sur la base **d'informations non nominatives transmises par l'ENT lors de la connexion** et sur la base **d'informations nominatives sur l'accédant, dont dispose au préalable le service Tiers** (« mapping d'identités » réalisé par le service Tiers).

Le processus d'inscription au service applicatif s'effectue hors ENT.

2.5.2.4.1. Inscription d'un utilisateur

Les services Tiers appartenant à la catégorie 4 relèvent d'un processus d'inscription non corrélé à la connexion à un ENT. L'utilisateur s'inscrit au service Tiers et les moyens mis en œuvre pour effectuer cette inscription sont gérés par le service Tiers lui-même : inscription sur le site internet du service Tiers, inscription « papier », etc.

2.5.2.4.2. Cinématique fonctionnelle

L'accès au service via l'ENT nécessite d'établir le « mapping » entre l'utilisateur de l'ENT et le compte créé par le service Tiers lors de l'inscription de la personne. Ce « mapping » est réalisé lors de la première connexion de la personne au service via l'ENT (première connexion ou réabonnement, nouvelle année scolaire…). Le cas particulier de la première connexion est donc décrit ci-après de façon distincte de la connexion nominale.

Cas de la première connexion

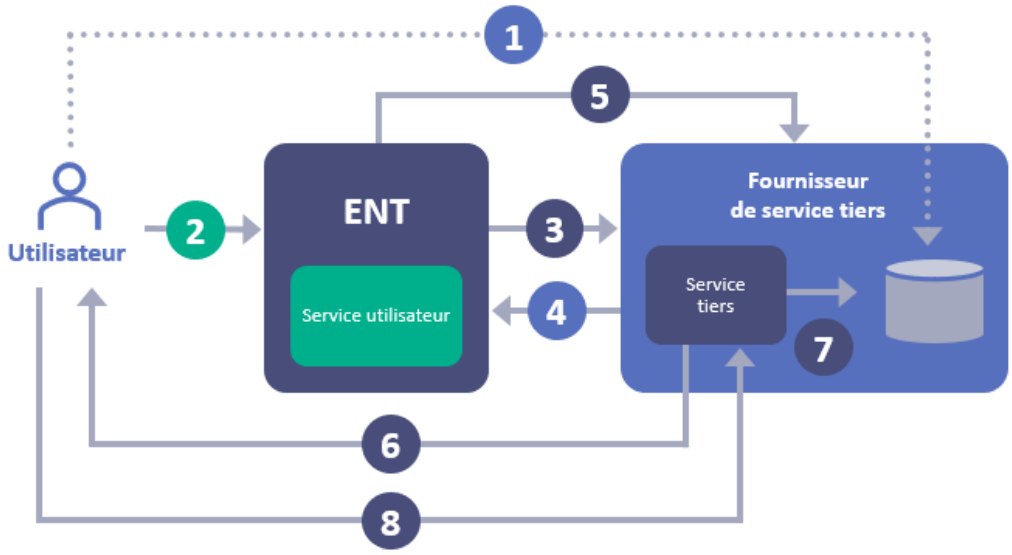

Figure 11 : Cinématique fonctionnelle pour les services de catégorie 4 (cas de la première connexion)

Comme illustré Figure 11, la cinématique d'accès à un service de la catégorie 4 est la suivante, pour la première connexion :

1) L'utilisateur s'est préalablement inscrit auprès du service via un processus hors ENT ;
2) L'utilisateur s'authentifie auprès de son ENT ou auprès d'un fournisseur d'identité externe à l'aide de son login et de son mot de passe ;
3) L'utilisateur demande l'accès au service via un lien fourni par l'ENT ;
4) Le service Tiers demande à la solution ENT la transmission d'informations sur l'accédant ;
5) La solution ENT transmet un identifiant unique pour chaque utilisateur au service Tiers qui servira de clé de jointure (par exemple, le code projet ENT et un identifiant utilisateur non associé à une identité) ;
6) À la première connexion, le service Tiers demande à l'utilisateur de s'authentifier à l'aide des informations d'authentification reçues lors de l'inscription préalable ;
7) Le service Tiers **réalise et stocke le lien entre l'identifiant fourni par l'utilisateur et celui transmis par l'ENT** (« mapping » d'identités) ;
8) L'utilisateur accède **de façon nominative** au service Tiers.

Cas de la connexion nominale

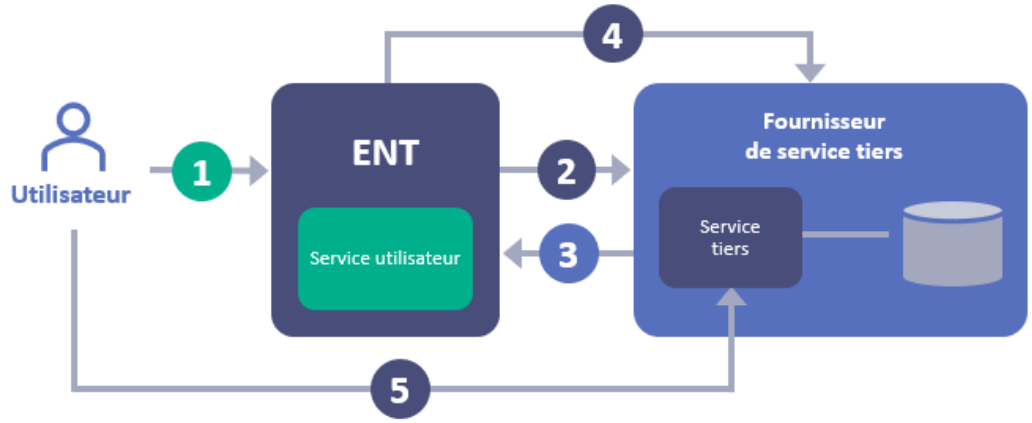

Figure 12 : Cinématique fonctionnelle pour les services de catégorie 4 (cas de la connexion nominale)

Comme illustré Figure 12, la cinématique d'accès à un service de la catégorie 4 est la suivante, dans le cas de la connexion nominale :

1) L'utilisateur s'authentifie auprès de son ENT ou auprès d'un fournisseur d'identité externe à l'aide de son login et de son mot de passe ;
2) L'utilisateur demande l'accès au service via un lien fourni par l'ENT ;
3) Le service Tiers demande à la solution ENT la transmission d'informations sur l'accédant ;
4) La solution ENT transmet un identifiant unique pour chaque utilisateur au service Tiers qui servira de clé de jointure (par exemple, le code projet ENT et un identifiant utilisateur non associé à une identité) ;
5) L'identifiant transmis par l'ENT est reconnu par le service Tiers, l'utilisateur accède au service sans s'authentifier à nouveau.

2.5.2.4.3. Données transmises

Les règles concernant les données transmises sont décrites dans les principes AAS-9 à AAS-12 (Cf. chapitre 2.6)

2.5.2.5. Services de catégorie 5

Rappel : l'accès au service s'effectue sur la base d'informations fournies par l'utilisateur lors de la première connexion au service Tiers via l'ENT (formulaire en ligne…).

Lors des connexions suivantes, l'accédant sera reconnu par le service Tiers sur la base d'informations utilisateur transmises par l'ENT (fonctionnement identique à la catégorie 4 : mapping d'identités).

2.5.2.5.1. Inscription d'un utilisateur

Pour les services Tiers appartenant à la catégorie 5, l'inscription s'effectue dynamiquement lors de la « première connexion » de l'utilisateur au service via l'ENT (première connexion ou réabonnement, nouvelle année scolaire…). À la différence de la catégorie 4, le processus d'inscription au service Tiers est corrélé à la connexion à un ENT.

Le cas particulier de la première connexion est donc décrit ci-après de façon distincte de la connexion nominale.

En conséquence, il est important pour les porteurs de projet et les responsables de traitement de s'assurer que les données définies dans le cadre de la convention de service comme pouvant être transmises via l'ENT, correspondent bien aux finalités du service Tiers. De plus, les utilisateurs doivent être acteurs dans la validation des données transmises qui les concernent.

2.5.2.5.2. Cinématique fonctionnelle

Cas de la première connexion

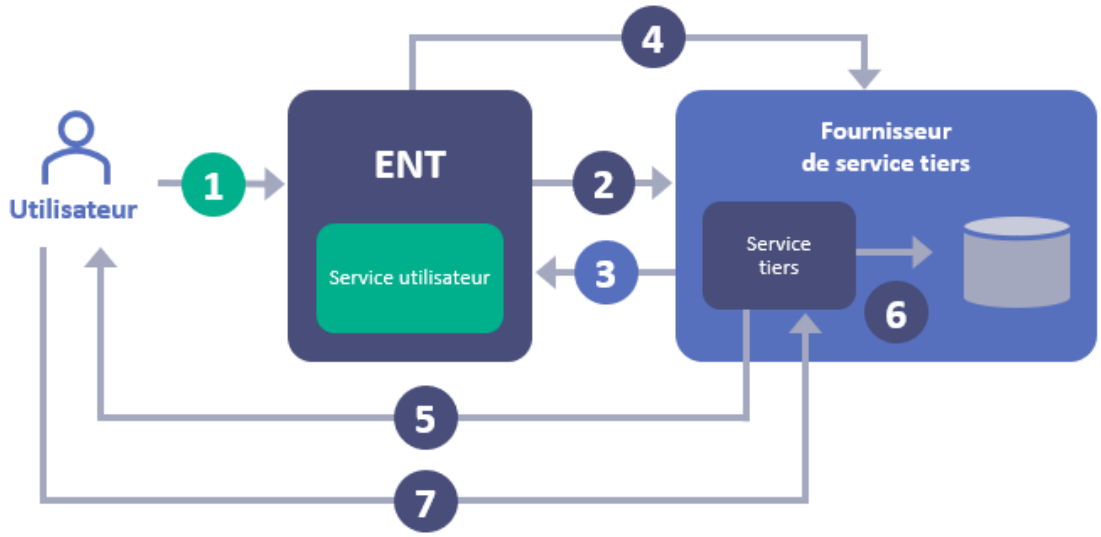

Figure 13 : Cinématique fonctionnelle pour les services de catégorie 5 (cas de la première connexion)

Comme le représente la Figure 13, la cinématique d'accès à un service de la catégorie 5 est la suivante pour la première connexion :

1) L'utilisateur s'authentifie auprès de son ENT ou auprès d'un fournisseur d'identité externe à l'aide de son login et de son mot de passe ;
2) L'utilisateur demande l'accès au service via un lien fourni par l'ENT ;
3) Le service Tiers demande à la solution ENT la transmission d'informations sur l'accédant ;
4) La solution ENT transmet un identifiant unique pour chaque utilisateur au service Tiers qui servira de clé de jointure (par exemple, le code projet ENT et un identifiant utilisateur non associé à une identité) ;

5) À la première connexion, l'utilisateur n'est pas reconnu par le service applicatif Tiers ; le service Tiers **demande alors à l'utilisateur de remplir un formulaire d'inscription** ;
6) Le service Tiers **stocke les informations transmises par l'utilisateur** ;
7) L'utilisateur accède de **façon nominative** au service Tiers.

Cas de la connexion nominale

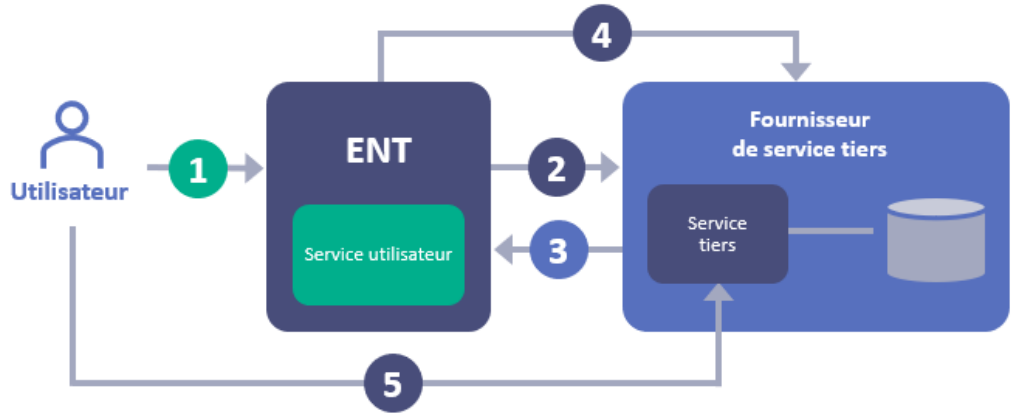

Figure 14 : Cinématique fonctionnelle pour les services de catégorie 5 (cas de la connexion nominale)

Comme le représente la Figure 14, la cinématique d'accès à un service de la catégorie 5 est la suivante, dans le cas d'une connexion nominale :

1) L'utilisateur s'authentifie à son ENT ou auprès d'un fournisseur d'identité externe via son login et son mot de passe ;
2) L'utilisateur demande l'accès au service via un lien fourni par l'ENT ;
3) Le service Tiers demande à la solution ENT la transmission d'informations sur l'accédant ;
4) La solution ENT transmet **un identifiant unique pour chaque utilisateur au service Tiers qui servira de clé de jointure** (par exemple, le code projet ENT et un identifiant utilisateur non associé à une identité) ;
5) L'identifiant fourni par la solution ENT est reconnu par le service, l'utilisateur accède au service **sans s'authentifier à nouveau**.

2.5.2.5.3. Données transmises

Les règles concernant les données transmises sont décrites dans les principes AAS-13 à AAS-17 (Cf. chapitre 2.6)

2.5.3. Conventions de service

Lorsque les acteurs du projet ENT (académie-collectivités, ou écoles / établissements scolaires) souhaitent interfacer l'ENT avec un service Tiers, une convention de service est élaborée entre les parties concernées, comme avait pu le préconiser la CNIL (délibération n°2006 – 104 du 27 avril 2007 relative aux ENT), afin que les rôles respectifs au sein de ces projets, leurs engagements et le traitement des données à caractère personnel des utilisateurs soient précisément définis.

Les points à traiter de ladite convention sont détaillés au chapitre 4 « Aspects juridiques » du présent document.

2.6. Récapitulatif des principes

- AAS-1 : La solution ENT ne transmet pas d'informations d'identité sur l'utilisateur à un service Tiers de catégorie 1.
- AAS-2 : Les données éventuellement transmises par la solution ENT afin d'assurer l'authentification et le contrôle d'accès pour des services de catégorie 2 sont :
  - L'identifiant du projet ENT (code projet ENT) à partir duquel le service Tiers est appelé (cf. Annexe 6 « Nomenclatures », chapitre 2) ;
  - L'identifiant de l'établissement (code UAI) à partir duquel le service Tiers est appelé (la solution ENT doit mettre en œuvre des traitements qui permettent d'identifier l'établissement auquel l'utilisateur accède dans l'ENT) ;
  - Le profil de l'accédant, non associé à une identité (cf. Annexe 6 « Nomenclatures », chapitre 7).
- AAS-3 : De plus d'autres attributs non associés à une identité sont transmis uniquement s'ils sont indispensables au fonctionnement du service Tiers de catégorie 2. Ces attributs sont décrits dans le Tableau 2 de l'Annexe 6 « Nomenclatures », au chapitre 4.1, et les définitions associées à ces attributs sont disponibles dans les annexes de l'ensemble annuaire.
- AAS-4 : Toute autre donnée n'est pas transmise dans le cadre d'un service de catégorie 2.
- AAS-5 : Les données éventuellement transmises afin d'assurer l'authentification et le contrôle d'accès à un service de catégorie 3 sont :
  - Un identifiant unique par utilisateur mais qui ne permette pas d'être associé à l'identité de l'accédant ;
  - L'identifiant du projet ENT (code projet ENT) à partir duquel le service Tiers est appelé (cf. Annexe 6 « Nomenclatures », chapitre 2) ;
  - L'identifiant de l'établissement (code UAI) à partir duquel le service Tiers est appelé ;

    - Le profil de l'accédant non associé à une identité (cf. Annexe 6 « Nomenclatures », chapitre 7).
- AAS-6 : De plus d'autres attributs non associés à une identité sont transmis uniquement s'ils sont indispensables au fonctionnement du service Tiers de catégorie 3. Ces attributs sont donnés dans le Tableau 2 de l'Annexe 6 « Nomenclatures », au chapitre 4.1, et les définitions associées à ces attributs sont disponibles dans les annexes de l'ensemble annuaire.
- AAS-7 : Toute autre donnée dans le cadre d'un service de catégorie 3 n'est pas transmise.
- AAS-8 : Des traitements sont réalisés par les solutions ENT afin de ne transmettre que les données relatives à l'établissement à partir duquel le service Tiers de catégorie 3, est appelé.
- AAS-9 : Lors de l'inscription préalable hors ENT, le service Tiers de catégorie 4 demande le cas échéant, à l'utilisateur des attributs afin de réaliser, par la suite, l'authentification, le contrôle d'accès ou la personnalisation.
- AAS-10 : Le service Tiers de catégorie 4 fait mention des conditions générales d'accès au service dans le respect des conditions définies dans le registre des traitements pour le traitement en question.
- AAS-11 : Les données éventuellement transmises par la solution ENT afin d'assurer l'authentification et le contrôle d'accès d'un service de catégorie 4 sont :
    - Un identifiant unique par utilisateur mais qui ne permette pas d'être associé à l'identité de l'accédant ;
    - L'identifiant du projet ENT (code projet ENT) à partir duquel le service Tiers est appelé (cf. Annexe 6 « Nomenclatures », chapitre 2) ;
    - L'identifiant de l'établissement (code UAI) à partir duquel le service Tiers est appelé ;
- AAS-12 : Toute autre donnée dans le cadre d'un service de catégorie 4 n'est pas transmise.
- AAS-13 : Les informations d'identité qui peuvent être demandées à l'utilisateur lors de la première connexion à un service de catégorie 5 sont déclarées préalablement dans la convention de service.
- AAS-14 : Les informations d'identité ne sont pas transmises au service Tiers de catégorie 5 de façon automatique par l'ENT : l'ENT présente à l'utilisateur la liste complète des informations d'identité demandées par le service Tiers et demande à l'utilisateur son consentement.
- AAS-15 : L'utilisateur a le choix de transmettre ou non ses informations d'identité à un service de catégorie 5.
- AAS-16 : Les informations d'identité sont demandées au détail et dans la limite du nécessaire par rapport à la finalité du service Tiers de catégorie 5 (authentification, contrôle d'accès, personnalisation, suivi de l'utilisateur).
- AAS-17 : Toutes les informations transmises lors de la première connexion à un service de catégorie 5 sont fournies sur la base du volontariat de l'accédant. À cette occasion, les conditions générales d'accès au service seront explicitement précisées.

- AAS-18 : En cas de mise en œuvre d'une délégation d'authentification à un fournisseur d'identité externe, le portail de l'ENT est le point d'accès privilégié aux différents services de l'ENT.
- AAS-19 : Des liens sont prévus entre l'ENT et les services externes afin de faciliter les usages.
- AAS-20 : Les attributs caractérisant les utilisateurs et nécessaires au contrôle des accès suivent un nommage et une sémantique communs au sein de la fédération.
- AAS-21 : Les moyens d'authentification partagés sont définis de manière commune dans toute la fédération.

3. Aspects juridiques

3.1. Préambule

Les aspects juridiques de l'annexe opérationnelle du SDET sont destinés à éclairer les porteurs de projets, les autorités académiques, les équipes d'accompagnement (personnels des DANE, des DSDEN, des circonscriptions, référents numériques) sur le cadre juridique relatif à la mise en œuvre et à l'exploitation d'un projet ENT.

Ce document est aussi l'occasion de rappeler les règles relatives à l'utilisation d'un ENT et s'adresse donc également aux responsables de traitement (chefs d'établissement, IA-DASEN, le cas échéant collectivités territoriales) et aux utilisateurs.

Il est destiné à éclairer le lecteur dans sa compréhension des enjeux juridiques du cadre de confiance d'un projet ENT et d'un usage responsable.

Les présents chapitres ne se substituent ni au Code de l'éducation, ni aux dispositions légales et réglementaires relatives aux ENT, et plus généralement aux outils et services du numérique éducatif.

Ils ne se substituent pas non plus aux dispositions légales et réglementaires relatives à la protection des données à caractère personnel.

Ils peuvent également être amenés à compléter les contrats ou les marchés conclus pour le déploiement et la maintenance d'un projet ENT ainsi que les conditions d'utilisation d'un ENT lorsque la présente annexe est intégrée aux documents contractuels les constituant.

Les éléments de ce chapitre sont par ailleurs complétés par le kit de conventionnement informatique et libertés, à disposition sur Éduscol, qui est dédié au respect des exigences contractuelles issues de la réglementation Informatique et Libertés et qui a vocation à proposer des outils et modèles tendant à faciliter la contractualisation auquel il leur appartient de se conformer au titre du RGPD à l'occasion du déploiement d'un ENT (ci-après le « Kit de conventionnement »). Ce kit de conventionnement fait partie intégrante du SDET en tant que document d'accompagnement.

3.2. Le cadre juridique

3.2.1. Le cadre juridique de l'ENT est issu d'une variété de textes législatifs et règlementaires

L'ENT est l'une des composantes sur lesquelles s'appuie le service public du numérique éducatif. L'article L.131-2 alinéa 2 du Code de l'éducation prévoit que :

> *« Dans le cadre du service public de l'enseignement et afin de contribuer à ses missions, un service public du numérique éducatif et de l'enseignement à distance est organisé pour, notamment :*
>
> *1° Mettre à disposition des écoles et des établissements scolaires une offre diversifiée de services numériques permettant de prolonger l'offre des enseignements qui y sont dispensés, d'enrichir les modalités d'enseignement et de faciliter la mise en œuvre d'une aide personnalisée à tous les élèves ;*
>
> *2° Proposer aux enseignants une offre diversifiée de ressources pédagogiques, des contenus et des services contribuant à leur formation ainsi que des outils de suivi de leurs élèves et de communication avec les familles ;*
>
> *3° Assurer l'instruction des enfants qui ne peuvent être scolarisés dans une école ou dans un établissement scolaire, notamment ceux à besoins éducatifs particuliers. Des supports numériques adaptés peuvent être fournis en fonction des besoins spécifiques de l'élève ;*
>
> *4° Contribuer au développement de projets innovants et à des expérimentations pédagogiques favorisant les usages du numérique à l'école et la coopération.*
>
> *5° Mettre à la disposition des familles assurant l'instruction obligatoire conformément au premier alinéa du présent article ainsi que de leurs circonscriptions ou établissements de rattachement, dans le respect des conditions fixées à l'article L. 131-5 :*
>
> > *a) Une offre numérique minimale assurant pour chaque enfant le partage des valeurs de la République et l'exercice de la citoyenneté, tels que prévus à l'article L. 111-1 ;*
> >
> > *b) Une offre diversifiée et adaptée pour les parents et les accompagnants des enfants instruits en famille ;*
> >
> > *c) Des outils adaptés et innovants de suivi, de communication, d'échange et de retour d'expérience avec les familles assurant l'instruction obligatoire.*
>
> *Dans le cadre de ce service public, la détermination du choix des ressources utilisées tient compte de l'offre de logiciels libres et de documents au format ouvert, si elle existe.*
> *»*

- Il s'agit d'un outil au service de la pédagogie. À ce titre, il se voit donc appliquer les dispositions du Code de l'éducation pour les dispositions qui lui sont applicables.
- L'ENT permet d'effectuer des démarches ou des formalités administratives, des échanges et collaborations entre écoles et établissements d'un même ENT ou d'ENT différents, ainsi que l'accès à des services Tiers en dehors du périmètre de responsabilité de l'ENT.
- L'ENT est aussi un espace de travail pour l'ensemble de la communauté éducative tel que mentionné dans la définition même des ENT qui s'appuie sur l'article L.111-3 du Code de l'éducation[6].

  À ce titre, pour les enseignants, l'ENT se verra appliquer les règles relatives aux droits et obligations des agents de la fonction publique et les règles d'organisation professionnelle qui y sont attachées.

  Concernant les élèves, la notion de travail renvoie au caractère éducatif et pédagogique de cet espace.

  À ce titre, les usages de l'ENT devront être conformes à sa destination et remplir les objectifs d'enseignement et d'échanges entre les membres de la communauté éducative.
- L'ENT est également un espace d'échanges de documentations et d'informations administratives relatives à la vie scolaire, aux enseignements et au fonctionnement de l'école ou de l'établissement.

  En tout état de cause, en tant qu'espace de travail, l'ENT se verra appliquer l'ensemble des règles relatives à la régulation des contenus et au droit de la propriété intellectuelle.
- L'ENT a une fonction dédiée. Etant, par nature, un ensemble intégré de services et contenus numériques, son développement, son déploiement et son utilisation sont régis par les règlementations en droit du numérique et des nouvelles technologies incluant le droit de l'internet ou des communications électroniques.
- Enfin, l'ENT, parce qu'il permet la collecte et le traitement de données à caractère personnel, doit se conformer aux dispositions légales et réglementaires relatives à la protection des données à caractère personnel (Cf. sur ce point infra au chapitre 4.5).

3.2.2. À retenir

L'ensemble des parties prenantes au projet ENT, porteurs de projet, autorités académiques, équipes d'accompagnement et utilisateurs, respecte les dispositions législatives et réglementaires (code de l'éduction, droit des marchés publics et des contrats, droit de la responsabilité, droit de l'internet, droit de la propriété intellectuelle, droit de la protection des données personnelles…).

[6] Article L.111-3 du Code de l'éducation : « *Dans chaque école, collège ou lycée, la communauté éducative rassemble les élèves et tous ceux qui, dans l'établissement scolaire ou en relation avec lui, participent à l'accomplissement de ses missions. Elle réunit les personnels des écoles et établissements, les parents d'élèves, les collectivités territoriales, les associations éducatives complémentaires de l'enseignement public ainsi que les acteurs institutionnels, économiques et sociaux, associés au service public de l'éducation* »

3.3. ENT et contractualisation

Différents niveaux de relations contractuelles doivent être envisagés.

3.3.1. Premier niveau : une convention de partenariat pour le portage du projet ENT

Les collectivités territoriales (ou groupement de collectivités territoriales) concernées, les autorités académiques, notamment pour le compte des écoles, et, le cas échéant, les établissements, signent une convention de partenariat ayant pour objet de définir le portage du projet et les rôles et responsabilités respectifs de ses différentes parties prenantes, relatifs à la promotion, l'accompagnement, la formation et l'assistance pour la mise en œuvre de l'ENT, la fourniture, au bénéfice des responsables de traitements, des données à caractère personnel nécessaires ainsi qu'un cadre de gouvernance et de pilotage.

La maîtrise d'ouvrage sera représentée généralement par les collectivités territoriales en partenariat avec les académies (cf. Chapitre « Objectifs, positionnement et organisation » du document principal).

Il est recommandé de conclure une convention de partenariat entre porteurs de projet que sont les collectivités territoriales ou groupements de collectivités et les académies notamment.

Le ou les prestataires chargés de la fourniture et de la mise en œuvre des solutions ENT sont sélectionnés par les parties à la convention de partenariat et ne sont pas partie à cette dernière. Afin que les collectivités territoriales le souhaitant puissent rejoindre une convention de partenariat, un mécanisme d'adhésion à ladite convention, par avenant, peut être envisagé.

En tout état de cause, la convention de partenariat doit être adaptée pour tenir compte de la réalité opérationnelle de chaque projet. Elle peut concerner par exemple d'autres structures que les établissements scolaires du premier et/ou du second degré.

Dans le cas particulier de l'extraction de données des annuaires ENT pour alimenter en données à caractère personnel les solutions de gestion des équipements fixes et mobiles et de gestion de classe conformes aux cadres de référence CARINE et CARMO, une convention de partenariat entre l'État et les collectivités territoriales concernées s'impose. Cette convention définit les modalités et conditions d'exploitation des données et en rappelle notamment les finalités. Cette extraction peut être opérée uniquement si le traitement est inscrit dans le registre du responsable de traitement et permet une extraction pour une telle finalité.

3.3.2. Deuxième niveau : une convention spécifique de sécurisation des traitements de données à caractère personnel (Accord de responsabilité du traitement)

Dès lors que les différentes parties à la convention de partenariat participent aux décisions stratégiques du projet et sont ainsi impliquées dans la détermination des finalités et des moyens des traitements de données à caractère personnel associés, elles recouvrent la qualité de responsable de traitement au sens de l'article 4 du RGPD.

Par suite et conformément aux dispositions de l'article 26 du RGPD, une convention de responsabilité de traitement conjointe doit impérativement être formalisée entre ces différentes entités.

Lorsque la responsabilité conjointe est également partagée avec les établissements d'enseignement, dès lors que ceux-ci disposent de la personnalité morale et qu'ils exercent un rôle actif sur ce traitement, ces établissements, bien que n'étant pas partie à la convention de partenariat, seront partie à la convention de responsabilité conjointe.

En effet, si les chefs d'établissements assument une part de responsabilité de traitement, dès lors qu'il leur appartient, notamment, de déterminer les modules de l'ENT dont ils entendent se doter, ils ne sont pas systématiquement signataires des conventions de partenariat.

C'est pourquoi et par souci de lisibilité, il demeure, à ce jour, plus aisé de formaliser une convention de responsabilité de traitement conjointe se référant à la convention de partenariat mais lui étant pour autant distincte.

Si une grande latitude est consentie aux parties dans la formalisation de ce type de convention, laquelle se doit de clarifier les responsabilités assumées par chacune des parties à l'égard des traitements en cause, des modèles types de convention sont néanmoins mis à leur disposition au sein du Kit de conventionnement.

3.3.3. Troisième niveau : convention(s) encadrant la réalisation, l'acquisition et l'exploitation d'une solution ENT

3.3.3.1. Convention pour la réalisation et acquisition

Aux fins de réalisation de l'ENT, un cahier des charges fonctionnel et technique est rédigé en vue de la sélection d'un prestataire pour la mise en œuvre et le déploiement de la solution ENT.

L'acquisition de la solution ENT suit les règles de la commande publique. La sélection du prestataire fournisseur de la solution ENT, la réalisation de la solution et sa mise en œuvre se conforment aux dispositions légales relatives aux marchés publics.

Les éditeurs, intégrateurs, exploitants ENT assurent la maîtrise d'œuvre, définie dans le marché public de la maîtrise d'ouvrage ou, à défaut, dans un contrat de prestations.

Quels que soient la nature et le choix du type de solution ENT, des clauses standards doivent être prévues : recette, maintenance, propriété intellectuelle, garanties, sécurité, responsabilité, qualité de service, réversibilité et portabilité des données, accès aux codes sources, etc.

La clause dédiée à la propriété intellectuelle peut différer selon qu'il est opté pour une solution standard (mise à disposition en mode SaaS ou concession d'une licence non exclusive) ou une solution développée spécifiquement dans le cadre du projet ENT à partir du cahier des charges fonctionnel et technique (et pour laquelle le porteur du projet peut souhaiter se réserver la propriété exclusive en prévoyant une clause de cession des droits de propriété intellectuelle exclusive).

Une clause adaptée doit prévoir et faciliter la réversibilité des projets ENT et ainsi préciser les exigences en cas de renouvellement/changement du marché et/ou du prestataire au cours du marché. Il doit être apporté un soin particulier, par le porteur de projet dans son cahier des charges, à la rédaction de cette clause afin de permettre la continuité du projet ENT.

Une clause de sous-traitance conforme aux exigences de l'article 28 du RGPD doit encore impérativement être intégrée à ce type de contrat. Un modèle de clause de sous-traitance est proposé dans le Kit de conventionnement. Il est à cet effet également recommandé, de solliciter, dans les documents de la candidature liée à la consultation en cause, une politique de protection des données à caractère personnel pour être en mesure de vérifier les garanties de sécurité desdits candidats. La portabilité de données personnelles des utilisateurs entre ENT doit permettre de faciliter la reprise de données en cas de réversibilité et la transition entre solutions ENT différentes.

Une clause d'accès aux codes sources doit être prévue pour des cas spécifiques et limités de défaillance du fournisseur de la solution ENT et des services associés (maintenance, support, formation…).

3.3.3.2. Convention pour l'hébergement

L'hébergement d'une solution ENT peut se faire par infogérance :

- Auprès d'une Entreprise de Services du Numérique (ESN) ;
- Ou auprès d'un service informatique de la collectivité territoriale ou de l'académie ;
- Ou auprès d'une société proposant une solution ENT en mode SaaS[7].

Dans l'hypothèse de l'infogérance, plusieurs acteurs seront amenés à intervenir. Les relations avec chaque professionnel devront être contractuellement encadrées et préciser les règles de sécurité qui leur sont applicables dans le cadre de l'hébergement de l'ENT et des prestations associées à cet hébergement.

La fourniture des prestations d'hébergement suit les règles de la commande publique. La sélection du prestataire hébergeur, et la fourniture de la prestation d'hébergement doivent se conformer aux dispositions légales relatives aux marchés publics.

Ce document contractuel devra impérativement contenir une clause de sous-traitance conforme aux exigences de l'article 28 du RGPD. Un modèle de clause de sous-traitance est proposé dans le Kit de conventionnement.

[7] SaaS : acronyme pour Software as a Service. Le mode Saas est un mode d'utilisation d'une solution logicielle qui se fait en utilisant l'application à distance qui est hébergée par l'éditeur.

L'hébergeur s'engage à héberger les données dans un pays membre de l'Union européenne, ou avec l'autorisation expresse du responsable de traitement, dans des pays qui assurent un niveau de protection suffisant de la vie privée et des libertés et droits fondamentaux des personnes à l'égard du traitement dont ces données font l'objet ou peuvent faire l'objet. En cas de transferts de données personnelles vers des pays hors Union européenne, le prestataire devra justifier de l'adoption d'un ou plusieurs outils reconnus par le RGPD pour permettre aux acteurs d'apporter un niveau de protection suffisant (tels que notamment les règles internes d'entreprise ou BCR, les clauses *contractuelles* types ou CCT), et, le cas échéant, de mesures qui complètent ces outils destinés à garantir le respect du niveau de protection des données à caractère personnel de l'UE[8].

Élaboré en 2016, et mis à jour en mars 2022, l'ANSSI a publié la version 3.2 du référentiel SecNumCloud[9], référentiel d'exigences applicables aux prestataires de services cloud. Ce référentiel permet ainsi à tout porteur de projet ENT de valider la qualification du prestataire de services qui gérera l'hébergement cloud.

Ce référentiel est conforme aux exigences européennes relatives à la protection des données personnelles et aux suites de l'arrêt « Schrems II »[10] de la Cour de justice de l'Union européenne rendu le 16 juillet 2020 qui a rappelé l'exigence de garantir une protection équivalente à celle offerte par le RGPD lorsque des données personnelles de citoyens européens sont transférées hors de l'Union européenne.

3.3.3.3. ENT et services Tiers

Les services natifs et les applications métier intégrées à l'ENT entrent dans le cadre de confiance tel que créé par le SDET. L'accès aux services Tiers (tels que définis au chapitre 2.6 de la présente annexe) est une finalité du traitement de données à caractère personnel mis en œuvre dans le cadre d'un ENT. Elle devra être visée dans le registre des traitements du responsable de traitement et être portée à la connaissance des personnes concernées[11].

Ces services peuvent nécessiter un cadre juridique particulier lorsque des données à caractère personnel sont transmises à des tiers ou stockées en dehors du cadre de confiance (cf. chapitre « Positionnement : un cadre de confiance entre les parties prenantes de l'ENT » du document principal du SDET pour plus de détails).

---

[8] CEPD, 18 juin 2021, *Recommandations 01/2020 sur les mesures qui complètent les instruments de transfert destinés à garantir le respect du niveau de protection des données à caractère personnel de l'UE*

[9] Référentiel SecNumCloud : https://www.ssi.gouv.fr/actualite/lanssi-actualise-le-referentiel-secnumcloud/

[10] Arrêt Schrems II : https://www.cnil.fr/fr/invalidation-du-privacy-shield-les-suites-de-larret-de-la-cjue

[11] Arrêté du 30 novembre 2006 portant création, au sein du ministère de l'éducation nationale, de l'enseignement supérieur et de la recherche, d'un traitement de données à caractère personnel relatif aux espaces numériques de travail (ENT) modifié par l'arrêté du 13 octobre 2017, article 1.

Le responsable de traitement de l'ENT ne doit pas donner accès aux utilisateurs vers les services Tiers si ces derniers ne respectent pas le SDET. Le responsable de traitement doit procéder aux vérifications nécessaires.

Les destinataires devront figurer dans le registre des traitements du responsable de traitement ainsi que dans l'information portée à la connaissance des personnes concernées conformément au RGPD.

L'interfaçage entre l'ENT et des services Tiers implique dès lors la signature d'une convention de service avec les fournisseurs de services ou une adhésion au GAR.

3.3.3.3.1. Convention de service

Concernant l'interopérabilité de la solution ENT avec des services Tiers, une convention de service doit être élaborée entre les porteurs de projets ENT et les fournisseurs de services Tiers concernés ainsi qu'avec les responsables de traitement dans le cas de transmission de données à caractère personnel (i.e. le DASEN dans le premier degré et du chef d'établissement dans le second degré) (ci-avant et ci-après la « convention de service »).

Cette convention doit permettre de préciser leurs rôles respectifs, leurs engagements et les modalités de traitement des données à caractère personnel des utilisateurs.

En conséquence, elle doit contenir un certain nombre de clauses fin de préciser les éléments suivants :

- Identification des parties concernées, par exemple :
  - Le responsable de traitement de l'ENT (chef d'établissement, IA-DASEN), dans le cas de transmission de données à caractère personnel ;
  - Le(s) responsable(s) de la mise en œuvre du projet ENT (collectivités, services académiques) ;
  - Le responsable du service Tiers ;

- Rôle de chacune des parties concernées :
  - Le responsable de traitement ;
  - Le fournisseur d'identité ;
  - Le fournisseur de service.

- L'organisation entre les différentes parties, en particulier :
  - Les moyens mis en œuvre pour assurer la coordination entre les différentes parties ;
  - Les conditions d'adhésion et de retrait du responsable de la mise en œuvre du projet ENT ;
  - Les conditions d'adhésion et de retrait du responsable du service Tiers ;

  - Les relations entre membres : définition des relations bilatérales acceptées entre un fournisseur de service et un fournisseur d'identité ;
  - La définition des documents de référence (dont les documents d'architecture technique).

- Les engagements respectifs des différents acteurs
  - Les responsabilités communes ;
  - Les engagements des fournisseurs d'identité ;
  - Les engagements des fournisseurs de service ;
  - Les engagements des administrateurs de la solution ENT ;
  - La durée de l'accord et les conditions de rupture et de renouvellement.
- Les conditions et modalités d'accès / retrait au service Tiers : la convention de service prévoit notamment les conditions (qualité de service par exemple) et modalités d'accès et de retrait d'un utilisateur à un service Tiers, notamment, celle-ci mentionnera les éléments suivants :
  - L'accès / retrait d'un utilisateur de sa propre initiative (via l'ENT, via un formulaire en ligne à la première connexion…) ;
  - L'accès / retrait d'un utilisateur par un tiers (directeur d'école, chef d'établissement, administrateur de l'ENT…) ;
  - La durée de conservation, récupération et suppression des données à caractère personnel dont les données produites dans les services Tiers.

- Les données transmises.

  La convention de service stipule clairement les données nécessaires devant être transmises par l'ENT afin d'assurer l'authentification et le contrôle d'accès et indispensables au fonctionnement du service Tiers ainsi que les destinataires et la finalité du traitement de données à caractère personnel le cas échéant, en respectant les données autorisées selon la catégorie du services Tiers définies plus haut et les dispositions légales et réglementaires en vigueur.

  Les données transmises ne peuvent pas être utilisées à d'autres finalités de traitement que celles indispensables à la fourniture du service.

- La capacité à sous-traiter.

  La convention de service précise la capacité d'un des acteurs du projet à sous-traiter tout ou partie de ses activités. Le cas échéant, les conditions, devoirs et responsabilités relatifs à cette sous-traitance sont précisés dans la convention.

- Une clause réversibilité.

- Une clause de sous-traitance conforme aux exigences de l'article 28 du RGPD lorsque la convention de service identifie un sous-traitant au sens du RGPD (un modèle de clause de sous-traitance est proposé dans le Kit de conventionnement).

Il est précisé que la liste fournie ci-dessus n'est pas exhaustive. Elle identifie les éléments indispensables pour qu'un service Tiers puisse s'interfacer avec un ENT. Les parties concernées sont libres de faire apparaître aux termes de la convention tous les éléments complémentaires qui leur semblent importants de souligner dans le cadre du projet ENT, sous réserve que ces éléments respectent la législation en vigueur, et soient notamment conformes aux informations visées dans le registre des traitements pour le traitement en question.

3.3.3.3.2. Gestionnaire d'accès aux ressources (GAR)

La solution ENT pourra également s'interfacer avec d'autres services Tiers via le GAR permettant de garantir le cadre de confiance. La CNIL l'encourage et note que le dispositif s'inscrit dans l'esprit du RGPD[12]. En pratique le contrat d'adhésion au GAR des services Tiers comprend également une charte éthique.

Ainsi, dans un premier temps, les fournisseurs de services Tiers doivent s'engager en signant un contrat d'adhésion et respecter un référentiel technique et fonctionnel. Dans un second temps, la mise en œuvre du traitement de données à caractère personnel permet aux utilisateurs et partenaires de bénéficier des services du GAR et de transmettre aux fournisseurs de ressources adhérents uniquement les données identifiées en amont comme nécessaires[13].

La liste des acteurs ENT (éditeurs, intégrateurs ENT, projets ENT) et des fournisseurs de ressources adhérents au GAR est publiée sur le site du GAR[14].

3.3.4. Quatrième niveau : la contractualisation avec les utilisateurs

Préalablement à toute utilisation, les utilisateurs de l'ENT devront prendre connaissance et accepter des conditions générales d'utilisation rappelant les droits et les obligations des parties. Pour cela, il est renvoyé au chapitre 4.4 « Accès et conditions d'utilisation » ci-après.

[12] Délibération n°2017-253 du 21 septembre 2017 portant avis sur un projet d'arrêté relatif à la mise en œuvre par le ministère de l'éducation nationale d'un traitement de données à caractère personnel dénommé gestionnaire d'accès aux ressources (AV n°17000891).

[13] Arrêté du 18 décembre 2017 relatif à la mise en œuvre par le ministère de l'éducation nationale d'un traitement de données à caractère personnel dénommé « gestionnaire d'accès aux ressources » (GAR) (https://www.legifrance.gouv.fr/eli/arrete/2017/12/18/MENN1729109A/jo/texte/fr).

[14] Site du GAR (https://gar.education.fr).

3.3.5. À retenir

Pour la mise en œuvre d'un projet ENT, un ensemble contractuel destiné à délimiter le périmètre d'intervention des différents acteurs impliqués, leurs obligations et engagements et leurs responsabilités respectives, est rédigé.

3.4. Accès et conditions d'utilisation

Les conditions générales de fonctionnement, d'accès, et d'utilisation de l'ENT sont généralement fixées dans un document de référence dénommé « charte d'usage des services numériques ».

Ces règles sont de nature contractuelle. L'utilisateur doit les accepter lors de sa première connexion à l'ENT.

L'utilisateur de l'ENT doit respecter les règles qui lui sont ainsi fixées. À défaut il pourra être sanctionné de différentes manières (restriction d'usage, suppression de compte, sanction disciplinaire…).

La terminologie et la forme de la charte d'usage des services numériques ne sont pas figés, l'essentiel étant que :

- Ses conditions soient claires dans leur rédaction ;
- Ses conditions soient acceptées formellement par l'utilisateur lors de leur première connexion pour leur être opposables ;
- Ses modifications soient portées à la connaissance de l'utilisateur de manière claire et explicite (idéalement comme une étape obligatoire à l'occasion de la prochaine connexion à l'ENT).

La charte d'usage des services numériques vient ainsi compléter d'autres documents tels que le règlement intérieur des écoles et des établissements.

La charte d'usage des services numériques doit énoncer les différentes règles de droit s'appliquant à l'utilisation de l'ENT. Elle comprend de manière non exhaustive, le respect de la vie privée, du droit à l'image, de la propriété intellectuelle, de la protection des données, la responsabilité du directeur de publication dans les espaces partagés.

La charte d'usage des services numériques doit également inciter les usagers à respecter les conditions de sécurité entourant l'ENT et à ne commettre aucun acte illicite ou portant atteinte aux droits des tiers.

Cette charte d'usage des services numériques doit également rappeler les principes de l'Éducation nationale et notamment le principe de neutralité religieuse, politique et commerciale.

3.4.1. Droits des utilisateurs

La charte d'usage des services numériques rappelle les droits des utilisateurs et notamment :

- Les conditions dans lesquelles les utilisateurs ont le droit d'accéder à l'ENT en précisant les services de base et les services complémentaires auxquels les utilisateurs accèdent suivant leur catégorie ;
- La possibilité de stocker du contenu dans l'ENT ;
- Tous les droits relatifs à la protection de leurs données à caractère personnel ;
- Le droit au respect de la vie privée résiduelle ;
- Les conditions d'accès et d'échanges aux espaces de contributions personnelles, aux espaces, de stockage d'informations individuelles et aux espaces de commentaires et de publication.

3.4.2. Obligations des utilisateurs

La charte d'usage des services numériques rappelle également les obligations des utilisateurs parmi lesquelles :

- Le respect du principe de neutralité religieuse, politique et commerciale ;
- Le respect des droits des tiers ;
- L'interdiction de diffuser et d'accéder à des contenus illicites ;
- Le respect des finalités de l'ENT ;
- Le respect de l'intégrité technique des systèmes d'information.

3.4.3. Identification / authentification

La charte d'usage des services numériques souligne le caractère éminemment personnel du couple identifiant / mot de passe permettant d'accéder aux services de l'ENT.

Ce rappel permet d'introduire le principe suivant lequel toute utilisation du mot de passe est présumée effectuée au nom de l'utilisateur, de sorte que l'utilisateur demeurera seul responsable de l'utilisation de l'ENT qui sera faite sous son identifiant.

3.4.4. Responsabilité

Outre les éléments de responsabilité généraux, la charte d'usage des services numériques à destination des utilisateurs précise que l'utilisateur est responsable de l'utilisation de son espace individuel et des contributions qu'il publie et des informations qu'il échange sur les espaces de commentaires et de publication.

3.4.5. Obligation de protection des données personnelles

S'agissant de l'ENT, la charte d'usage des services numériques précise que le ou les responsable(s) du traitement met(tent) en œuvre un traitement de données à caractère personnel ainsi que les caractéristiques dudit traitement (finalités, base légale, catégorie de données collectées, conditions de collecte, destinataires, durée de conservation).

La charte d'usage des services numériques informe également l'utilisateur des droits dont il dispose concernant la protection de ses données à caractère personnel et précise les modalités d'exercice de ses droits (voir en ce sens l'article 4.5 Protection des données à caractère personnel ci-après).

3.4.6. À retenir

Pour la mise en œuvre d'un projet ENT impose, des conditions générales d'utilisation contenant les clauses relatives aux droits des utilisateurs, à leurs obligations, aux responsabilités attachées à l'utilisation de l'ENT ainsi qu'aux sanctions éventuelles sont rédigées.

Un processus d'acceptation de ces conditions générales d'utilisation (et de leurs modifications) est prévu en vue de s'assurer de leur opposabilité.

Ces conditions générales d'utilisation sont généralement fixées dans un document de référence dénommé « charte d'usage des services numériques ».

3.5. Protection des données à caractère personnel

3.5.1. Principes fondamentaux applicables au traitement des données à caractère personnel

Un ENT donne lieu à un traitement de données à caractère personnel. De fait, l'ENT s'inscrit nécessairement dans le cadre du respect du RGPD, entré en application le 25 mai 2018 et de la loi relative à l'Informatique, aux fichiers et libertés modifiée.

A cet effet, il convient impérativement de porter une forte attention à la conformité à cette réglementation, dans le déploiement comme dans la gestion ultérieure de ces ENT.

Pour ce faire, le premier réflexe demeure **celui d'associer à la réflexion les délégués à la protection des données de chaque collectivité, autorité académique et établissements impliqués**.

En synthèse ensuite, il importe de retenir :

- **La nécessité de garantir le respect des grands principes de la réglementation Informatique et Libertés définis à l'article 6 du RGPD** et ce dès la conception du projet. Ce faisant, notamment, seules les données absolument nécessaires à l'atteinte des finalités du traitement seront traitées (conformément au principe de minimisation) et pour une durée limitée (principe d'adéquation de la durée de conservation). Toutes les mesures élémentaires de sécurité recommandées par les autorités autorisées (CEPD, CNIL, ANSSI) seront encore déployées pour prévenir les risques d'altération des données, de perte ou d'accès non autorisé à ces dernières ;
- **La nécessité de garantir une contractualisation conforme entre les différents acteurs du traitement** (voir en ce sens le Kit du conventionnement) ;
- **La nécessité d'informer les personnes concernées** (soit toutes les personnes dont les données sont traitées) sur les conditions de traitement de leurs données. A cet effet, le cadre de référence est fixé par les dispositions des articles 13 et 14 du RGPD., il est, ainsi conseillé, d'intégrer directement sur les ENT, en pied de page des écrans d'accueil et de connexion, l'accès à une information de ce type

- En complément : MODELE D'INFORMATIONS RELATIVES AU TRAITEMENT DE DONNEES PERSONNELLES RELATIF A LA GESTION DE L'ESPACE NUMÉRIQUE DE TRAVAIL (à adapter par chaque académie ou collectivité, selon les caractéristiques du traitement) :

Cette page a pour objectif de vous informer :
Des engagements de la collectivité x et des autorités académiques en matière de protection des données à caractère personnel traitées dans le cadre de la gestion de cet ENT.

RESPONSABLES DE TRAITEMENT
La collectivité x, les autorités académiques et l'établissement x [*pour le second degré uniquement puisque dans le premier degré, les établissements ne disposent pas de la personnalité morale*] assument conjointement la responsabilité de traitement associée à la gestion de cet ENT.
Les grandes lignes de l'accord de responsabilité de traitement conjointe signé les parties sont disponibles ici [*intégrer un lien vers les grandes lignes*].

FINALITES DU TRAITEMENT
Le traitement des données a pour finalité la fourniture d'un service ENT à la communauté éducative de x, soit plus précisément :

- de saisir et de mettre à la disposition des élèves ou des personnes responsables des élèves, des étudiants, des enseignants, des personnels administratifs, des équipes d'accompagnement et plus généralement de tous les membres de la communauté éducative de l'enseignement du premier et du second degré, en fonction des habilitations de chaque usager, des contenus éducatifs et pédagogiques, des informations administratives, relatives à la vie scolaire, aux enseignements et au fonctionnement de l'école ou de l'établissement ainsi que de la documentation en ligne ;
- de permettre des échanges et des collaborations entre écoles et établissements d'un même ENT ainsi qu'avec des écoles et des établissements utilisant des ENT différents ;
- de réaliser des statistiques en vue de permettre la mesure des accès aux différents services proposés ;
- Le cas échéant, de permettre un accès à des services tiers.

BASE LEGALE :
Le traitement des données est fondé sur l'exécution d'une mission d'intérêt public au sens de l'article 6.1.e du règlement général (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 sur la protection des données (RGPD).

DESTINATAIRES DES DONNÉES
Les destinataires de vos données (liste non exhaustive) sont, dans la limite de leur besoin d'en connaître :
L'établissement scolaire,
…

Le ministère de l'Éducation nationale, de la Jeunesse (uniquement pour les données nécessaires à la mise en œuvre du GAR)
Ainsi que des sous-traitants au travers d'une contractualisation conforme aux attendus du RGPD gage de garanties fortes de sécurité pour les données personnelles traitées.

DURÉE DE CONSERVATION DES DONNÉES
Les données à caractère personnel traitées dans le cadre d'un compte ENT sont conservées, en base active, pour la durée de l'année scolaire ou, au besoin, pour la durée du cycle scolaire.
Les données de connexion (logs et adresses IP, traces des accès, consultations, créations et modifications de données) sont conservées pour une durée maximale de douze mois.
Enfin, les données sont supprimées de l'ENT dans un délai de trois mois dès lors que la personne concernée n'a plus vocation à détenir un compte.

DROIT DES PERSONNES
Toutes les personnes dont les données sont traitées disposent d'un droit d'information, d'accès, de rectification des données les concernant, ainsi que d'un droit d'opposition et d'un droit à la limitation du traitement. Vous pouvez exercer les droits d'accès, de rectification, de limitation et d'opposition que vous tenez des articles 15, 16, 18 et 21 du RGPD en suivant les indications suivantes.
Vous trouverez ci-après les cordonnées utiles pour exercer une telle demande de droit :
[*à préciser : en distinguant le cas échéant selon l'auteur de la demande lorsqu'il a été prévu dans les conventions de responsabilité de traitement conjointe que la réponse aux demandes de droit n'était pas centralisée mais répartie entre chaque responsable de traitement, selon leur origine (élève, enseignant, membre du personnel)]*
Dans le cadre de l'exercice de vos droits, vous devez justifier de votre identité par tout moyen. En cas de doute sur votre identité, les services chargés du droit d'accès et le délégué à la protection des données se réservent le droit de vous demander les informations supplémentaires qui leur apparaissent nécessaires, y compris la photocopie d'un titre d'identité portant votre signature (ce justificatif ne sera pas conservé).
Si vous estimez, même après avoir introduit une réclamation, que vos droits en matière de protection des données à caractère personnel ne sont pas respectés, vous avez la possibilité d'introduire une plainte auprès de la Commission nationale de l'informatique et des libertés (CNIL) à l'adresse suivante : 3 Place de Fontenoy – TSA 80715 – 75334 Paris Cedex 07.

- La nécessité de documenter la conformité de cette activité de traitement, via, *a minima*, une inscription au sein du registre des activités de traitement de chaque responsable de traitement et de chaque sous-traitant (conformément au cadre défini à l'article 30 du RGPD), voire la réalisation d'une analyse d'impact relative à la protection des données (AIPD) conformément aux dispositions de l'article 35 du RGPD.

Sur ces AIPD, il semble permis de retenir que leur réalisation s'impose essentiellement pour les ENT mutualisés à une échelle régionale. En effet, il est patent que la gestion des ENT ne figure pas dans la liste établie par la CNIL des traitements obligatoirement soumis à la réalisation d'une AIPD (issue de la délibération de la CNIL n°2018-3267). De sorte que la soumission à cette obligation doit être appréciée selon l'identification de 2 critères parmi une liste de 9 établis par le G29 au sein de ses lignes directrices adoptées le 4 octobre 2017 (WP 248 rév.01).

Or, si l'on s'en tient à cette liste, deux de ces critères semblent pouvoir être réunis : soit la vulnérabilité des personnes concernées (en l'occurrence des enfants), d'une part, et le fait qu'il s'agisse d'une collecte à large échelle, d'autre part. Reste que sur cette notion de « large échelle », le considérant 91 du RGPD évoque un niveau régional, national ou international. De sorte que ce critère sera essentiellement satisfait pour les ENT mutualisés à une échelle régionale.

Il appartient en tout état de cause, à chaque délégué à la protection des données d'apprécier de la nécessité ou non de réaliser ce type d'analyse de conformité approfondie.

Dès lors que l'inscription au sein du registre de cette activité de traitement constitue, en revanche, une obligation commune à l'ensemble des acteurs, il est proposé ci-après, à titre indicatif, un exemple type de fiche de registre afférent à la gestion d'un ENT :

Activité de traitement n°x.x à compléter – Gestion d'un ENT

Responsables de traitement	Collectivité(x) x Autorités académiques (Etablissements dans le 2nd degré)	**Date de création**	
Base juridique	6.1 e)	**Dernière mise à jour**	
Références juridiques	RGPD + LIL		
Finalités du traitement	• saisir et mettre à la disposition des élèves ou des personnes responsables des élèves, des étudiants, des enseignants, des personnels administratifs, des équipes d'accompagnement et plus généralement de tous les membres de la communauté éducative de l'enseignement du premier et du second degré, en fonction des habilitations de chaque usager, des contenus éducatifs et pédagogiques, des informations administratives, relatives à la vie scolaire, aux enseignements et au fonctionnement de l'école ou de l'établissement ainsi que de la documentation en ligne ; • de permettre des échanges et des collaborations entre écoles et établissements d'un même ENT ainsi qu'avec des écoles et des établissements utilisant des ENT différents ; • de réaliser des statistiques en vue de permettre la mesure des accès aux différents services proposés ; • de permettre un accès à des services tiers (le cas échéant)		
Catégories de personnes concernées	Elèves Responsables légaux des élèves Personnels enseignants et non enseignants		
Catégories de données collectées	**En ce qui concerne les élèves** : numéro d'identifiant national (INE), civilité, noms, prénoms , date de naissance et, le cas échéant, lieu de naissance, ville et pays de naissance dans l'hypothèse où l'INE n'est pas enregistré ou en cas de conflit d'INE, photographie et coordonnées personnelles, adresse postale, téléphones fixe et portable, adresse électronique, tout élément concernant sa vie scolaire sa scolarité, ses productions scolaires **En ce qui concerne les personnes responsables des élèves** : civilité, noms, prénoms, date de naissance, adresse postale, téléphones fixe et portable, adresse électronique **En ce qui concerne les personnels enseignants et non enseignants :** civilité, noms, prénoms, date de naissance, situation professionnelle, structure de rattachement, coordonnées professionnelles, informations administratives les concernant, toute information concernant la scolarité des élèves ou des étudiants dont ils ont la charge, productions pédagogiques et administratives		
Durée de conservation	Les données à caractère personnel traitées dans le cadre d'un compte ENT sont conservées, en base active, pour la durée de l'année scolaire ou, au besoin, pour la durée du cycle scolaire. Les données de connexion (logs et adresses IP, traces des accès, consultations, créations et modifications de données) sont conservées pour une durée maximale de douze mois. Enfin, les données sont supprimées de l'ENT dans un délai de trois mois dès lors que la personne concernée n'a plus vocation à détenir un compte.		
Catégorie de destinataires	Les destinataires de vos données sont, dans la limite de leur besoin d'en connaître : L'établissement scolaire, L'académie ou l'autorité académique concernée (à préciser) Le ministère de l'Éducation nationale, de la Jeunesse (uniquement pour les données nécessaires à la mise en œuvre du GAR) Ainsi que des sous-traitants au travers d'une contractualisation conforme aux attendus du RGPD gage de garanties de protection des données fortes.		
Transfert des données hors UE	Pas de transfert hors UE		

Mesures de sécurité	[*Selon les pratiques : développer ou renvoyer à un document synthétisant les mesures de sécurité mises en œuvre par l'organisme ou lister les principales mesures de sécurité techniques et organisationnelles mises en œuvre*]

3.5.2. À retenir

La mise en œuvre d'un projet ENT implique une prise en compte des impératifs du RGPD et de la loi relative à l'informatique, aux fichiers et aux libertés modifiée.

3.6. Identification / authentification

3.6.1. Identifiants

Classiquement, la sécurisation de l'accès à l'ENT repose sur la fourniture et l'utilisation d'un couple identifiant/mot de passe. L'identité de l'utilisateur est vérifiée lors de l'accès à l'ENT. Ces identifiants et mots de passe sont strictement personnels à l'utilisateur. Ils sont distribués aux utilisateurs par la personne désignée comme référente de l'établissement ou de l'école.

Tout accès à l'ENT via le détournement de ces identifiants et mots de passe sera considéré comme un accès frauduleux. Les identifiants communiqués à chaque utilisateur sont associés à des droits d'accès aux services de la solution ENT définis en fonction des profils applicatifs.

Chaque utilisateur est responsable de ses identifiants et mots de passe et s'interdit de les communiquer.

Les administrateurs de l'ENT ou les fournisseurs d'identité externes en cas de délégation d'identification et d'authentification en assurent la gestion technique.

3.6.2. Présomption

L'utilisation des identifiants et mots de passe personnels de l'utilisateur entraîne une présomption d'identification de l'utilisateur. L'identifiant étant personnellement attribué à un usager déterminé, les usagers sont seuls responsables de la préservation et de la confidentialité de leur identifiant et de leur mot de passe et doivent accepter le fait que toute utilisation de leur identifiant et de leur mot de passe dans le cadre des services de l'ENT constitue une preuve de leur identité sauf dénonciation préalable de fraude.

En cas d'utilisation des codes d'accès d'un tiers ou par un tiers, l'accès peut être qualifié de frauduleux, et il peut aussi constituer les infractions que sont l'usurpation d'identité ou une captation frauduleuse de données personnelles[15].

Dès lors, lorsqu'un utilisateur a accès accidentellement à un espace non autorisé de l'ENT, il lui incombe de prévenir sans délai le référent ENT pour éviter d'engager sa propre responsabilité.

La charte d'usage des services numériques doit prévoir que les identifiants doivent être modifiés à chaque demande et qu'ils doivent être modifiés régulièrement à une fréquence déterminée.

Pour des raisons de sécurité ou dans le cadre d'un usage frauduleux ou illicite d'un ENT, mais également dans le cadre de nécessités techniques ou de maintenance, il est possible pour le responsable de l'ENT d'utiliser les codes administrateurs pour accéder à tout ou partie de l'ENT.

La mise en place d'un projet ENT impose de :

- Déterminer les conditions relatives à la remise des identifiants, à leur modification et au niveau de sécurité qui les entoure ;
- Déterminer une procédure d'opposition à mettre en œuvre en cas d'utilisation frauduleuse d'identifiants par des tiers ;
- Informer les usagers, dans la charte d'usage des services numériques, de la procédure de gestion des identifiants et du fait qu'ils sont seuls responsables de leur utilisation ;
- Déterminer une procédure relative au contrôle par l'administrateur des identifiants et des mots de passe.

[15] Article 226-4-1 du Code pénal, issu de l'article 2 de la Loi 2011-267 du 14-3-2011 d'orientation et de programmation pour la performance de la sécurité intérieure dite Loppsi 2, dispose que : « *Le fait d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération, est puni d'un an d'emprisonnement et de 15.000 euros d'amende. Cette infraction est punie des mêmes peines lorsqu'elle est commise sur un réseau de communication au public en ligne* ».

3.6.3. Usurpation d'identité numérique

Le délit d'usurpation d'identité susvisé appartient à la catégorie des délits d'atteinte à la personnalité, et plus précisément d'atteinte à la vie privée. La Cour Européenne des Droits de l'Homme a adopté une interprétation extensive de la notion de vie privée permettant en principe d'inclure les activités professionnelles ou commerciales[16].

Lorsqu'il est commis par une personne morale, celle-ci est passible d'une amende dont le montant est quintuplé par rapport à celui encouru par les personnes physiques, soit 75 000 euros[17].

Ce délit, pour son volet numérique, comprend un élément matériel qui est caractérisé par le fait d'usurper l'identité d'un tiers « *[…] sur un réseau de communication au public en ligne […]* »[18].

Dans la mesure où l'ENT intègre une forte dominante identitaire (noms, pseudonymes, comptes, codes…), des usages détournés de ces éléments d'identité d'un utilisateur par un autre sont susceptibles de se produire et, sous réserve de l'interprétation qui sera faite par les juridictions, être qualifiés de délit d'usurpation d'identité numérique.

De tels agissements pourront assurément être considérés comme relevant de l'usurpation d'identité s'il est démontré la réalité de l'usurpation mais également l'élément intentionnel visant à nuire à l'utilisateur légitime. Cet élément sera constitué dès lors que l'usurpation de l'identité d'un tiers ou que l'usage de données de toute nature permettant d'identifier ce tiers est commise *« […] en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération […] »*.

[16] CEDH, 16-2-2000, Amann c/ Suisse, § 65, définition issue de CEDH, 16-12-1992, Nemietz c/ Allemagne, série A n°251-B, p.33-34, § 29

[17] Article 131-38 du Code pénal

[18] Cf. Article 226-4-1 du Code pénal cité *supra*.

3.6.4. À retenir

Pour la mise en place d'un projet ENT, il convient de :

- Déterminer les conditions relatives à la remise des identifiants/mots de passe, à leur modification et au niveau de sécurité qui les entoure ;
- Déterminer une procédure d'opposition à mettre en œuvre en cas d'utilisation frauduleuse d'identifiants par des tiers ;
- Informer les utilisateurs, dans la charte d'usage des services numériques, de la procédure de gestion des identifiants/mots de passe et du fait qu'ils sont seuls responsables de leur utilisation ;
- Déterminer une procédure relative au contrôle par l'administrateur des identifiants/mots de passe.

Les données constitutives de l' « identité numérique », peuvent notamment recouvrir, sous réserve de l'interprétation qui sera faite par les juridictions de cette notion, les éléments suivants :

- Adresses de messagerie ;
- Profil numérique ;
- Traces numériques de toutes natures (données de trafic et de connexion) ;
- Personnages créés dans le monde virtuel (avatars) ;
- Pseudonymes ;
- Blogs personnels ainsi que les contenus de ces blogs ;
- Noms de domaine personnels ;
- Identifiants ;
- Mots de passe ;
- Données bancaires ou financières (numéro de carte bancaire, etc.) ;
- Données d'identification biométriques diverses telles que l'iris, la forme du visage ou de la main, la lecture électronique des empreintes digitales.

Pourraient être comprises dans la définition des données de toutes natures les adresses IP permettant d'identifier un système, et indirectement, le propriétaire de ce système.

3.7. Espaces d'échanges et de collaboration

L'ENT propose des espaces d'échanges et de collaboration sur lesquels les utilisateurs peuvent s'exprimer. Des espaces de travail collaboratifs sont par ailleurs mis en œuvre et favorisent les échanges entre les utilisateurs d'un ENT, mais aussi entre ceux des écoles, des établissements et des degrés. Différents outils concourent à cet échange de données entre les différents acteurs et ENT.

La charte d'usage des services numériques édicte la responsabilité de chacun, la référence au cadre de confiance, et indique aux utilisateurs lorsque ces espaces d'échanges et de collaboration sont publics et donc accessible par les autres utilisateurs. Pour ces espaces, la charte d'usage des services numériques rappelle aux utilisateurs qu'ils doivent, par conséquent, s'abstenir d'y publier :

- Des données à caractère privé, confidentiel ou personnel ;
- Des informations et/ou messages, commentaires et autres contenus malveillants, dénigrants, diffamatoires, injurieux, obscènes, pornographiques, violents, à caractère raciste, xénophobe, discriminatoire, volontairement trompeurs, illicites et/ou contraires à l'ordre public ou aux bonnes mœurs.

Ces espaces posent essentiellement la problématique de la responsabilité des contenus et des moyens de modérer les échanges entre utilisateurs en cas de propos abusifs.

La loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN) fait reposer sur l'éditeur du site internet la responsabilité de l'ensemble des contenus publiés par ses utilisateurs, alors que l'hébergeur du site internet bénéficie d'un régime de responsabilité atténuée. Le critère du « rôle actif » dans le contrôle des contenus diffusés sur les espaces de discussions et de commentaires permet de déterminer si l'éditeur du site internet a un rôle d'éditeur ou d'hébergeur des contenus publiés :

- S'il adopte un rôle actif (par exemple en contrôlant les contenus avant leur publication), il est alors qualifié d'éditeur et est responsable de ce qui est publié ;
- S'il ne contrôle pas ces contenus, il est qualifié d'hébergeur et n'est pas responsable de ce qui est publié ; il est dans cas tenu à simple obligation de supprimer promptement un contenu manifestement illicite qui lui est signalé.

L'ouverture ou la fermeture de tels espaces fait l'objet d'une décision et s'inscrit dans le cadre de ce qui est prévu aux termes de la charte d'usage des services numériques.

Les espaces d'échanges et de collaboration peuvent être administrés par une personne de l'établissement sous le contrôle du chef d'établissement ou par une personne de l'école sous le contrôle du directeur d'école ou de l'académie.

Chacun des espaces d'échanges et de collaboration peut disposer de conditions d'utilisation particulières qui devront être visées dans la charte d'usage des services numériques.

Dans tous les cas, en présence même d'un espace d'échanges et de collaboration, le responsable primaire reste celui qui publie un contenu. Ce dernier en assumera la responsabilité en cas de publication de contenus manifestement illicites. Néanmoins, en tout état de cause, l'espace collaboratif est par essence même, un espace collectif reposant sur une modération collective. À ce titre, il convient de se reporter au développement relatif à l'obligation d'alerte.

3.7.1. À retenir

Il est conseillé de mettre en place une modération des espaces d'échanges et de collaboration.

Il convient de traiter au sein de conditions particulières d'utilisation de l'espace, distinctes de la charte d'usage des services numériques, et qui doivent être expressément acceptées par l'utilisateur un ensemble de règles juridiques et notamment :

- La gestion des droits de propriété intellectuelle ;
- Le régime de responsabilité au regard de la diffusion et la protection de la création sur internet ainsi que les obligations en découlant ;
- Les obligations au regard de la réglementation sur les données à caractère personnel ;
- L'anticipation des risques d'atteintes au système de traitement automatisé de données ;
- Les obligations en matière de respect de la vie privée des utilisateurs ;
- La notion d'identité numérique ;
- Les sanctions qui sont susceptibles de s'appliquer en cas d'actes manifestement illicites ou interdits par les conditions d'utilisation.
- La définition des droits et obligations respectifs des utilisateurs dans le cadre du réseau social.

Des sessions d'information et de formations peuvent être organisées à ce sujet par l'établissement ou les porteurs de projet ENT.

3.8. Messagerie électronique et messagerie instantanée

3.8.1. Messagerie électronique

Les solutions ENT doivent permettre de générer des adresses électroniques propres à l'ENT pour chacun des utilisateurs. En fonction des situations les porteurs de projet ENT, les administrateurs locaux des ENT, ou toute personne habilitée à cet effet, peuvent paramétrer les modalités et périmètres d'utilisation de ces adresses électroniques et au besoin d'en limiter l'usage inter-utilisateurs de la solution ENT.

La messagerie électronique de l'ENT, lorsqu'elle est limitée à un usage interne n'est pas à proprement parler une messagerie publique comme le proposent les grands acteurs de l'internet ou opérateurs de communications électroniques.

La messagerie électronique de l'ENT est un outil mis à la disposition des utilisateurs mais dont l'utilisation doit suivre les mêmes fins que l'ENT, c'est-à-dire être utilisée uniquement dans un cadre scolaire, à des fins éducatives et pédagogiques.

Dans le cas où sont fournies des adresses électroniques, celles-ci doivent être utilisées conformément aux dispositions des conditions générales ou spécifiques et supprimées (y compris le contenu des boîtes de messagerie). D'une manière générale, la messagerie électronique doit faire l'objet d'un usage conforme à la charte d'utilisation de l'ENT et aux finalités éducatives et pédagogiques de l'ENT.

S'agissant des contenus et messages échangés, ces derniers relèvent par principe du droit de la correspondance privée. Ils sont donc couverts par les dispositions légales concernant les correspondances privées. Il existe des exceptions reconnues par la jurisprudence, notamment les courriels émis dans des listes de discussions publiques (dont le contenu est public) ou des listes à inscription libre et ouverte à tout le monde.

En outre, dans la mesure où cette messagerie s'inscrit dans le cadre particulier de l'ENT, la légitimité du droit du chef d'établissement ou directeur de l'école ou des porteurs de projet d'en protéger la bonne utilisation et l'usage licite peut être invoquée et justifier leur pouvoir d'exercer des contrôles sur lesdites correspondances (Cf. sur ce point *infra* au chapitre « Audit et contrôle). Ce droit de contrôle sera mentionné dans les conditions d'utilisation encadrant l'usage de la messagerie électronique. En tout état de cause, en cas de difficulté, le responsable de l'ENT dispose toujours du droit de demander une autorisation de contrôle à la juridiction compétente.

Dans le cadre d'une utilisation massive ou collective de la messagerie électronique, conférant alors à la messagerie la qualité d'outil de communication publique, il sera dès lors possible et normal pour le responsable de l'ENT de prendre connaissance des messages échangés et d'en demander ou de procéder à leur suppression en cas de contenus inappropriés.

3.8.2. Messagerie instantanée

Un message instantané est un courrier privé (il est envoyé à une ou plusieurs personnes physiques ou morales déterminées). Il est donc régi par les mêmes règles explicitées ci-dessus.

3.8.3. À retenir

Pour la mise en œuvre de la messagerie électronique et de la messagerie instantanée, il convient de :

- Préciser dans la charte d'usage des services numériques que l'adresse de courrier électronique est mise à disposition des utilisateurs de l'ENT dans la limite d'un usage conforme aux principes de l'Éducation nationale ; en ce sens, les utilisateurs doivent utiliser cette adresse de courrier électronique strictement à des fins pédagogiques, éducatives, d'apprentissage, administratives et de vie scolaire ;
- Définir les différentes personnes qui devront exercer une mission de contrôle de l'utilisation qui est faite du contenu des messageries ;
- Définir dans le cadre de ces différents contrôles et rappeler la nécessité du respect de la vie privée résiduelle des utilisateurs ;
- Déterminer dans les conditions d'utilisation et les sanctions qui s'appliqueront aux utilisateurs en cas d'acte illicite ou interdit par les conditions d'utilisation.

3.9. Espace individuel

La plupart des ENT proposent un « espace individuel » sous le seul contrôle de l'utilisateur.

Il est recommandé que la charte d'usage des services numériques informe les utilisateurs que cet espace individuel n'est pas un espace « privé » et qu'il pourra faire l'objet de contrôle, et notamment être accessible Etant toutefois rappelé les enseignants et le personnel conservent un droit à la vie privée résiduelle qui devra être organisé par chaque établissement scolaire de rattachement (soit dans l'ENT, soit hors ENT).

3.9.1. À retenir

La charte d'usage des services numériques à destination des utilisateurs précise que :

- L'espace individuel est mis à disposition des utilisateurs de l'ENT dans la limite d'un usage conforme aux principes de l'Éducation nationale. En ce sens, les utilisateurs doivent utiliser cet espace à des fins pédagogiques ou éducatives ;
- L'utilisateur est responsable de l'utilisation de son espace personnel
- cet espace peut faire l'objet d'un contrôle, notamment à l'occasion d'audit.

3.10. ENT et responsabilités

Dans un ENT la responsabilité est plurielle, comme le sont les intervenants.

En matière de responsabilité relative au déploiement et à l'exploitation, le projet ENT s'inscrit dans le cadre de la répartition de compétences entre les collectivités territoriales et l'État, conformément aux conventions de partenariat établies dans le cadre du portage du projet ENT.

En matière de responsabilité de réalisation/intégration et d'hébergement, la responsabilité porte sur l'éditeur / intégrateur, l'hébergeur / exploitant de la solution ENT elle-même qui doit nécessairement répondre aux exigences fixées par les porteurs de projet et la maîtrise d'ouvrage. Les règles de responsabilité sont précisées dans les marchés publics liant la maîtrise d'ouvrage du projet aux prestataires de solution ENT.

En matière de responsabilité relative à la publication, il apparaît, compte tenu de ses activités et responsabilités, que le directeur de la publication de l'ENT doit être :

- Le chef d'établissement pour le second degré ;
- Le directeur d'école ou l'IA-DASEN dans la mesure où l'école n'a pas la personnalité juridique. Néanmoins, la direction des Affaires juridiques du ministère indiquait dans sa lettre A3 n° 2010-0093 du 6 avril 2010[19], à propos d'un site internet d'une école primaire que *«[…] il semble exclu que le « service » en question soit fourni par l'inspecteur d'académie, directeur des services départementaux de l'Éducation nationale […] »* et que *« dans la mesure où le contenu du site est nécessairement décidé au niveau de l'école, il semble donc préférable que ce soit son directeur qui remplisse la fonction de directeur de la publication […] »*.

En matière d'utilisation de l'ENT, la responsabilité réside avant tout sur les épaules de l'utilisateur lui-même qui, quel que soit son statut, est responsable de ses agissements. L'utilisateur doit, par principe, respecter la loi et s'interdit tout usage illicite ou contraire à la charte d'utilisation ses services numériques de l'ENT (et ses éventuelles conditions particulières).

L'utilisateur peut se voir appliquer d'autres règles particulières telles que celles prévues par une charte du personnel pour les enseignants ou le règlement intérieur de l'établissement pour les élèves.

[19] Lettre d'information juridique n°146 juin 2010 (http://www.education.gouv.fr/lettre-information/lettre-information-juridique/PDF/LIJ_146_juin-2010.pdf)

L'ENT ayant vocation à être utilisé par des personnes mineures, il doit être porté une attention particulière à la protection de celles-ci. Dans le cadre de l'obligation de surveillance et de sécurité de l'établissement scolaire sur les élèves mineurs[20], la mise en œuvre d'un ENT devra être organisée au regard de cette obligation.

3.10.1. À retenir

Une clause « responsabilité » est prévue dans toute relation contractuelle, que ce soit en phase de commande, de réalisation, d'intégration de services du projet ENT ou encore de l'utilisation de l'ENT.

3.11. Droit des tiers

L'ENT est un espace de travail à finalité pédagogique. À ce titre, il doit être utilisé par les utilisateurs dans le cadre des activités éducatives et pédagogiques.

L'ENT permet notamment l'accès à de nombreux contenus et ressources et la réalisation de travaux sous diverses formes. Il convient dès lors de porter une attention particulière aux droits des tiers et notamment aux droits de propriété intellectuelle des fournisseurs de ressources mais également à ceux des utilisateurs et aux droits à l'image tant des utilisateurs que des tiers.

3.11.1. Propriété littéraire et artistique

Les contenus externes et les créations numériques des utilisateurs partagés en ligne sur l'ENT sont protégés par le droit de la propriété intellectuelle.

Il existe néanmoins des dispositions prévoyant plusieurs exceptions à l'obligation de recueillir l'accord de l'auteur. Notamment, l'article L.122-5 e) du Code de la propriété intellectuelle prévoit ainsi :

[20] Article 1242 du Code civil énonçant le principe de la responsabilité des membres de l'enseignement public à raison des dommages causés par les élèves qui leur sont confiés, du fait de fautes, d'imprudences ou de négligences ; Article L.911-4 du Code de l'éducation prévoyant, pour les mêmes dommages - et devant les juridictions de l'ordre judiciaire - la substitution de la responsabilité de l'État à celle des membres de l'enseignement public ; Articles L.912-1 et L.913-1 du Code de l'éducation selon lequel les enseignants sont responsables de l'ensemble des activités scolaires des élèves ; Article R.421-5 du Code de l'éducation, relatif aux EPLE, définissant les droits et les devoirs de chacun des membres de la communauté éducative dans les conditions fixées par le règlement intérieur de l'établissement.

« e) La représentation ou la reproduction d'extraits d'œuvres, sous réserve des œuvres conçues à des fins pédagogiques et des partitions de musique, à des fins exclusives d'illustration dans le cadre de l'enseignement et de la recherche, y compris pour l'élaboration et la diffusion de sujets d'examens ou de concours organisés dans la prolongation des enseignements à l'exclusion de toute activité ludique ou récréative, dès lors que cette représentation ou cette reproduction est destinée, notamment au moyen d'un ***espace numérique de travail,*** *à un public composé majoritairement d'élèves, d'étudiants, d'enseignants ou de chercheurs directement concernés par l'acte d'enseignement, de formation ou l'activité de recherche nécessitant cette représentation ou cette reproduction, qu'elle ne fait l'objet d'aucune publication ou diffusion à un tiers au public ainsi constitué, que l'utilisation de cette représentation ou cette reproduction ne donne lieu à aucune exploitation commerciale et qu'elle est compensée par une rémunération négociée sur une base forfaitaire sans préjudice de la cession du droit de reproduction par reprographie mentionnée à l'article L. 122-10 ».*

3.11.2. Vie privée et droit à l'image

Le droit au respect de la vie privée est un principe garanti par l'article 9 du Code civil.

De plus, le Code pénal condamne notamment la captation frauduleuse de paroles ou d'images. Il est ainsi prévu par les articles 226-1 et suivants les dispositions suivantes :

- « Est puni d'un an d'emprisonnement et de 45 000 euros d'amende le fait, au moyen d'un procédé quelconque, volontairement de porter atteinte à l'intimité de la vie privée d'autrui :
  - 1° en captant, enregistrant ou transmettant, sans le consentement de leur auteur, des paroles prononcées à titre privé ou confidentiel ;
  - 2° en fixant, enregistrant ou transmettant, sans le consentement de celle-ci, l'image d'une personne se trouvant dans un lieu privé. ».

Chacun a le droit au respect de sa vie privée et de son droit à l'image. Ni l'activité professionnelle, ni même les activités dites « publiques » ne sont de nature à remettre en cause cette règle de principe.

À ce titre, la charte d'utilisation des services numériques doit contenir une clause par laquelle chaque usager s'engage à ne pas diffuser sur l'ENT d'informations ou d'images qui porteraient atteinte à la dignité humaine, à la vie privée d'autrui et d'une manière générale, sans en avoir préalablement obtenu l'autorisation de la personne concernée.

Le droit à l'image constitue un attribut de la vie privée. Il est important de veiller au respect du droit à l'image dans le cadre de la réutilisation de photographies et vidéos via l'ENT. Il n'est pas pour autant interdit d'utiliser ces éléments, notamment dans le cadre d'utilisation pédagogique encadrée par les enseignants.

Néanmoins, l'image constituant une « donnée personnelle » qui contribue à identifier directement un individu, il est nécessaire d'obtenir l'autorisation écrite de la personne majeure et de ses représentants légaux s'il s'agit d'un mineur pour la prise de vue et pour la diffusion de l'image.

Par dérogation, il existe des exceptions à l'obligation d'obtenir l'autorisation de la personne, notamment lorsque celle-ci est photographiée dans le cadre d'un lieu public et lorsque l'image illustre une actualité, lorsque la personne n'est pas identifiable sur l'image en cause.

3.11.3. À retenir

Pour la mise en œuvre d'un ENT, il convient d'encadrer la problématique générale de la propriété et tout particulièrement de la propriété intellectuelle et du droit à l'image.

Il convient également d'obtenir les autorisations ou cessions nécessaires à l'exploitation des contenus des tiers et des utilisateurs. La propriété de l'ensemble de ces contenus devra être prévue dans un ensemble contractuel adapté ainsi que dans la charte d'utilisation de services numériques de l'ENT.

Articles à consulter :

Outils pédagogiques vie privée (source : Éducation numérique pour tous par la CNIL)[21] ;

Utilisation de l'image des personnes (source : CNIL)[22].

3.12. Traçabilité

L'ENT est par nature un espace numérique. Dans le cadre d'un espace numérique, l'ensemble des actions sont tracées par nature (logs de connexion).

La traçabilité est également nécessaire pour des raisons juridiques. Cela permet d'identifier les utilisateurs de l'ENT et de conserver les données de trafic relatives à l'usage de l'ENT.

L'objectif de cette traçabilité est de contrôler le bon fonctionnement de l'ENT mis au service des utilisateurs et de détecter les éventuelles anomalies ou dysfonctionnements de la solution ENT.

[21] Outils pédagogiques vie privée (https://www.cnil.fr/fr/ressources-pedagogiques-vie-privee)

[22] Utilisation de l'image des personnes (https://www.cnil.fr/fr/lutilisation-de-limage-des-personnes-0)

Ces éléments (données de connexion ou données de trafic) peuvent également servir de témoin de connexion et d'usages faits de l'ENT par les utilisateurs. Ils permettent en effet de rejouer le parcours d'un utilisateur.

Il existe d'ailleurs un certain nombre de dispositions réglementaires qui imposent la conservation pendant des durées variables selon certaines catégories de données.

Ces éléments (données de connexion ou données de trafic) peuvent par ailleurs être communiqués aux autorités administratives habilitées ou judiciaires compétentes en cas de difficultés ou d'enquête.

La durée de conservation de ces données doit être conforme aux obligations et aux contraintes réglementaires propres à chaque catégorie de données.

Afin de garantir le cadre de confiance prévu par le SDET, une journalisation des accès aux ressources et des actions associées, aussi bien des usagers que des personnels techniques (administrateurs, exploitants…) doit être mise en place. Les journaux ainsi constitués doivent contenir les informations relatives à l'identifiant nominatif, la date et heure de l'accès et les opérations effectuées. Il est accordé une attention particulière aux informations liées à l'utilisation des privilèges. La journalisation des événements qui comprennent des données à caractère personnel doit être conforme aux exigences du RGPD et de la loi relative à l'Informatique, aux fichiers et libertés modifiée.

Toutes les opérations d'exploitation (prise de main à distance, sauvegarde, arrêt et redémarrage d'un service, suppression de fichiers…) doivent être tracées.

3.12.1. À retenir

Pour la mise en œuvre d'un projet ENT, il convient de de :

- Mettre en place une politique relative à la traçabilité des logs de connexion et des mots de passe ;
- Informer les utilisateurs et de prévoir dans la charte d'utilisation les conventions de preuve s'appliquant dans le cadre de l'utilisation de l'ENT ;
- Conserver sur des supports fiables les données et documents pouvant être produits à titre de preuve ;
- Mettre en place un système de traçabilité assurant la conservation et l'intégrité des données d'identification qui pourront être utilisées à titre de preuve qui devra être mis en place d'une part pour répondre aux obligations légales en la matière et d'autre part pour pouvoir l'utiliser à titre probatoire ;
- Respecter les exigences du RGPD et de la loi relative à l'Informatique, aux fichiers et libertés modifiée si les événements journalisés comprennent des données à caractère personnel.

3.13. Atteinte à l'ENT

La solution ENT est par nature un système de traitement automatisé de données.

Les articles 323-1 à 323-7 du Code pénal sanctionnent l'accès et le maintien frauduleux dans un système de traitement automatisé de données.

Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 60 000 € d'amende.

Néanmoins, la qualité de la sécurisation est une condition déterminante en matière de protection. La jurisprudence impose aux responsables de systèmes d'information de pouvoir prouver que des mesures de sécurité ont été mises en œuvre[23].

3.13.1. À retenir

La mise en place d'un niveau de sécurité adapté permet aux porteurs de projet de bénéficier des articles 323-1 et suivants du Code pénal relatifs aux atteintes à des systèmes de traitements automatisés de données.

3.14. Audit et contrôle

L'audit et le contrôle ont pour objectif d'assurer la qualité des services de l'ENT et la protection des utilisateurs et des contenus.

L'audit a pour finalité d'apprécier, à un moment donné, la mise en œuvre des prestations effectuées, des mesures de sécurité ainsi que le fonctionnement des services de l'ENT afin, par exemple, de faire des propositions d'amélioration des services en question.

Le contrôle a pour finalité de vérifier que l'utilisation faite de l'ENT est conforme aux conditions d'utilisation.

[23] TGI de Créteil du 23 04 2013 – Ministère public c/ M. X, CA Paris. 05 02-2014 « Olivier L./ Ministère public ».

Dans le cadre de l'obligation de surveillance et de sécurité de l'établissement scolaire sur les élèves[24], la mise à disposition de l'ENT impose au chef d'établissement ou au directeur de l'école[25] de :

- Définir les règles de contrôle et les différentes personnes qui devront exercer cette mission de contrôle de l'utilisation qui est faite de l'ENT ; par exemple, l'administrateur de l'ENT a une mission de contrôle relative au bon fonctionnement de l'ENT et devra également reporter tout dysfonctionnement qu'il pourrait constater ; les enseignants devront contrôler l'utilisation qui est faite par les « apprenants » de l'ENT dans le cadre des activités éducatives et pédagogiques mises en place ;
- Définir dans les conditions d'utilisation, les conditions de ces différents contrôles et rappeler la nécessité du respect de la vie privée résiduelle des usagers ;
- Déterminer dans les conditions d'utilisation les sanctions qui s'appliqueront aux usagers en cas d'acte illicite ou interdit par les conditions d'utilisation.

Les audits et contrôles ainsi réalisés sont légitimes dans la forme et dans le fond. Ils doivent s'inscrire dans le respect des règles établies et doivent être diligentés à la demande d'une personne compétente.

Il convient de préciser que de tels audits ou contrôles peuvent révéler un usage illicite ou inapproprié et peuvent dès lors fonder une démarche appropriée voire une sanction.

3.14.1. À retenir

Les contrats concernés, la charte d'utilisation et les conditions d'utilisations prévoient la possibilité d'effectuer des audits et contrôles des prestations effectuées dans le cadre des projets ENT et des usages faits de l'ENT.

[24] L'article 1242 du Code civil énonce le principe de la responsabilité des membres de l'enseignement public à raison des dommages causés par les élèves qui leur sont confiés, du fait de fautes, d'imprudences ou de négligences. L'article L.911-4 du Code de l'éducation prévoit, pour les mêmes dommages - et devant les juridictions de l'ordre judiciaire - la substitution de la responsabilité de l'État à celle des membres de l'enseignement public. Les articles L.912-1 et L.913-1 du Code de l'éducation précisent quant à eux que les enseignants sont responsables de l'ensemble des activités scolaires des élèves et que les personnels administratifs, techniques, ouvriers, sociaux, de santé et de service concourent directement aux missions du service public de l'éducation et contribuent à assurer le fonctionnement des établissements et des services de l'Éducation nationale.

[25] Même s'il n'exerce pas de pouvoir hiérarchique sur ses collègues, le directeur d'école est celui qui « veille à la bonne marche de l'école et au respect de la réglementation qui lui est applicable » et « représente l'institution auprès de la commune et des autres collectivités territoriales » (article 2 du décret n° 89-122 du 24 février 1989 relatif aux directeurs d'école)

3.15. Suivi des accès, cookies et statistiques

Le suivi des accès et le relevé de statistiques ont pour finalité d'apprécier le taux d'usage des différents services de l'ENT ainsi que leur organisation et leur efficacité afin de répondre au mieux aux besoins des utilisateurs. Historiquement, l'article 1er de l'arrêté du 30 novembre 2006 modifié par l'arrêté du 13 octobre 2017 prévoyait expressément cette finalité : « Les ENT ont également une finalité statistique en vue de permettre la mesure des accès aux différents services proposés ».

Le projet ENT utilise des outils de statistiques et des *cookies*. Néanmoins aucun d'eux n'est intrusif au regard de la vie privée des utilisateurs.

À ce titre, les données de suivi et statistiques doivent être anonymisées, traitées et conservées conformément au RGPD et à la loi relative à l'Informatique, aux fichiers et libertés modifiée ainsi qu'à la fiche de traitement du registre.

L'utilisation de *cookies* dans le cadre d'un ENT devra s'effectuer en conformité avec les dispositions légales et réglementaires applicables. Un recueil de consentement valide devra être mis en place pour les cookies soumis au recueil du consentement.

Plus précisément, l'utilisation de cookies devra s'effectuer en conformité avec :

- La délibération n° 2020-091du 17 septembre 2020 portant adoption de lignes directrices relatives à l'application de l'article 82 de la loi du 6 janvier 1978 modifiée aux opérations de lecture et écriture dans le terminal d'un utilisateur (notamment aux « cookies et autres traceurs ») et abrogeant la délibération n°2019-093 du 4juillet 2019 ;
- La délibération n° 2020-092du 17 septembre 2020 portant adoption d'une recommandation proposant des modalités pratiques de mise en conformité en cas de recours aux «cookies et autres traceurs.

3.15.1. À retenir

Les données statistiques sont soumises aux obligations de la règlementation de protection des données développées précédemment.

L'utilisation de cookies est soumise au consentement strict des utilisateurs hors cas des traceurs du DNMA qui bénéficient d'une exemption de consentement, et doit respecter plus généralement le cadre fixé par les lignes directrices de la CNIL en la matière du 17 septembre 2020.

3.16. Conservation des données

L'ENT n'a pas vocation à assurer l'archivage des données au sens du Code du patrimoine[26].

Il est important de respecter les prescriptions générales et les règles propres à chaque acteur en fonction de ses obligations et de ses besoins.

3.16.1. Principes

La durée de conservation d'une donnée est fonction de plusieurs critères :

- sa nature (par exemple message, cahier de texte, blog, liste de correspondant, publications…) ;
- sa datation (création, validation, diffusion…) ;
- sa durée d'utilité administrative ou DUA (réglementairement définie) ;
- sa durée d'utilité pratique ou DUP (définie, en l'absence de DUA, selon les besoins du service et validée par l'autorité assurant le contrôle scientifique et technique ou CST).

La circulaire DPACI_RES/2005/003 relative au Tri et à la conservation des archives des services concourant à l'éducation nationale (rectorats, inspections académiques, établissements d'enseignement supérieur, secondaire, primaire, collectivités territoriales, centres de formation et d'apprentissage) et parue au Bulletin officiel n° 24 du 16 juin 2005, propose un tableau de gestion détaillant les règles applicables.

Tout projet d'ENT doit donc intégrer les fonctionnalités nécessaires à la mise en œuvre des actions d'identification, sélection et export pour conservation prévues par cette circulaire.

A noter que la circulaire de 2005, bien que toujours en vigueur, concerne plus particulièrement une production sur support papier. D'autres textes parus depuis peuvent avoir des impacts sur la gestion des éléments numériques produits ou stockés dans les ENT.

[26] Livre II, Titre 1er, Chapitre 2, Section 1 du Code du patrimoine

Le RGPD par exemple nécessite de s'interroger sur le caractère « données personnelles » ou non des informations contenues dans les ENT. Cependant, le RGPD ne saurait être opposable au code du patrimoine. En effet, il impose une vigilance quant à la durée de présence des données à caractère personnel dans les « bases actives » des ENT. Cela signifie que les données peuvent rester accessibles une ou deux années (selon la nature même de la donnée) pour le gestionnaire, mais qu'au-delà de ce terme elles devront être transférées sur une base spécifique ayant un accès réglementé par habilitation (par exemple un système d'archivage numérique). Dans ce système d'archivage les durées de conservation réglementairement définies seront appliquées.

Par ailleurs, le RGPD et la loi « Informatique et libertés » prévoient que, sous réserve de certaines garanties, certains droits relatifs aux données personnelles ne s'appliquent pas dans le cadre d'un traitement archivistique : La mise en œuvre du RGPD ne peut donc en aucun cas justifier l'élimination de certaines données sans visa préalable du service d'archives concerné.

3.16.2. Conservation du cahier de textes numérique

Autre exemple de nouvelles mesures en lien avec la modification des supports, la circulaire n° 2010-136 du 6 septembre 2010 relative au cahier de textes numérique [2] prévoit que : « à la fin de chaque année scolaire, les cahiers de textes numériques seront accessibles pendant une année scolaire entière, dans les conditions des cahiers de textes actifs. Ils pourront être consultés par les enseignants, les conseils d'enseignement, le conseil pédagogique, les conseils de classe et les corps d'inspection. Ils seront ensuite archivés et conservés pendant une durée de cinq ans ».

La durée de conservation des cahiers de texte préalablement définie à 2 ans dans la circulaire de 2005, passe à 7 ans, les deux premières années en base active (donc accessibles à la communauté éducative et aux gestionnaires d'établissement) puis les 5 suivantes dans un système garantissant leur archivage tel que défini par le code du patrimoine.

3.16.3. Conservation des données à caractère personnel

Comme évoqué *supra,* le RGPD et la loi Informatique et libertés imposent s'agissant du traitement de données à caractère personnel de respecter le principe de limitation de la conservation (article 5.1 e) du RGPD).

Plus précisément, il est attendu que les données soient conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées.

De plus, le RGPD consacre également le droit à l'oubli, soit le droit d'obtenir du responsable du traitement l'effacement de l'ensemble des données concernant une personne, ainsi que la cessation de la diffusion de ses données lorsque :

- Les données ne sont plus nécessaires au regard de la finalité pour lesquelles elles ont été collectées ;
- Lorsque le délai de conservation des données a expiré ;
- Le traitement des données n'est pas conforme au règlement.

L'articulation de ces exigences avec les obligations d'archivage public se trouve néanmoins garantie dès lors que le RGPD prévoit expressément, en son sein, que « *les données à caractère personnel peuvent être cependant conservées pour des durées plus longues, dans la mesure où elles seront traitées exclusivement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques, pour autant que soient mises en œuvre les mesures techniques et organisationnelles appropriées, requises par le RGPD et la loi relative à l'Informatique, aux fichiers et aux libertés modifiée afin de garantir les droits et libertés de la personne concernée* » (article 5.1 e) du RGPD).

Pour déterminer la durée de conservation adéquate, en base active, au regard des exigences du RGPD, il importe alors de se référer aux dispositions de l'arrêté du 30 novembre 2006, lequel prévoit que les données personnelles doivent être mises à jour au début de chaque année scolaire et supprimées de l'ENT dans un délai de trois mois dès lors que la personne concernée n'a plus vocation à détenir un compte.

Il est précisé encore que les contributions personnelles laissées dans les espaces communautaires et espaces de stockage d'informations personnelles ou de publication ne pourront, sauf opposition du contributeur lors de la fermeture de son compte ENT, être conservées par l'établissement qu'à des fins de recherche scientifique ou historique ou à des fins statistiques dans les conditions fixées à l'article 5 du RGPD.

Au-delà et conformément à ce qui a été évoqué supra, les données peuvent être conservées plus longtemps dans des conditions d'accès plus restreintes, dès lors que des dispositions légales ou réglementaires prévoient cette conservation obligatoire (conformément donc aux durées fixées dans le kit conservation et archivage).

De façon opérationnelle, dès lors qu'auront été définies les durées de conservation à respecter sous forme numérique, il est recommandé de solliciter du prestataire en charge du déploiement et de la maintenance de la solution logicielle, la mise en œuvre de règles automatiques d'archivage ou de suppression.

3.16.4. À retenir

La mise à disposition d'un ENT impose la mise en œuvre d'une organisation des contenus produits et stockés dans l'outil. En effet le statut d'archives publiques des données des établissements nécessite leur gestion selon les contraintes réglementaires en termes de conservation, de sélection et d'élimination. Cette dernière ne peut avoir lieu sans validation par l'instance en charge du contrôle scientifique et technique.

Les ENT contenant des données à caractère personnel, l'outil devra permettre l'application du RGPD et donc la protection des données sensibles en termes d'accessibilité.

La nécessaire information des utilisateurs quant aux règles de gestion à appliquer rend préférable le recours à un référentiel de conservation des données produites par les ENT rappelant les différentes réglementations en vigueur et intégrant les besoins des utilisateurs.

3.17. Archivage

L'archivage est un ensemble d'actions qui a pour but de garantir l'accessibilité à long terme d'informations (documents ou données) que l'on doit ou souhaite conserver. Ce traitement s'entend tout au long du cycle de vie du document ou de la donnée : de sa création à son sort final (conservation définitive ou élimination). Le traitement d'archives, et tout particulièrement des archives publiques, est défini au livre II du code du patrimoine.

Cette partie présente les principales notions juridiques applicables aux archives, et plus particulièrement aux archives publiques que sont les données produites et stockées dans les ENT.

En complément de cette partie, un « Guide d'accompagnement sur la conservation et l'archivage des données des ENT » a été rédigé par la Mission des archives et du patrimoine culturel (MAPC) du ministère chargé de l'Éducation nationale. Ce guide développe plus précisément le contexte réglementaire et normatif de l'archivage, et présente plusieurs notions essentielles : cycle de vie de la donnée, Records Management, acteurs et périmètre de l'archivage, différences entre sauvegarde et archivage électronique. Un référentiel de conservation, outil de gestion de l'information, et un glossaire sont annexés à ce guide.

3.17.1. La notion d'archives

Il s'agit de l'ensemble des documents et données produits dans l'exercice d'une activité pour garder trace des actions d'une personne, ou d'une organisation publique ou privée.

Le terme « archives » s'emploie quelle que soit la date des documents ou données concernées, de la charte la plus ancienne à la base de données la plus contemporaine.

Tout document peut être archive, quel que soit son support : papier, supports photographiques (plaques de verre, pellicules…), supports audiovisuels (bandes magnétiques, disques…) mais également supports électroniques (disque dur, serveur…).

La notion d'archives est définie à l'article L211-1 du code du patrimoine.

3.17.2. Les archives publiques

Les archives publiques sont l'ensemble des documents, y compris les données, quels que soient leur date, leur lieu de conservation, leur forme et leur support, produits ou reçus, dans l'exercice de leur activité, par toute personne morale de droit public ou toute personne de droit privé dans l'exercice d'une mission de service public.

Les archives publiques sont définies à l'article L211-4 du code du patrimoine.

3.17.3. Le contrôle scientifique et technique (CST)

Le contrôle scientifique et technique est un ensemble de procédures destiné à garantir et protéger le patrimoine culturel en France. Dans le cadre des archives publiques, il permet à l'État de s'assurer des conditions de gestion, de collecte, de sélection et d'élimination, de traitement, de classement, de conservation et de communication de ces archives. Ce contrôle est exercé, par l'instance qui en a la charge, sur pièces et sur places, au moyen d'inspections et de visites de conseil.

Le CST est notamment défini par les articles L212-4 et L212-6 du code du patrimoine.

3.17.4. Les sanctions pénales prévues

Le détournement, la soustraction ou la destruction sans accord préalable de l'administration des archives, intentionnellement ou par négligence, de tout ou partie d'un ensemble d'archives publiques constituent un délit et sont donc pénalement répréhensibles.

Les peines encourues peuvent aller jusqu'à trois ans d'emprisonnement et 45 000 € d'amende.

Ces sanctions pénales sont définies à l'article L214-3 du code du Patrimoine.

3.18. Commerce électronique

Lorsque l'ENT permet d'acquérir des produits, des ressources et/ou des services pour l'école ou l'établissement, le droit du contrat sous forme électronique et du commerce électronique a vocation à s'appliquer.

Dans une telle hypothèse, outre la charte d'usage des services numériques, il est important de prendre en considération, notamment :

- Les dispositions relatives au commerce électronique de la loi n° 2004-575 pour la confiance dans l'économie numérique du 21 juin 2004 lorsque celles-ci sont susceptibles de s'appliquer (en cas notamment de commerce avec des prestataires extérieurs, d'accès payant à des services, de solutions de paiement en ligne) ,
- La protection spécifique des consommateurs résultant du Code de la consommation, et notamment en matière de ventes de biens ou de prestations de services à distance (Chapitre Ier du Titre II du Livre II du Code de la consommation)
- Les dispositions spécifiques relatives à la loyauté des plateformes prévues notamment aux articles 49, 50 et 51 de la loi n° 2016-1321 du 7 octobre 2016 pour une République numérique, ainsi que les dispositions favorisant la dématérialisation, prévues aux articles 24, 93, 103, 104 et 107 de la même loi.

Ces dispositions législatives encadrent les obligations, la responsabilité et les relations contractuelles entre le vendeur et le consommateur.

À ce titre, le vendeur est tenu à de nombreuses obligations, notamment d'information précontractuelle issues du Code de la consommation (notamment les articles L. 111-1, L. 111-2 et L. 221-5).

Il est également nécessaire que l'utilisateur de l'ENT soit clairement informé quant aux engagements qu'il prend et particulièrement du fait que le contrat conclu en ligne constitue un contrat qui lui sera opposable, conformément aux dispositions du Code de la consommation. Ainsi, pour que le contrat soit valablement conclu, le destinataire de l'offre doit notamment avoir eu la possibilité de vérifier le détail de sa commande et son prix total, et de corriger d'éventuelles erreurs, avant de confirmer celle-ci pour exprimer son acceptation. L'auteur de l'offre doit accuser réception sans délai injustifié et par voie électronique de la commande qui lui a été ainsi adressée.

Le paiement en ligne est une autre source d'obligations juridiques qu'il convient de prendre en compte.

Le Code monétaire et financier contient des dispositions concernant l'utilisation des cartes de paiement et l'utilisation de monnaie électronique. Ces dispositions impactent les éditeurs de sites de commerce électronique qui proposent des services pouvant être réglés en ligne.

Il convient de se reporter aux articles L.133-1 et suivants du Code monétaire et financier concernant les règles applicables aux autres instruments de paiement.

Par ailleurs, l'ENT est un espace contrôlé, sans sollicitation commerciale des usagers, et à ce titre, les éditeurs / intégrateurs d'ENT comme les éditeurs de ressources intégrées à l'ENT n'ont pas vocation à publier de contenu promotionnel ou publicitaire au sein des différentes pages de l'ENT.

À retenir

Dans l'hypothèse où l'ENT propose une activité de commerce électronique à destination des usagers, cette activité est régie par les dispositions législatives encadrent les obligations, la responsabilité et les relations contractuelles entre le vendeur et le consommateur., les porteurs de projets doivent identifier des mécanismes de paiement en ligne applicables et effectuer les opérations suivantes :

Choix des moyens de paiement à préciser dans le cahier des charges ;

Établissement de conditions générales de vente ;

rédaction ou audit des contrats avec l'établissement bancaire en charge du service de paiement.

3.19. Récapitulatif des principes juridiques relatifs aux ENT

Principes relatifs à la protection des données à caractère personnel

- Les traitements mis en œuvre par l'ENT sont inscrits dans le registre des traitements du responsable de traitement préalablement à leur mise en œuvre.
- Si le traitement est mené à une échelle régionale, une analyse d'impact relative à la protection des données est également intégrée dans la documentation de conformité du responsable de traitement.
- Toutes les données à caractère personnel traitées au sein de l'ENT font l'objet de mesures de sécurité techniques et opérationnelles adéquates, de façon qu'elles ne soient pas supprimées ou endommagées ou qu'un tiers non autorisé y ait accès.
- Un accord contractuel de responsabilité de traitement conjointe est formalisé lorsque plusieurs entités (autorités académiques, collectivités, EPLE), interviennent sur le traitement de données personnelles lié au déploiement d'un ENT en qualité de responsable de traitement.
- Au sens des dispositions applicables à la protection des données à caractère personnel, les sous-traitants se voient imposées les mêmes exigences juridiques de sécurité et de confidentialité des données que le responsable de traitement. Un document contractuel est régularisé par exemple sous la forme d'une annexe dédiée à la protection des données. Celle-ci reprend les obligations du sous-traitant telles que visées par le RGPD.
- Une mention est insérée sur la page d'accueil de l'ENT pour porter à la connaissance des personnes concernées les informations exigées par le RGPD.
- Le site d'hébergement et la localisation des données sont notamment précisés et répondre aux dispositions applicables à la protection des données à caractère personnel, en particulier les dispositions relatives aux flux transfrontières.
- La traçabilité et journalisation nécessaires sur un plan technique, et sur un plan juridique pour la gestion des preuves, respectent les durées de conservation des données à caractère personnel, ce qui implique de prévoir un système de purge. Les exigences de la loi relative à l'Informatique, aux fichiers et libertés modifiée sont respectées si les événements journalisés comprennent des données à caractère personnel.
- La durée de conservation des données en ligne, sauvegardées ou archivées est en conformité avec les besoins exprimés, les règles de sécurité et de confidentialité, les accords des personnes concernées et la législation en vigueur notamment les règles de conservation des archives publiques.
- Les éditeurs de sites internet et les émetteurs de cookies respectent l'obligation d'information des utilisateurs de l'ENT et obtenir le consentement de ces-derniers avant toute utilisation ou lecture de cookies sur leur terminal.

Autres principes

- Pour la mise en œuvre d'un projet ENT, un ensemble contractuel destiné à délimiter le périmètre d'intervention des différents acteurs impliqués (partenaires, prestataires et fournisseurs de services Tiers, utilisateurs), leurs obligations et engagements et leurs responsabilités respectives, est rédigé.
- S'agissant plus précisément des utilisateurs, des conditions d'utilisation encadrant la mise en œuvre d'un projet ENT au travers de clauses relatives aux droits des utilisateurs, à leurs obligations et responsabilités attachées à l'utilisation de l'ENT ainsi qu'aux sanctions éventuelles, sont rassemblées dans un document de référence dénommé « charte d'usage des services numériques » dont le contenu et les modifications font l'objet d'un processus d'acceptation par les utilisateurs en vue de s'assurer de leur opposabilité.
- Les conditions relatives à l'identification et à l'authentification pour accéder et utiliser un ENT (règles applicables à la remise des identifiants/mots de passe, à leur modification et au niveau de sécurité qui les entoure) sont prévues dans la charte d'usage des services numériques.
- Il est conseillé de mettre en place une modération des espaces d'échanges et de collaboration, qui font, en tout état de cause, l'objet de conditions particulières d'utilisation de l'espace, distinctes de la charte d'usage des services numériques, soumises à l'acceptation expresse de par l'utilisateur.
- La messagerie électronique et de la messagerie instantanée est utilisée à des fins pédagogiques, éducatives, d'apprentissage, administratives et de vie scolaire uniquement ; ceci est rappelé dans la charte d'usage des services numériques qui en précise par ailleurs le cadre d'utilisation (définition des différentes personnes pouvant exercer un contrôle de l'utilisation, rappel de la nécessité du respect de la vie privée résiduelle des utilisateurs ; conditions d'utilisation et sanctions).
- Les contenus diffusés dans respectent les droits des tiers (vie privée, droit à l'image, propriété intellectuelle).
- Les contrats conclus prévoient la possibilité d'effectuer des audits et contrôles des prestations effectuées dans le cadre des projets ENT et des usages faits de l'ENT.
- Lorsqu'un ENT propose une activité de commerce électronique à destination des usagers, cette activité est régie par les dispositions législatives encadrent les obligations, la responsabilité et les relations contractuelles entre le vendeur et le consommateur. Le paiement en ligne est une autre source d'obligations juridiques qu'il convient de prendre en compte.

4. Grilles de conformité

La grille de conformité regroupe l'ensemble des principes identifiés à travers le SDET, dans l'objectif de proposer aux acteurs de l'écosystème un document intégré permettant de :

- Clarifier les obligations auxquelles doivent se conformer les solutions et projets ENT ;
- Proposer aux éditeurs / intégrateurs / mainteneurs et exploitants / hébergeurs de solution ENT et porteurs de projet un dispositif facilitant l'évaluation de la conformité au SDET.

Elles font l'objet d'un document séparé disponibles sur Éduscol au format tableur.