SERVICES NUMERIQUES DE DEMAIN DANS LE MONDE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE AU REGARD DU CADRE INFORMATIQUE ET LIBERTES

Charte de confiance réalisée dans le cadre d'un accompagnement à la formalisation d'une annexe du SDET dédiée à l'ESR

Version 1.2
Première version élaborée 2018. Revue en 2019.

Infhotep

6 rue d'Antin - 75002 Paris
Tél : +33 (0) 155 353 636
Fax : +33 (0) 155 353 640

Mail : contact@infhotep.com
Site : www.infhotep.com
Blog : demain.infhotep.com

Sommaire

Introduction

Ce document résulte d'un travail d'analyse confié au cabinet d'étude Infhotep par la MIPNES (Mission pour la Pédagogie et le Numérique dans l'Enseignement Supérieur, Direction Générale de l'Enseignement Supérieur et de l'Insertion Professionnel, Ministère de l'Enseignement Supérieur de la Recherche et de l'Innovation) en 2017.

Le but de ce travail était de dresser des cadres de confiance dans la gestion des données à caractère personnel impliquées dans un certain nombre d'usages de services numériques en cours de déploiement dans des établissements de l'enseignement supérieur. Conformément à la loi Informatique et Libertés[1] alors en usage, le déploiement d'un service utilisant des données à caractère personnel par un établissement devait faire l'objet de formalités préalables, le cas échéant d'une demande d'avis auprès de la CNIL. Pour éviter des démarches fastidieuses et répétées pour tous les établissements ayant des besoins en général assez similaires, l'idée a été d'établir des cadres de confiance établis afin de répondre aux attendus de la CNIL et de rendre la demande d'avis beaucoup plus simple à construire et à instruire lorsque l'établissement déploie un service dans le respect du cadre de confiance. D'un point de vue très pratique l'explication de ces cadres de confiance visait l'écriture d'une annexe au Schéma Directeur des Espaces de Travail (SDET, https://eduscol.education.fr/cid56994/sdet-version-en-vigueur.html) spécifique pour le supérieur (le SDET établissant des exigences techniques pour le numérique valables pour toute l'éducation nationale ainsi que le supérieur).

Entre temps, est entré en application le 25 mai 2018 le RGPD[2] qui a sensiblement changé le contexte. Aujourd'hui, par application du RGPD, un établissement qui déploie un service numérique n'a plus à formuler une demande d'avis à la CNIL. Nous sommes passé d'une logique déclarative à une logique responsabilisation. L'établissement doit documenter ses traitements de données pour répondre au principe d' « accountability » afin d'être en mesure de rendre compte du respect des obligations attendues par le cadre informatique et libertés en cas de contrôle. Ce travail de documentation obligatoire reprend des préconisations des cadres de confiance et va beaucoup plus loin avec le besoin d'études d'impacts notamment.

Ce document est donc un guide pour aider les établissements d'enseignement supérieur dans le déploiement raisonné des usages impliquant des traitements de données à caractère personnel. Ce guide s'adresse spécifiquement aux Délégués à la Protection des Données, aux Directions des Systèmes d'Information, aux services de scolarité et aux services d'appuis à la pédagogie. Il inventorie un ensemble de recommandations encadrant les nouveaux services liés à l'ENT à fort potentiel, pour certains déjà mis en place dans des établissements pilotes.

[1] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
[2] Le règlement européen EU 2016-679 du Parlement européen et du Conseil du 27 avril 2016

Remerciements

Sources : gouvernement.fr

Nous adressons tous nos remerciements aux représentants des organisations pour leur contribution dans la rédaction de ce document.

Sous la direction de David BESSOT.

Rédacteur pour Infhotep : Alessandro FIORENTINO et Claire DE LA FOUCHARDIERE

Contributeurs

Mission de la pédagogie et du numérique pour l'enseignement supérieur du Ministère de l'enseignement supérieur, de la recherche et de l'innovation : Marie-Françoise CROUZIER, Pierre BEUST, Franck ESTAY, Philippe PORTELLI, Jean-Christophe BURIE, Philippe DEDIEU, Alain MAYEUR, Didier BALTAZART, François GIRAULT, Isabelle DUCHATELLE, Perrine DE COETLOGON, Thierry BEDOUIN et Philippe WERLE.

Les informations présentées dans ce document sont des analyses réalisées conjointement par l'équipe des experts de la MIPNES et les consultants du cabinet Infhotep. Ces travaux ont pour but d'alimenter la réflexion autour du sujet de la protection de la vie privée et des nouveaux usages numériques dans le monde ESR.

A propos d'infhotep

Infhotep est une entreprise de conseil qui accompagne les organisations dans la définition de leur stratégie numérique. Infhotep édite Adequacy, une solution de management et la protection des données à caractère personnel. 6 Rue d'Antin - contact@infhotep.com

Démarche méthodologique

Notre objectif est de s'interroger sur les nouvelles pratiques numériques dans le monde ESR et d'analyser les impacts sur la protection des données à caractère personnelle au regard du RGPD.

Nous avons identifié des pratiques innovantes (sous la forme de « services numériques ») et avons regroupé dans un cadre de référence les règles communes.

Enfin, chaque service a fait l'objet d'une analyse liée aux fondamentaux Informatique et Libertés.

- Objectif(s) poursuivi(s) par le traitement (finalités)
- Données personnelles concernées
- Durée de conservation des données
- Prédétermination des destinataires des données concernées
- Information des personnes et respect des droits « informatique et libertés »
- Sécurité et confidentialité
- Encadrement des transferts de données hors de l'Union Européenne si nécessaire.
- Mesures organisationnelles à mettre en place
- Dispositifs techniques à mettre en œuvre

Les services numériques

Voici la liste des différents services traités par la présente charte de confiance :

- ePortfolio accompagnant l'apprenant tout au long de la vie
- Télésurveillance d'étudiants (examens en ligne)
- Traces d'apprentissages (learning analytics)
- Interfaçage avec des plateformes de certifications
- Coffres forts numériques des étudiants
- Applications mobiles / Les fonctionnalités de géolocalisation possibles par le biais des smartphones
- Votes en ligne dans les établissements
- Valorisation des données collectées
- Questionnaires en ligne à des fins pédagogiques
- Questionnaires en ligne à des fins de recherche
- Système d'alerte et d'information des populations universitaires

1. Règles communes à tous les cadres de référence

Pour l'ensemble des services, des règles communes seront présentes en lien avec les principes ou les domaines ci-dessous :

- L'information des personnes concernées
- Les obligations légales et les formalités Informatique et Libertés
- Les transferts hors UE
- Le consentement
- Les mesures de sécurité

1.1. L'information des personnes concernées

L'obligation d'information et de transparence existe déjà dans la loi Informatique et Libertés. Elle est renforcée par le RGPD : l'information doit être plus complète et plus précise. Elle est par ailleurs assouplie sur les modalités de fourniture et de présentation de cette information.

La transparence permet aux personnes concernées :

- de connaître la raison de la collecte des différentes données les concernant ;
- de comprendre le traitement qui sera fait de leurs données ;
- d'assurer la maîtrise de leurs données, en facilitant l'exercice de leurs droits.
- Pour les responsables de traitement, elle contribue à un traitement loyal des données et permet d'instaurer une relation de confiance avec les personnes concernées.

Vous devez informer les personnes concernées :

- en cas de collecte directe des données : lorsque les données sont recueillies directement auprès des personnes (exemples : formulaire, questionnaire en ligne) ou lorsqu'elles sont recueillies via des dispositifs ou des technologies d'observation de l'activité d'étudiants (exemples : télésurveillance à distance, analyse des traces d'apprentissages, géolocalisation et learning analytics, etc.) ;

- en cas de collecte indirecte des données personnelles : lorsque les données ne sont pas recueillies directement auprès des étudiants (exemples : données récupérées auprès de partenaires institutionnels, via des plateformes « Learning Management System », de sources accessibles au public ou d'autres personnes).

Dans le cadre de la collecte directe vous devez informer au moment du recueil des données ;

Les mentions d'information doivent comporter :

- Identité et coordonnées de l'établissement (responsable du traitement de données) ;
- Finalités (à quoi vont servir les données collectées) ;
- Base juridique du traitement de données (c'est-à-dire ce qui autorise légalement le traitement : il peut s'agir du consentement des personnes concernées, du respect d'une obligation prévue par un texte, de l'exécution d'un contrat, etc.) ;
- Caractère obligatoire ou facultatif du recueil des données (ce qui suppose une réflexion en amont sur l'utilité de collecter ces données au vu de l'objectif poursuivi – principe de « minimisation » des données) et conséquences pour l'étudiant en cas de non-fourniture des données ;
- Destinataires ou catégories de destinataires des données (qui a besoin d'y accéder ou de les recevoir au vu des finalités définies) ;
- Durée de conservation des données (ou critères permettant de la déterminer) ;
- Droits que peuvent exercer les étudiants (opposition, accès, rectification, effacement ; nouveaux droits RGPD : limitation, portabilité) ;
- Droit d'introduire une réclamation (plainte) auprès de la CNIL ;
- Coordonnées du délégué à la protection des données de l'organisme, s'il a été désigné, ou d'un point de contact sur les questions de protection des données à caractère personnel ;

Selon le cas :

- existence d'un transfert des données vers un pays hors Union européenne (ou vers une organisation internationale) et garanties associées ;
- existence d'une prise de décision automatisée ou d'un profilage, les informations utiles à la compréhension de l'algorithme et de sa logique, ainsi que les conséquences pour la personne concernée ;
- le fait que les données sont requises par la réglementation, par un contrat ou en vue de la conclusion d'un contrat;
- les intérêts légitimes poursuivis par le responsable du traitement ou par un tiers (exemple : prévention de la fraude) ;
- le droit au retrait du consentement à tout moment ;
- la faculté d'accéder aux documents autorisant le transfert de données hors de l'Union européenne (exemples : clauses contractuelles types de la Commission européenne) ;

Informations supplémentaires à donner en cas de collecte indirecte :

- Catégories de données recueillies ;
- Source des données (en indiquant notamment si elles sont issues de sources accessibles au public).

Exemple :

« Les informations recueillies sur ce service sont enregistrées dans un fichier informatisé par [nom de l'établissement et coordonnées de l'organisme (responsable du traitement de données)] pour la mise à disposition du [nom du service].

Ce traitement a pour finalité [la ou les finalité(s)].

Ce traitement repose sur le [fondement juridique (c'est-à-dire ce qui autorise légalement le traitement : il peut s'agir du consentement des personnes concernées, du respect d'une obligation prévue par un texte, de l'exécution d'un contrat, etc.), (à décliner par finalité s'il y en a plusieurs) et préciser les conséquences en cas de non-fourniture des données pour les traitements reposant sur le consentement]

Ce traitement aura pour destinataires [les destinataires des données]

La durée de conservation des données dans le cadre de ce service est [durée ou égale à un période (exemple : la période de formation ou du cursus de l'étudiant*)]. A l'issue du cette durée, vos données seront (supprimées ou anonymisées).*

Conformément aux dispositions de la Loi Informatique et Libertés n°78-17 du 6 janvier 1978 modifiée (ci-après « Loi Informatique et Libertés »), vous disposez d'un droit d'accès, de rectification et d'opposition pour motif légitime relativement aux données vous concernant, ainsi que du droit de définir des directives concernant le sort de ses données après votre mort.

Vous disposez en outre :

- *Du droit de solliciter une limitation du traitement ;*
- *D'un droit à l'oubli et à l'effacement numérique ;*
- *D'un droit à la portabilité de vos données ;*
- *Du droit d'introduire une réclamation auprès de la Commission Nationale de l'Informatique et Libertés (CNIL).*

Vous pouvez exercer vos droits sur ces données sur simple demande auprès [du délégué à la protection des données].

Des dispositifs renforcés en termes de sécurité sont mis en œuvre afin de permettre une collecte et un traitement des données personnelles dans les conditions garantissant leur confidentialité, leur intégrité et de manière plus générale leur sécurité dans le respect des dispositions de la Loi Informatique et Libertés.

1.2. Les obligations légales et les formalités Informatique et Libertés

Ces services, qu'ils soient mis en œuvre dans le cadre de l'ENT ou mis à disposition par un prestataire de services tiers des établissements pourvoyeurs de services, seront soumis au Référentiel Général de Sécurité (RGS).

Considérée comme autorité administrative délivrant à ses usagers (les étudiants) lorsqu'un service est considéré comme un téléservice au sens de l'ordonnance n°2005-1516 du 8 décembre 2005, l'établissement devra initier une démarche d'homologation de sécurité définie par le Référentiel Général de Sécurité (RGS).

Le traitement devra être inscrit au registre des activités de traitement de l'établissement conformément à l'article 30 du Règlement Général sur la Protection des Données.

L'article 35 du RGPD prévoit la conduite d'une analyse d'impact relative à la protection des données (AIPD - Data Protection Impact Assessment), lorsqu'un traitement de données personnelles est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées.

Une analyse d'impact relative à la protection des données doit obligatoirement être menée quand le traitement est « susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées ».

Ainsi, généralement, les traitements qui remplissent au moins deux des critères suivants doivent faire l'objet d'une analyse d'impact :

- évaluation/scoring (y compris le profilage) ;
- décision automatique avec effet légal ou similaire ;
- surveillance systématique ;
- collecte de données sensibles ;
- collecte de données personnelles à large échelle ;
- croisement de données ;
- personnes vulnérables (patients, personnes âgées, enfants, etc.) ;
- usage innovant (utilisation d'une nouvelle technologie) ;
- exclusion du bénéfice d'un droit/contrat.

1.3. Les transferts hors UE

Avec la globalisation des échanges et l'utilisation croissante des nouvelles technologies, le nombre de transferts de données hors de France ne cesse de croître. Or, le transfert de données hors de l'Union européenne (UE) et de l'Espace Economique Européen (EEE) est possible, à condition d'assurer un niveau de protection des données suffisant et approprié. Ces transferts doivent être encadrés en utilisant différents outils juridiques.

Toutefois, le recours à des prestataires situés sur le territoire de l'Union européenne est à privilégier.

Toutefois, si un prestataire de service tiers des établissements pourvoyeurs de ce service n'étant pas établi sur le territoire de l'Union européenne assurait ce service, il conviendrait d'encadrer le transfert de données hors UE afin d'assurer un niveau de protection adéquat et à cet effet de recourir à des outils.

Le RGPD élargit la gamme d'outils juridique permettant d'encadrer les transferts. Ils pourront être utilisés tant par les responsables de traitement que par les sous-traitants.

Afin d'assurer un haut niveau de protection des données transférées du territoire européen à des Etats tiers, les établissements souhaitant transférer des données peuvent recourir aux outils suivants :

- La décision d'adéquation (art. 45 du RGPD), qui constitue le premier outil juridique d'encadrement, dans la mesure où elle est prise sur la base d'un examen global de la législation en vigueur dans un Etat, sur un territoire ou applicable à un ou plusieurs secteurs déterminés au sein de cet Etat ;

- En l'absence d'une telle décision, des « garanties appropriées » (art. 46 du RGPD), constituées pour la majorité de décisions des autorités de contrôle et qui sont prises à la lumière des engagements des organismes concernés ;

- En l'absence de telles garanties appropriées, le transfert peut enfin être réalisé par dérogation à ces outils globaux d'encadrement, dans des situations particulières et des conditions spécifiques. Les mécanismes actuels d'encadrement des transferts actuels restent valables

En effet les transferts hors UE peuvent être fondés sur :

- une décision d'adéquation de la Commission européenne concernant certains pays assurant un niveau de protection adéquat ;
- des clauses contractuelles types (CCT) de la Commission européenne ;
- des règles internes d'entreprises (BCR) ;
- des clauses contractuelles spécifiques (considérées comme conformes aux modèles de clauses de la Commission européenne) ;

Avec le RGPD, les transferts peuvent également être encadrés par :

- des clauses contractuelles types adoptées par une autorité de contrôle et approuvées par la Commission européenne ;
- un code de conduite approuvé (comportant l'engagement contraignant et exécutoire pris par les destinataires hors UE d'appliquer les garanties appropriées) ;
- un mécanisme de certification approuvé (comportant l'engagement contraignant et exécutoire pris par les destinataires hors UE d'appliquer les garanties appropriées) ;
- un arrangement administratif ou un texte juridiquement contraignant et exécutoire pris pour permettre la coopération entre autorités publiques (Mémorandum of Understanding dit MOU ou MMOU, convention internationale…).

Dans certains cas une autorisation de la CNIL reste nécessaire

Si le transfert est fondé sur :

- Des clauses contractuelles spécifiques entre le responsable d'un fichier ou un sous-traitant et un autre responsable de fichier, un sous-traitant ou un destinataire des données dans le pays tiers ou l'organisation internationale ;

- Des dispositions à intégrer dans des arrangements administratifs entre les autorités publiques ou les organismes publics qui prévoient des droits opposables et effectifs pour les personnes concernées ;

- Obligations règlementaires.

1.4. Le consentement

Le recueil du consentement exprès et spécifique de l'étudiant est opéré via une case à cocher formalisant son accord éclairé, lors de l'activation du service par le biais de l'ENT ou lors de son inscription à une plateforme mise à disposition par un prestataire de service tiers des établissements pourvoyeurs de services.

Conformément aux lignes directrices relatives au consentement, endossées par le Comité Européen de Protection des Données (CEPD), le consentement doit être :

Libre – Pour être valable, le consentement ne doit pas être lié ou conditionné. Cela implique que la fourniture d'un bien ou d'un service ne peut être subordonnée à l'obtention du consentement de l'intéressé.

Spécifique – Le CEPD défend la "granularité" du consentement, qui suppose un opt-in distinct pour chaque type de finalité.

Informé – Le consentement n'est valable que s'il a été donné en pleine connaissance de cause, ce qui implique une information préalable exhaustive et claire sur le traitement et ses finalités.

Les conséquences du refus de l'étudiant sont à formaliser de manière explicite dans la formule de recueil du consentement.

1.5. Les mesures de sécurité

Dispositifs techniques

Le responsable de traitement doit s'assurer que chaque utilisateur ne peut accéder qu'aux seules données dont il a besoin pour l'exercice de son activité. Pour cela, chaque utilisateur doit disposer d'un identifiant unique et s'authentifier avant d'accéder au système. Les mécanismes permettant d'authentifier les utilisateurs peuvent, par exemple, prendre la forme de mots de passe rattachés à un identifiant ou à une carte à puce. Lorsque l'authentification ou l'identification des utilisateurs est assurée par des mots de passe conforme à la recommandation de la CNIL du 27 janvier 2017.

L'accès privé ou public aux différents services devra être sécurisé avec un protocole web : HTTPS validé par une autorité de certification.

2. Règles spécifiques dédiées aux différents services

2.1. ePortfolio accompagnant l'apprenant tout au long de la vie

Description du service

L'e-Portofolio est un service mis à disposition de l'étudiant par défaut dans le bouquet de services offert par l'ENT ou pouvant être proposé de manière indépendante via une plateforme éditée par un prestataire de service tiers des établissements pourvoyeurs de services d'e-Portfolio.

Le service a vocation à alimenter la réflexion de l'étudiant sur son parcours personnel, professionnel, social (engagements associatifs, activités culturelles…) engagé dans le cadre d'une formation tout au long de la vie.

Il permet de :

- centraliser du contenu relatif au niveau de compétence de l'étudiant (productions numériques, contribution à des projets, traces d'activités réalisées sur une plateforme d'enseignement, évaluations effectuées par le corps professoral, certificats, diplômes, formations, CV, lettre de motivation…) (ci-après désigné « preuves de compétences ») ;

- permettre à différents groupes de personnes appartenant à un périmètre défini par l'étudiant d'évaluer l'étudiant, en fonction de leur domaine académique de compétence ;

- formaliser une présentation des compétences de l'étudiant dans un objectif de valorisation et de promotion de son parcours personnel de formation auprès de partenaires ou de recruteurs potentiels.

L'étudiant est l'unique acteur pouvant intégrer du contenu dans l'e-Portfolio. Il est également le seul à maîtriser pour chaque contenu le caractère public ou privé de chaque donnée, qui a accès à quelles données, et est en mesure de supprimer le contenu de son e-Portfolio à tout moment. En cas de non utilisation de ce service, l'e-Portfolio contiendra uniquement les compétences acquises qui auront été validées par l'équipe pédagogique. Ces compétences acquises resteront privées.

Toutefois, les différents éléments de contenu du e-Portofolio peuvent être partagés par l'étudiant à différents groupes de personnes, selon le ou les périmètres qu'il a lui-même défini(s). Les personnes ainsi habilitées par l'étudiant à accéder à ses éléments de contenu du e-Portfolio peuvent alors effectuer des évaluations de l'étudiant, en fonction de leur domaine académique de compétences.

Responsables de traitements concernés

- Etablissements d'enseignement supérieur

Services chargés de la mise en œuvre

- Equipes pédagogiques
- Services d'appui à la pédagogie numérique
- Services universitaires de pédagogie
- Prestataires de services tiers des établissements pourvoyeurs de services – devant se conformer à l'article 28 du Règlement Général sur la Protection des Données. (Pour en savoir plus voir le guide du sous-traitant de CNIL)

Fondement juridique

Le service est proposé à titre facultatif à chaque étudiant qui le souhaite, sur la base de son consentement.

Le refus de consentement de l'étudiant ne lui permet pas de bénéficier de ce service.

Finalités poursuivies par le traitement

Finalité 1 : la centralisation de preuves de compétences de l'étudiant à des fins d'alimentation de la réflexion de l'étudiant sur son parcours personnel, social et professionnel engagé dans le cadre d'une formation tout au long de la vie.

Finalité 2 : La présentation formalisée des preuves de compétence de l'étudiant dans un objectif de valorisation et de promotion de son parcours personnel de formation auprès de partenaires ou de recruteurs potentiels.

Catégories de données

<u>Données concernant les étudiants :</u>

- Civilité, noms, prénoms, date et lieu de naissance, ville et pays de naissance, identifiant national étudiant (INE), photographie et coordonnées personnelles
- Données relatives à la vie universitaire et/ou professionnelle de l'étudiant : CV, établissements scolaires, formation professionnelle, distinctions, travaux personnels de l'étudiant (devoirs, mémoires, etc.) … ; données en lien avec la formation (diplômes, stages, expériences) et l'apprentissage de l'étudiant (CV en ligne, lien vers les réseaux sociaux professionnels…) ;
- Données relatives à la vie personnelle : situation familiale (facultatif, information mentionnée sur le CV à la discrétion de l'étudiant)
- Données relatives aux habitudes de vie : loisirs, activités sportives… (facultatif, information mentionnée sur le CV à la discrétion de l'étudiant)

- Données relatives au suivi des compétences formelles et informelles (académiques, relationnelles, non techniques…)
- Données d'ouverture d'un compte ENT / plateforme : identifiant, mot de passe

Données concernant les personnels enseignants et non enseignants :

Les personnels enseignants et non enseignants désignent toute personne amenée à valider ou à rendre un avis sur les activités et productions réalisées par un étudiant dans le cadre de son cursus – en ce compris un maître de stage ou un tuteur d'apprentissage.

- Civilité, noms, prénoms, date de naissance, situation professionnelle, structure de rattachement, coordonnées professionnelles, informations administratives les concernant,
- Toute information concernant la scolarité des étudiants dont ils ont la charge
- Données d'ouverture d'un compte ENT : identifiant, mot de passe
- Pour les tuteurs de stage et maîtres d'apprentissage : situation professionnelle du tuteur de stage ou du maître d'apprentissage, dénomination de l'entreprise partenaire et nom des étudiants suivis en stage ou en apprentissage.

Durée de conservation des données

Les données ont vocation à être conservées à l'issue de la formation supérieure de l'étudiant. Elles sont conservées jusqu'à ce que l'intéressé demande leur suppression.

Lorsque le service est intégré à l'ENT, une demande explicite d'accord de l'étudiant à la conservation de ses données lui est adressée une fois par an.

Les contributions personnelles laissées dans les espaces communautaires et espaces de stockage d'informations personnelles ou de publication peuvent, sauf opposition du contributeur lors de la fermeture de son compte ENT, être conservées par l'établissement à des fins informatives, pédagogiques ou scientifiques dans les conditions fixées à l'article 36 de la Loi Informatique et Libertés.

Le droit à la portabilité est pris en charge dans le cadre du e-Portfolio, par la mise à disposition d'une fonction d'export de l'ensemble des contenus du e-Portfolio. Quel que soit le type de mise à disposition du service, l'étudiant peut exporter vers un format HTML ou un format Leap2A (format standard des e-Portfolios) et compatible avec des dispositifs extérieurs (type mahara).

Destinataires des données

- Etudiants
- Personnels enseignants et non enseignants habilités par l'étudiant à avoir accès aux données concernées dans le cadre de leurs fonctions
- Prestataires de services tiers des établissements pourvoyeurs de services – devant se conformer à l'article 28 du Règlement Général sur la Protection des Données. (Pour en savoir plus voir le guide du sous-traitant de CNIL)

Mesures de sécurité et de confidentialité

Les mesures organisationnelles :

L'étudiant sera le seul à pouvoir choisir, pour chaque contenu, du caractère public ou privé de chaque donnée.

Il devra être formalisé que l'e-Portfolio ne devra pas induire de conséquences juridiques ou administratives sur l'évolution ou le parcours de l'étudiant qui ne serait pas bienveillante à la suite d'une analyse de ce dernier. La finalité qui est prédéterminée est la présentation des acquis de la formation (apprentissage, connaissances, savoirs compétences, expériences, réalisations, et les évaluations). En aucun cas il ne devra servir à évaluer globalement un étudiant.

2.2. Télésurveillance d'étudiants (examens en ligne)

Description du service

Le service de télésurveillance des étudiants est mis à disposition de l'étudiant par défaut dans le bouquet de services offert par l'ENT ou est proposé de manière indépendante via une plateforme éditée par un prestataire de service tiers des établissements pourvoyeurs de services de télésurveillance.

Le développement des formations à distance dans l'enseignement supérieur implique que les modalités de certification et de passage d'examens soient aussi adaptées à la distance.

Le service a vocation à assurer des modalités d'examens alternatives aux examens présentiels, dans le cadre d'une formation à distance, au moyen d'une télésurveillance d'épreuves par webcam au domicile de l'étudiant ou de tout autre lieu qui réponde aux conditions posées (neutre, sans présence d'autres personnes), par exemple une pièce dédiée dans une université proche du lieu de domiciliation de l'étudiant.

L'identité de l'étudiant est vérifiée par un surveillant connecté avant le démarrage de l'examen, sur présentation de la pièce d'identité de l'étudiant.

Il est recommandé d'intégrer les présentes modalités de mise en œuvre du service de télésurveillance d'étudiants dans le règlement intérieur de l'établissement d'enseignement supérieur.

Responsables de traitement concernés

- Etablissements d'enseignement supérieur

Services chargés de la mise en œuvre

- Services de pilotage de la formation à distance
- Prestataires de services tiers des établissements pourvoyeurs de services de télésurveillance – devant se conformer à l'article 28 du Règlement Général sur la Protection des Données. (Pour en savoir plus voir le guide du sous-traitant de CNIL)

Fondement juridique

Le service est proposé à titre facultatif à chaque étudiant qui le souhaite, sur la base de son consentement.

Le refus de consentement de l'étudiant ne lui permet pas de bénéficier de ce service. Le cas échéant, il doit se déplacer physiquement sur le lieu d'examen.

Données personnelles concernées

Données concernant les étudiants :

- Civilité, noms, prénoms, date et lieu de naissance, ville et pays de naissance, identifiant national étudiant (INE), photographie et coordonnées personnelles
- Données relatives à la vie universitaire et/ou professionnelle de l'étudiant : parcours universitaire (inscription aux diplômes/certificats)
- Type de connexion internet : débit ascendant et descendant (Cette information est collectée lors du test effectué en amont et est nécessaire pour s'assurer que la connexion de l'étudiant est adaptée pour l'utilisation du service.)
- Captation vidéo de la surveillance
- Données d'ouverture d'un compte ENT /plateforme : identifiant, mot de passe

Données concernant les surveillants :

- Civilité, noms, prénoms
- Fonction du surveillant au sein de l'établissement

Durée de conservation des données

L'ensemble des informations inhérentes à ce service sont conservées jusqu'à ce que l'ensemble des examens soit corrigé. En cas d'incident pendant l'examen les données pourront être conservées le temps du contentieux.

Les données d'ouverture d'un compte utilisateur sur une plateforme indépendante devront être mises à jour au début de chaque année universitaire et supprimées dans un délai de trois mois dès lors que l'étudiant n'a plus vocation à détenir un compte.

Destinataires des données

- Etudiants (en temps réel et a posteriori en cas de litige)
- Surveillant assurant le contrôle du bon déroulé de l'examen (en temps réel et a posteriori en cas de litige)
- Personnels enseignants habilités à avoir accès aux données concernées dans le cadre de leurs fonctions (a posteriori en cas de litige)
- Personnels administratifs habilités à avoir accès aux données concernées dans le cadre de leurs fonctions (a posteriori en cas de litige)
- Prestataires de services tiers des établissements pourvoyeurs de services de télésurveillance – devant se conformer à l'article 28 du Règlement Général sur la Protection des Données. (Pour en savoir plus voir le guide du sous-traitant de CNIL)

Mesures de sécurité

La sensibilité des données collectées dans le cadre de la télésurveillance doit être déterminée pour mettre en place les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté aux risques.

Les mesures organisationnelles :

La Webcam devra filmer l'étudiant uniquement, un mur neutre en fond est recommandé, afin de respecter une forme de minimisation de la collecte évitant les potentiels phénomènes de sérendipité[3] concomitants à la collecte d'informations (ex : bibliothèque en fond permettant de profiler un étudiant en fonction de ces lectures ou tout autre type d'information qui permettrait indirectement d'effectuer du profilage ou de simplement collecter des informations qui n'ont aucune pertinence avec la finalité prédéterminée en sus).

Aucune fenêtre ne devra être présente dans le champ de la captation vidéo, il s'agit d'éviter la collecte de données à caractère personnel d'un voisin dont le consentement n'aurait pas été recueilli.

L'étudiant devra être seul dans la pièce où il se trouve afin d'éviter la collecte de données à caractère personnel d'un parent dont le consentement n'aurait pas été recueilli, par exemple une captation audio.

Tout écart de l'étudiant au cadre de télésurveillance qui lui est imposé par son établissement d'enseignement supérieur ne pourra être invoqué par l'étudiant dans le cadre d'un recours à l'encontre de l'établissement.

[3] La notion de sérendipité désigne le fait de collecter des données, sans que ces dernières n'aient été requises ni anticipées.

2.3. Traces d'apprentissages (learning analytics)

Description du service

L'analyse de l'apprentissage (Learning Analytics) est une tendance émergente en France. La généralisation de l'usage des outils numériques par les étudiants permet de constituer des corpus de données importantes sur leur comportement.

Ce service permet de traiter et d'analyser les données liées aux traces d'apprentissage de l'étudiant afin de (i) comprendre les apprenants et d'optimiser les outils et les contextes, dans un objectif d'amélioration de leur apprentissage et de réponse à leurs attentes, (ii) d'identifier des apprenants en difficulté, d'identifier des pratiques d'enseignement efficaces, d'adapter et de personnaliser les services numériques mis à disposition par l'établissement d'enseignement supérieur, pour favoriser la réussite de l'étudiant, (iii) de transmettre ces données à des fournisseurs de services à des fins de proposition d'offres pédagogiques adaptées (par exemple, une start-up spécialisée le conseil en orientation).

En pratique, le recueil de traces d'apprentissages pour cette dernière finalité permettra un profilage à des fins prédictives en fonction des données collectées. Néanmoins, ce service n'a aucune vocation présente ou future à permettre qu'un étudiant fasse l'objet d'une décision fondée exclusivement sur un traitement automatisé.

Le service est mis à la disposition des étudiants disposant d'un compte ENT ou via une plateforme indépendante.

Responsables de traitement concernés

- Etablissements d'enseignement supérieur

Services chargés de la mise en œuvre

- Equipes pédagogiques
- Services d'appui à la pédagogie numérique
- Services universitaires de pédagogie
- Prestataires de services tiers des établissements pourvoyeurs de services – devant se conformer à l'article 28 du Règlement Général sur la Protection des Données. (Pour en savoir plus voir le guide du sous-traitant de CNIL)

Fondement juridique

Le service est proposé à titre facultatif à chaque étudiant qui le souhaite, sur la base de son consentement, associé à chaque finalité.

Le refus de consentement de l'étudiant ne lui permet pas de bénéficier de ce service.

Finalités

Finalité 1 : Traitement et analyse des traces numériques des étudiants afin de comprendre les apprenants et d'optimiser les outils et les contextes, dans un objectif d'amélioration de leur apprentissage et de réponse à leurs attentes.

Finalité 2 : Traitement et analyse des traces numériques des étudiants afin d'identifier des apprenants en difficulté, d'identifier des pratiques d'enseignement efficaces, d'adapter et de personnaliser les services numériques mis à disposition par l'établissement d'enseignement supérieur, pour favoriser la réussite de l'étudiant.

Finalité 3 : Transmission des traces numériques à des fournisseurs de services (statut étudiant, statut boursier…), notamment à des LMS externes (Learning Management System).

Consentement

À tout moment dans le cadre de son utilisation du service, l'étudiant peut retirer son consentement pour toutes ou partie des finalités du service, via le compte ENT, sans aucune conséquence sur l'utilisation des autres services numériques.

En cas d'opposition, toutes les données collectées concernant cet étudiant seront automatiquement anonymisées, sans aucun délai de rétention des données identifiantes.

Si l'étudiant redonne son consentement a posteriori, la collecte des traces d'apprentissage repartira de zéro.

Données personnelles concernées

Les catégories de données à caractère personnel traitées par ce service sont les suivantes :

<u>Données concernant les étudiants :</u>

Finalité 1 :

- Données d'ouverture d'un compte ENT /plateforme : identifiant, mot de passe
- Données d'utilisation des différents services numériques pédagogiques : données de connexion, durée de connexion, nombre de connexions, nature de l'activité réalisée

Finalités 2 et 3 (requérant l'identification) :

- Données administratives : civilité, noms, prénoms, date et lieu de naissance, ville et pays de naissance, identifiant national étudiant (INE)
- Données en lien avec la scolarité (historique, programme actuel, filière d'origine, temps de transport, notes, diplômes, inscriptions)
- Données d'ouverture d'un compte ENT /plateforme : identifiant, mot de passe

Durée de conservation des données

Les données sont conservées pour la période de formation de l'étudiant.

A l'issue du cursus universitaire de l'étudiant au sein de l'établissement ou à son départ de l'établissement, ses données sont anonymisées.

Destinataires des données personnelles

- Personnels enseignants habilités à avoir accès aux données concernées dans le cadre de leurs fonctions
- Etudiant, par le biais d'un tableau de bord personnel accessible via l'ENT
- Etudiant, par le biais de la fonction d'extraction assurant le droit à la portabilité
- Prestataires de services tiers des établissements pourvoyeurs de services – devant se conformer à l'article 28 du Règlement Général sur la Protection des Données. (Pour en savoir plus voir le guide du sous-traitant de CNIL)
- Fournisseurs de services externes, sous réserve du consentement de l'étudiant :
    - Organisme public, après conclusion d'une convention d'échanges de données, en réponse à une obligation légale
    - Organisme de statistique, Observatoire… (destinataire de données anonymisées uniquement, selon une technique ne permettant ni individualisation, ne corrélation, ni inférence, conformément aux recommandations du CEPD).

Mesures de sécurité et de confidentialité

La sensibilité des données collectées dans le cadre du service learning analytics doit être déterminée pour mettre en place les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté aux risques.

2.4. Interfaçage avec des plateformes de certifications

Description du service

Le temps où les ENT pouvaient être décrits en termes de bouquets de services internes est largement dépassé.

Aujourd'hui, des services tiers sont accessibles à partir d'un portail ENT. Parmi les plateformes identifiables dans le paysage de l'ESR peut par exemple être citée FUN-MOOC, la future plateforme PIX pour la certification en compétences numériques, et potentiellement tout environnement extérieur à un établissement lié à l'activité d'apprentissage d'un étudiant (un e-portfolio national, des coffres forts numériques...).

Le service d'interfaçage des plateformes permet :

- L'accès transparent à une plateforme de certification engagée contractuellement avec l'établissement, à partir d'une authentification depuis l'ENT impliquant une fédération d'identité numérique pour des accès simplifiés, sans nouvelle demande d'authentification de l'utilisateur dès qu'il mobilise un service tiers ;

- La remontée vers l'ENT des données collectées dans le cadre de l'utilisation par les étudiants d'une plateforme de certification engagée contractuellement avec l'établissement ;

- La fourniture aux plateformes de certification engagées contractuellement avec l'établissement de données statistiques relatives à l'utilisation par les étudiants des services numériques de l'ENT.

Responsables de traitement concernés

- Etablissements d'enseignement supérieur

Services chargés de la mise en œuvre

- Service d'aide à l'insertion professionnelle
- Equipes pédagogiques
- Services d'appui à la pédagogie numérique
- Services universitaires de pédagogie
- Plateformes de certification engagées contractuellement avec l'établissement

Finalités

Finalité 1 : L'authentification unique depuis l'ENT pour accéder à des services tiers mis à disposition sur des plateformes partenaires.

Finalité 2 : La remontée vers l'ENT des données relatives à l'apprentissage de l'étudiant collectées dans le cadre de l'utilisation d'un service tiers sur des plateformes partenaires (ex : MOOC).

Finalité 3 : La fourniture aux plateformes de certification engagées contractuellement avec l'établissement de données statistiques relatives à l'utilisation par les étudiants des services numériques de l'ENT.

Fondement juridique

Le service est proposé à titre facultatif à chaque étudiant qui le souhaite, sur la base de son consentement.

Le refus de consentement de l'étudiant ne lui permet pas de bénéficier de ce service. À tout moment en cours d'année, l'étudiant peut retirer son consentement.

Données personnelles concernées

Données concernant l'étudiant :

- État-civil, identité, données d'identification…
- Données d'ouverture d'un compte ENT /plateforme : identifiant, mot de passe
- Données d'utilisation des différents services numériques pédagogiques : données de connexion, durée de connexion, nombre de connexions, nature de l'activité réalisée

Durée de conservation des données

Les données doivent être conservées au minimum, sur une durée équivalente à celle du cursus de l'étudiant au sein de l'établissement, néanmoins elles peuvent être conservées au-delà de cette période, à la demande expresse de l'étudiant et avec accord (tacite ou exprès) de l'établissement.

Destinataires des données

- Plateformes de certifications engagées contractuellement avec l'établissement, agissant en qualité de co-responsable de traitement

Mesures de sécurité et de confidentialité

L'ensemble des données privées issues de l'ENT et fournies aux différentes plateformes potentielles doit être chiffrées par le biais d'un système de chiffrement asymétrique lors du transfert. Un système de hashage ante-transfert et post-transfert doit également être mis en place afin d'assurer l'intégrité des données expédiées.

2.5. Coffres forts numériques des étudiants

La gestion des documents administratifs à destination des étudiants est une tâche relativement lourde pour l'établissement d'enseignement supérieur.

L'objet de ce service est de dématérialiser un maximum les flux de gestion de ces documents, en offrant aux étudiants la possibilité de placer leurs documents personnels mais aussi de recevoir les versions numériques des documents administratifs émis par l'établissement d'enseignement supérieur.

Ce coffre-fort peut également être ouvert à d'autres entités partenaires de l'établissement d'enseignement supérieur (comme par exemple les mutuelles, le CROUS) afin de leur permettre d'ajouter des documents concernant l'étudiant.

Le coffre-fort numérique est mis à disposition de l'étudiant dans le bouquet de services offert par l'ENT ou peut être proposé de manière indépendante via une plateforme éditée par un prestataire de service tiers des établissements pourvoyeurs du service. Seul l'étudiant peut consulter le contenu du coffre-fort.

Responsables de traitement concernés

- Etablissements d'enseignement supérieur

Services chargés de la mise en œuvre

- La Direction des Études et de la Vie Étudiante (DEVE)
- Tout service équivalent pour la gestion quotidienne des coffres forts
- Un opérateur existant pourrait garantir une mise en œuvre adéquate sur l'ensemble des établissements d'enseignement supérieur.

Finalités

Finalité 1 : le stockage des documents administratifs propres à l'étudiant (quittances de loyer, scan des déclarations d'impôts, factures, relevés de banque, etc.).

Finalité 2 : la réception des documents administratifs officiels émis par l'établissement d'enseignement supérieur ou par des entités partenaires, au choix de l'étudiant parmi une liste de partenaires mises à sa disposition par l'établissement d'enseignement supérieur.

Fondement juridique

Le service est proposé à titre facultatif à chaque étudiant qui le souhaite, sur la base de son acceptation des conditions générales d'utilisation du service.

La réception des documents administratifs officiels émis par l'établissement supérieur ou par des entités partenaires repose sur le consentement de l'étudiant, pour chaque entité émettrice.

Le refus de consentement de l'étudiant ne lui permet pas de bénéficier de ce service. À tout moment en cours d'année, l'étudiant peut retirer son consentement.

Données personnelles concernées

Données concernant l'étudiant :

- État-civil, identité, données d'identification…
- Données d'ouverture d'un compte ENT /plateforme : identifiant, mot de passe
- Données relatives à la vie universitaire et/ou professionnelle de l'étudiant : parcours universitaire (inscription aux diplômes/certificats)
- Données issues des documents administratifs déposés par l'étudiant, et par l'établissement d'enseignement supérieur ou par ses partenaires, le cas échéant

Durée de conservation des données

À tout moment, l'étudiant peut supprimer son coffre-fort, sur simple demande effectuée auprès du service gestionnaire de l'applicatif. Le cas échéant, les données présentes dans son coffre-fort numériques sont supprimées. Aussi, si l'étudiant souhaite les conserver, il lui appartient d'effectuer préalablement des sauvegardes de ses documents, l'établissement d'enseignement supérieur n'y ayant pas accès.

Option 1 : A l'issue du cursus de l'étudiant et si ce dernier ne souhaite pas souscrire à la prolongation du service, l'étudiant aura uniquement la possibilité d'exporter son contenu pendant une durée de 12 mois.

Deux messages d'information sont envoyés à l'étudiant préalablement à la suppression de son coffre-fort (1 an et 2 mois avant la suppression du coffre-fort). Le coffre-fort est ensuite fermé et l'ensemble de son contenu détruit.

Option 2 : A l'issue de son cursus, si l'étudiant souscrit à la prolongation du service, ses données sont conservées pour la durée de souscription su service.

A l'issue de la période de souscription de l'étudiant au service, l'étudiant aura uniquement la possibilité d'exporter son contenu pendant une durée de 12 mois.

Deux messages d'information sont envoyés à l'étudiant préalablement à la suppression de son coffre-fort (1 an et 2 mois avant la suppression du coffre-fort.). Le coffre-fort est ensuite fermé et l'ensemble de son contenu détruit.

Mesures de sécurité et de confidentialité

Recommandation 1 : Le service de coffre-fort numérique collecte, dans le cadre de la création d'un compte, des données d'identification pertinentes et proportionnées au regard de la finalité. L'identification de l'étudiant détenteur du coffre ne peut, en aucun cas, être réalisée au moyen du numéro de sécurité sociale (RNIPP). L'identification de l'utilisateur lors de l'accès au service de coffre-fort numérique est assurée par un moyen d'identification électronique adapté aux enjeux de sécurité du service

Recommandation 2 : En l'absence d'agrément ministériel pour l'hébergement de données de santé, l'établissement informe l'étudiant de l'interdiction de stocker des données relatives à la santé. Il ne prévoit pas la création par défaut de dossiers relatifs à la santé.

Recommandation 3 : L'établissement informe l'étudiant de l'interdiction de stocker des contenus illicites (exemple : incitation au meurtre, incitation à la haine raciale, pédopornographie…).

Recommandation 4 : Le service de coffre-fort numérique ne permet la consultation des documents dématérialisés stockés que par l'étudiant concerné, et le cas échéant, par les personnes spécialement mandatées par ce dernier (par exemple un notaire, pour permettre aux ayants droits d'accéder à ses données…).

Recommandation 5 : Le service de coffre-fort numérique efface les documents supprimés définitivement par l'étudiant, ainsi que leurs métadonnées, de tous les endroits où ils sont stockés :

- sans délai pour les espaces de stockage courants et les éventuelles copies répliquées en ligne (synchronisées en temps réel ou en miroir) ;
- dans un délai maximum d'un mois pour les sauvegardes (incrémentales, complètes… réalisées à fréquence donnée).

Recommandation 6 : L'établissement garantit la pérennité du stockage, conformément aux durées de conservation définies ci-dessus.

Recommandation 7 : L'établissement rend accessible, sans surcoût, un outil permettant aux étudiants, de récupérer l'intégralité du contenu de leur coffre-fort de façon simple, sans manipulation complexe ou répétitive, et dans un format électronique structuré et couramment utilisé, afin de faciliter le changement de fournisseur, et ce sans collecter d'informations confidentielles (telles que les identifiants bancaires, les mots de passe de service en ligne, etc.).

Recommandation 8 : L'établissement informe au préalable les étudiants :

- de l'identité de l'opérateur du service de coffre-fort numérique et de celle du fournisseur du service;
- de la ou des finalité(s) poursuivie(s) ;
- de l'absence de destinataire des données conservées, incluant les documents stockés et leurs métadonnées ;
- de tout transfert de données à caractère personnel envisagés si l'hébergement n'est pas assurer sur le territoire, en indiquant si cet État, sur la base de sa propre législation, pourrait effectuer des demandes visant à accéder directement aux données conservées ;
- des droits dont disposent les personnes concernées sur leurs données à caractère personnel et les modalités d'exercice de ses droits ;
- de la possibilité de mandater des personnes (par exemple pour permettre à l'utilisateur de récupérer ses données en cas de perte de sa clef, ou à ses ayants droits en cas de décès) ;
- du type d'espace mis à leur disposition et de ses conditions d'utilisation associées ;
- des mécanismes techniques utilisés, notamment les mécanismes de chiffrement ;
- de la politique de confidentialité ;
- de l'existence et les modalités de mise en œuvre des garanties de bon fonctionnement ;
- des modalités de résiliation du service et de récupération des données stockées ;
- en cas d'offre de service associé de récupération de documents auprès de services tiers, des conséquences de l'utilisation par l'établissement des identifiants et mots de passe des étudiants pour se connecter en leur nom à ces services ;
- de l'identité du délégué à la protection des données.

L'ensemble de ces informations sont également mises à disposition en ligne et, le cas échéant, mises à jour.

Recommandation 9 : Le service de coffre-fort numérique fait l'objet d'une analyse d'impact sur la vie privée, révisée au moins tous les trois ans.

Recommandation 10 : Le service de coffre-fort numérique intègre des outils permettant de bloquer des connexions faites par des robots et de retarder et/ou de bloquer les connexions illégitimes faites par des personnes.

Recommandation 11 : Le service de coffre-fort numérique intègre des mesures visant à garantir l'intégrité, la disponibilité des données (centre de stockage redondant, sauvegardes régulières…) et l'exactitude de l'origine des données et des documents stockés. L'établissement s'assure des garanties en termes d'indemnisation des étudiants en cas d'ineffectivité de ces mesures (par exemple en souscrivant à une assurance dans le but de couvrir les dommages relatifs à ses engagements).

Recommandation 12 : Le service de coffre-fort numérique intègre des fonctions de traçabilité permettant aux étudiants de consulter l'activité récente sur leur coffre-fort (par exemple en journalisant et en horodatant les réussites et échecs de connexion, l'adresse IP et le protocole utilisé, ainsi que les opérations effectuées sur les répertoires et les fichiers, l'utilisateur ayant effectué une opération, l'objet sur lequel une opération est effectuée et la nature de l'opération effectuée). Les durées de conservation de ces données de traçabilité constituent une mention obligatoire du contrat de fourniture de service de coffre-fort électronique

Recommandation 13 : Le service de coffre-fort numérique fait l'objet d'une vérification indépendante (par exemple par un auditeur externe, par un service de contrôle interne…) de l'effectivité et de l'efficacité des mesures choisies, au moins une fois tous les trois ans, et le cas échéant des mesures correctives.

Recommandation 14 : L'établissement procède à une notification à l'étudiant en cas d'accès à ses données par un tiers non mandaté par l'étudiant, même si ces données sont chiffrées.

Recommandation 15 : Le service de coffre-fort numérique intègre une fonction de chiffrement / déchiffrement des données conservées, incluant les documents stockés et leurs métadonnées.

Recommandation 16 : Le service de coffre-fort numérique intègre une fonction qui facilite la sauvegarde et la récupération des clefs de chiffrement/déchiffrement pour permettre à l'étudiant de continuer à accéder à ses données en cas de perte de ses clefs, par exemple avec la gestion de questions et de réponses secrètes.

Recommandation 17 : Le service de coffre-fort numérique intègre une fonction de chiffrement de tous les transferts d'informations vers et depuis le coffre-fort. Cette fonction est conforme aux règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques du référentiel général de sécurité de l'Agence nationale de sécurité des systèmes d'information.

Recommandation 18 : Le service de coffre-fort numérique met en œuvre des mécanismes d'authentification pour :

- les étudiants;
- les personnes physiques spécialement mandatées par ces derniers ;
- les tiers auxquels les étudiants ont recours pour importer des données depuis un espace de dépôt vers le coffre ;
- ainsi que les administrateurs informatiques pour la seule gestion du coffre.

Recommandation 19 : Le service de coffre-fort numérique permet à l'étudiant d'activer un mécanisme d'authentification robuste sans surcoût (mots de passe à usage unique, envoi de codes par SMS…). Il assure que l'étudiant, et les personnes physiques spécialement mandatées par ce dernier, sont authentifiés par le serveur hébergeant les données. Tous ces mécanismes sont conformes aux règles et recommandations du référentiel général de sécurité de l'Agence nationale de sécurité des systèmes d'information. Si l'authentification comprend l'utilisation de mots de passe, ces règles font l'objet d'une information des étudiants (affichage du niveau de sécurité du mot de passe choisi par exemple) et d'un contrôle (système de blocage si insuffisant).

Recommandation 20 : Les documents émis par l'établissement et placés dans le coffre-fort numérique sont signés numériquement, permettant ainsi à l'étudiant de prouver l'authenticité des documents.

2.6. Service de géolocalisation au sein du campus universitaire

Les étudiants – et dans une moindre mesure les personnels – sont maintenant largement équipés de terminaux mobiles depuis lesquels ils attendent désormais d'accéder aux informations ou aux outils (compatibles) des établissements d'enseignement supérieur.

Les étudiants et les personnels détenant un smartphone peuvent bénéficier d'un service de géolocalisation pour les orienter vers les différents sites et équipements du campus universitaire (bibliothèque, restaurant universitaire, sandwicherie, équipements sportifs… les plus proches) et leur indiquer le taux d'occupation ou trafic correspondant.

Le service est mis à disposition à partir d'applications mobiles dont le développement est assuré par des sociétés privées tiers ou par l'établissement d'enseignement supérieur lui-même, lorsque la conception d'applications pour les terminaux mobiles est dans le projet de l'établissement et que la compétence existe.

Responsables de traitement concernés

- Etablissements d'enseignement supérieur

Services chargés de la mise en œuvre :

- Tous les services correspondant aux différents sites et équipements (exemples : bibliothèque, cafétéria…)
- Prestataires de services tiers des établissements pourvoyeurs de service – devant se conformer à l'article 28 du Règlement Général sur la Protection des Données. (Pour en savoir plus voir le guide du sous-traitant de CNIL)

Finalité

Le traitement de données personnelles a pour finalité la facilitation de l'expérience étudiant sur le campus par sa géolocalisation au sein du campus lui permettant d'optimiser ses temps de déplacements en fonction de ses besoins.

Fondement juridique

Le service est proposé à titre facultatif à chaque étudiant ou membre du personnel qui le souhaite, sur la base de son consentement.

Le refus de consentement de l'étudiant ou du membre du personnel ne lui permet pas de bénéficier de ce service.

Données personnelles concernées

Données concernant les étudiants :

- Civilité, noms, prénoms, identifiant national étudiant (INE)
- Données d'ouverture d'un compte ENT /plateforme : identifiant, mot de passe
- Données de géolocalisation

Données concernant les personnels :

- Civilité, noms, prénoms
- Données d'ouverture d'un compte ENT /plateforme : identifiant, mot de passe
- Données de géolocalisation

Durée de conservation des données

Les informations relatives aux déplacements des individus ne sont pas conservées.

Lorsqu'un étudiant souhaite savoir où se trouve le restaurant universitaire le plus proche, il n'est pas nécessaire d'enregistrer sa géolocalisation, cette dernière permettant uniquement l'exécution de la requête.

Si l'établissement souhaite agréger les données de géolocalisation pour l'analyse des zones du campus les plus fréquentées, les données collectées permettent uniquement le comptage quotidien des étudiants ayant fréquenté les zones ciblées et sont purgées chaque soir.

Destinataires des données

- Etudiants
- Personnels enseignants
- Personnels administratifs
- Prestataires de services tiers des établissements pourvoyeurs de service – devant se conformer à l'article 28 du Règlement Général sur la Protection des Données. (Pour en savoir plus voir le guide du sous-traitant de CNIL)

Sont destinataires de données statistiques :

- Tous les services correspondant aux différents sites et équipements (exemples : bibliothèque, cafétéria…)

Mesures de sécurité et de confidentialité

Partage des données du smartphone

Aucune donnée non pertinente du smartphone ne devra être collectée (exemple : la liste des contacts). Le responsable de traitement devra s'assurer qu'aucune donnée sans lien avec le déplacement de l'individu sur le campus n'est collectée (un contrôle sur ce point devra être effectué à chaque mise à jour dans le cas où cette application est mise à disposition par un prestataire tiers des établissements pourvoyeurs de service).

L'ensemble des données privées d'identification liées à l'ENT permettant le suivi des déplacements d'un individu devront faire l'objet d'un hashage.

Ce système d'empreinte permettra à l'établissement de répondre à la finalité prédéterminée sans être en mesure d'identifier de manière directe le bénéficiaire du service.

2.7. Votes en ligne dans les établissements

Description du service

Le développement des outils numériques donne aujourd'hui la possibilité de mettre en place des dispositifs de votes électronique en ligne qui peuvent être utilisés pour l'élection des représentants du personnel et des usagers au sein de différentes instances des établissements. Il s'agit donc d'élections officielles qui nécessitent des plateformes sécurisées pour la gestion des questionnaires et des données associées tout en garantissant l'anonymat des utilisateurs.

L'objectif principal est de réaliser les scrutins par voie électronique. Il s'agit notamment de récupérer le(s) choix des électeurs tout en conservant la liste des personnes ayant voté.

Responsables de traitement concernés

- Etablissements d'enseignement supérieur

Services chargés de la mise en œuvre

- Services centraux et juridiques des établissements.
- Prestataires de services tiers des établissements pourvoyeurs de service

Finalités

Réaliser les scrutins par voie électronique.

Fondement juridique

Le service est proposé à titre facultatif à chaque étudiant qui le souhaite, sur la base de son consentement.

Le refus de consentement de l'étudiant ne lui permet pas de bénéficier de ce service. À tout moment en cours d'année, l'étudiant peut retirer son consentement.

Données personnelles concernées

La prise en compte du vote électronique nécessite de mémoriser :

- État-civil, identité, données d'identification
- Données de connexion (adresses IP, journaux d'événements...)

De manière complètement décorrélées pour garantir l'anonymat

- Les choix du votant

Durée de conservation des données

Conservation limitée : 1 à 3 mois, le temps de valider les élections ou de répondre à d'éventuel contentieux.

Destinataires des données

- Etudiants
- Enseignants
- Chercheurs
- Personnels administratifs
- ou plus généralement toute personne des établissements devant exprimer leur voix

Recommandation CNIL :

La recommandation n° 2010-371 du 21 octobre 2010 : vote électronique (MAJ de la recommandation 03-036 du 1er juillet 2003)

Mesures de sécurité et de confidentialité

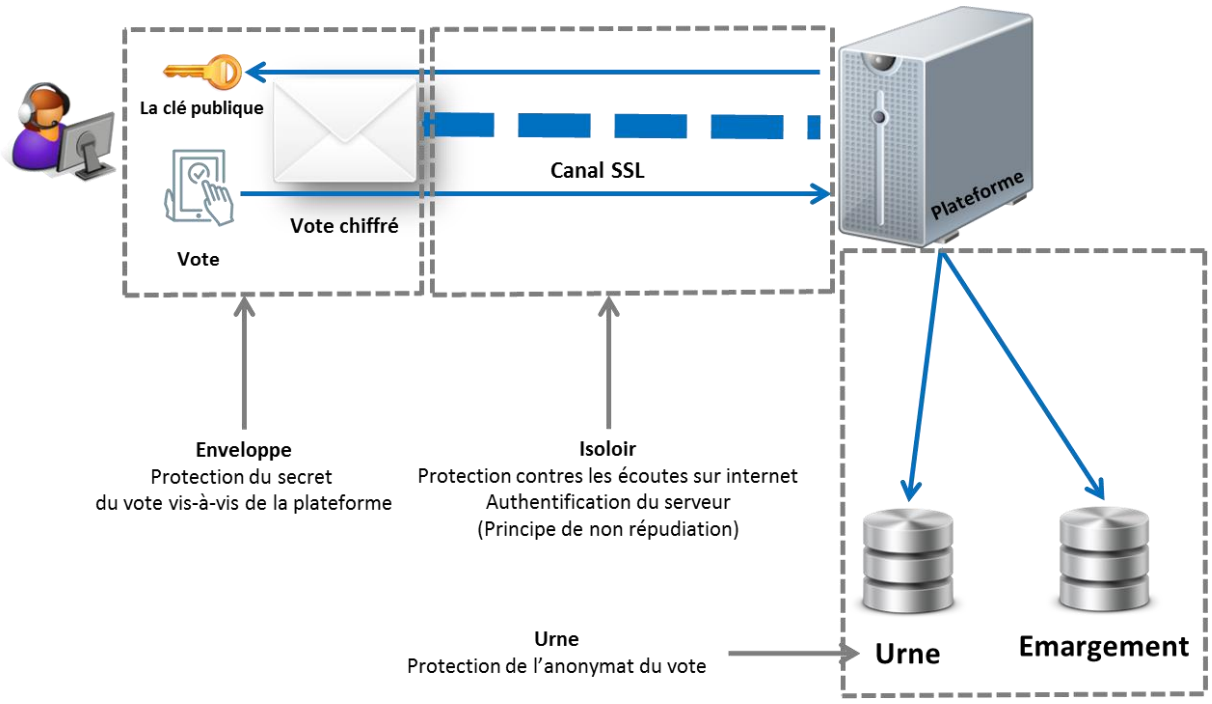
Au vu de la sensibilité des données traitées dans le cadre de ce service, des mesures techniques et organisationnelles appropriées doivent être mises en place afin de garantir un niveau de sécurité adapté aux risques.

L'état de l'art attendu souhaiterait que l'ensemble des recommandations ci-dessous soient prises compte :

- L'expertise indépendante.
- L'usage des données des électeurs aux seules fins du scrutin.
- La sécurité de l'envoi des moyens d'authentification.
- Le chiffrement des données (confidentialité).
- La séparation des données nominatives et des votes (émargement / urne).

- L'horodatage de la liste d'émargement.
- L'absence d'horodatage de l'urne.
- La sécurité informatique (logiciel, infrastructure, procédures).
- Le scellement du dispositif de vote électronique y compris du fichier des électeurs.
- L'existence d'une solution de secours.
- La localisation du système de vote sur le territoire national.
- Une confidentialité des données opposable aux prestataires techniques.
- Le test préalable du système de vote.
- L'information des électeurs.
- Une procédure publique de génération des clés de dépouillement.
- Le partage de plusieurs clés de dépouillement au sein du bureau de vote.
- L'authentification des électeurs.
- La possibilité de voter blanc, de revenir sur son choix initial avant validation, de conserver une trace de la confirmation du vote.
- Le chiffrement de bout en bout du bulletin de vote.
- L'impossibilité d'obtenir un décompte partiel durant le scrutin.
- Une cérémonie publique de dépouillement.
- La conservation des données jusqu'à l'épuisement des délais de recours contentieux.

Synoptique de l'architecture



Les 5 points d'attention

1. Réaliser une expertise INDEPENDANTE

« Indépendance » du prestataire.

- Recommandation sur les critères de sélection

Objectifs :

- Vérifier la conformité du système à vos demandes
- Vérifier l'application des recommandations de la CNIL
- Rassurer les organisateurs du vote

Périmètre :

- Le système informatique et sa documentation et le « code source »
- Avant, pendant et après le scrutin
- Mesures techniques et organisationnelles

Résultat :

- Un rapport de l'expert remis au responsable de traitement

2. Garantir l'intégrité du dispositif de vote

- Vérifier l'intégrité du logiciel du système de vote
- Le système de vote installé le jour du vote est bien celui qui a été expertisé.
- Le système de vote n'a pas été modifié pendant le vote, contrôle d'intégrité avec un calcul d'empreinte (hash)
- L'urne est vide au début du vote et ne peut être modifiée que par l'ajout d'un bulletin légitime
- Imposer le contrôle effectif du « bureau de vote » sur le déroulement du scrutin.
- Une documentation claire et disponible au bureau de vote
- Un processus d'alerte automatique prévient le bureau de vote avant toute intervention sur le système de vote par le prestataire.
- Vérifier la sécurité physique et logique du système de vote
- Locaux sécurisés et machines scellées.
- Accès par le réseau protégé (firewall)

3. Garantir l'anonymat du vote

Vérifier qu'aucun lien entre le bulletin de vote et l'électeur ne puisse être établi :

- Par une absence de séparation stricte de l'urne et de la liste d'émargement
- Par une inclusion d'informations « identifiantes » dans le bulletin
- Par déduction chronologique, si la liste d'émargement est horodatée ou si les bulletins sont enregistrés dans un ordre d'arrivé
- Par des traces diverses (Journaux, traces, …)

4. Assurer un chiffrement de bout en bout du bulletin

La bonne approche :

- Le bulletin est rempli dans le navigateur de l'électeur
- Le bulletin est chiffré dans le navigateur (exemple : applet)
- Le bulletin est transmis au serveur de vote
- Le bulletin est chiffré et envoyé dans un canal réseau (SSL)
- Le bulletin est extrait et déchiffré du canal réseau (SSL) sur le serveur
- Le bulletin chiffré est stocké directement dans l'urne

5. Protéger les éléments secrets du système de vote

Protéger les identifiants/mots de passe des électeurs :

- Lors de leur envoi initial
- Lors des procédures d'urgence (perte ou vol de mot de passe)
- Privilégier des mécanismes « défi / réponse » ou des certificats

Protéger la clé de déchiffrement du vote :

- Elle est générée avant le vote
- Elle est partagée en 3 parties dont deux au moins sont nécessaires pour reconstituer la clé.
- Chaque partie est détenue par un membre distinct du bureau de vote
- Idée : stockage de chaque partie dans une enveloppe sécurisée ou un support protégé par mot de passe

Le contrôle du vote doit être entre les mains des organisateurs du vote et non pas entre les mains du prestataire technique.

2.8. Valorisation des données collectées

Description du service

L'établissement d'enseignement supérieur dispose de nombreuses données liées aux étudiants dans son système d'information, et notamment l'adresse mail des étudiants.

Le service de valorisation des données a pour objectif de permettre à l'établissement d'enseignement de proposer des offres promotionnelles mises en place par des partenaires commerciaux, à destination des étudiants (par exemple, l'organisation de campagnes marketing pour des partenaires commerciaux, exclusivement mises en œuvre par l'établissement d'enseignement supérieur).

Le service est mis à la disposition des étudiants disposant d'un compte ENT.

Responsables de traitement concernés

- Etablissements d'enseignement supérieur

Services chargés de la mise en œuvre

- Service d'aide à l'insertion professionnelle
- Equipes pédagogiques
- Services d'appui à la pédagogie numérique
- Services universitaires de pédagogie

Finalités

Proposition d'offres promotionnelles mises en place par des partenaires commerciaux, à destination des étudiants.

Fondement juridique

Le service est proposé à titre facultatif à chaque étudiant qui le souhaite, sur la base de son consentement.

Le refus de consentement de l'étudiant ne lui permet pas de bénéficier de ce service. À tout moment en cours d'année, l'étudiant peut retirer son consentement.

Données personnelles concernées

Données concernant l'étudiant :

- Etat civil : noms, prénoms, sexe, civilité, date et lieu de naissance
- Adresse mail
- Données d'ouverture d'un compte ENT : identifiant, mot de passe

Durée de conservation des données

Au terme du cursus de l'étudiant au sein de l'établissement d'enseignement supérieur, les données à caractère personnel le concernant sont supprimées.

Destinataires des données

- Personnels strictement habilités des établissements de l'enseignement supérieur chargés de la mise en œuvre du service de valorisation des données.

Mesures de sécurité et de confidentialité

Au vu de la sensibilité des données traitées dans le cadre de ce service, des mesures techniques et organisationnelles appropriées doivent être mises en place afin de garantir un niveau de sécurité adapté aux risques.

Mesures organisationnelles

L'établissement d'enseignement supérieur intervient nécessairement en qualité d'intermédiaire au titre de la mise en œuvre des opérations promotionnelles. En aucun cas, les données à caractère personnel relatives aux étudiants ne sont transmises à un partenaire commercial.

2.9. Questionnaires en ligne à des fins pédagogiques

Description du service

Le développement des outils numériques au sein des établissements (ENT, plateforme pédagogique…) permet désormais de mettre en place facilement et rapidement des questionnaires et votes en ligne :

- soit dans un cadre pédagogique : évaluation des connaissances acquises, avis sur les enseignements ;
- soit afin d'établir des enquêtes de satisfaction ou sur les besoins auprès des étudiants ou des personnels des établissements. Si certains usages se contentent de questionnaires anonymes, d'autres cependant nécessitent de conserver l'identité des utilisateurs.

Le service est mis à la disposition des étudiants disposant d'un compte ENT ou via une plateforme indépendante.

Responsables de traitement concernés

- Etablissements d'enseignement supérieur

Services chargés de la mise en œuvre

- Service d'aide à l'insertion professionnelle
- Equipes pédagogiques
- Services d'appui à la pédagogie numérique
- Services universitaires de pédagogie
- Prestataires de services tiers des établissements pourvoyeurs de service – devant se conformer à l'article 28 du Règlement Général sur la Protection des Données. (Pour en savoir plus voir le guide du sous-traitant de CNIL)

Finalités

Finalité 1 : Evaluation des étudiants à des fins pédagogiques, par le biais d'un support numérique

Finalité 2 : Mise en œuvre d'enquêtes de satisfactions ou à vocation statistiques sur les usages ou les besoins

Fondement juridique

L'évaluation des étudiants à des fins pédagogiques, par le biais d'un support numérique (finalité 1) correspond à la mission d'intérêt public de l'établissement d'enseignement supérieur.

La mise en œuvre d'enquêtes de satisfactions ou à vocation statistiques sur les usages ou les besoins (finalité 2) est proposée à titre facultatif à chaque étudiant qui le souhaite, sur la base de son consentement.

Le refus de consentement de l'étudiant ne lui permet pas de bénéficier de ce service. À tout moment en cours d'année, l'étudiant peut retirer son consentement.

Données personnelles concernées

Concernant les données relatives aux évaluations pédagogiques :

- Données d'identification (nom, prénom, numéro d'étudiants…)
- Données d'ouverture d'un compte ENT /plateforme : identifiant, mot de passe
- Opinions personnelles, selon les réponses pouvant être apportées par l'étudiant aux questions posées, avec un facteur non négligeable de sérendipité[4]

Concernant les données relatives aux questionnaires :

- Données sur la vie personnelle, professionnelle, opinions personnelles diverses, selon les réponses pouvant être apportées par l'étudiant aux questions posées, avec un facteur non négligeable de sérendipité

Durée de conservation des données

Concernant les données relatives aux évaluations pédagogiques :

Au terme du cursus de l'étudiant au sein de l'établissement d'enseignement supérieur, les données à caractère personnel le concernant sont supprimées.

Concernant les données à caractère personnel collectées dans le cadre des questionnaires et sondages (non anonymes) sont conservées pour une durée de 1 à 3 mois.

[4] La notion de sérendipité désigne le fait de collecter des données, sans que ces dernières n'aient été requises ni anticipées.

Destinataires des données

- Personnels enseignants
- Personnels administratifs

Mesures de sécurité et de confidentialité

Au vu de la sensibilité des données traitées dans le cadre de ce service, des mesures techniques et organisationnelles appropriées doivent être mises en place afin de garantir un niveau de sécurité adapté aux risques.

Mesures organisationnelles

Un document formalisant la gestion des habilitations permettant de consulter les réponses aux différents types de questionnaire en fonction de la matière concernée et de l'équipe pédagogique en charge des étudiants concernés afin d'assurer la confidentialité des réponses afin d'exclure tout accès illégitime aux réponses effectuées.

Un journal permettant la traçabilité des accès ainsi que l'historique des actions effectuées, devra permettre d'effectuer des analyses a posteriori.

Chaque jeu de réponse devra faire l'objet d'une empreinte à la validation du questionnaire par l'étudiant, afin d'assurer l'intégrité des réponses a posteriori, pour exclure toute altération des réponses effectuées.

L'ensemble des questionnaires devront également être redondé sur une sauvegarde physiquement distincte, pour assurer la disponibilité.

2.10. Questionnaires en ligne à des fins de recherche

Des activités de recherche entrant dans le périmètre de recherche du Ministère de l'enseignement supérieur, de la recherche et de l'innovation peuvent être menées par l'établissement d'enseignement supérieur à partir de questionnaires en ligne. En fonction des objectifs de la recherche poursuivie par l'établissement, des données personnelles et des opinions peuvent être demandés aux étudiants interrogés.

Le service est mis à la disposition des étudiants disposant d'un compte ENT ou via une plateforme indépendante.

Responsables de traitement concernés

- Etablissements d'enseignement supérieur

Services chargés de la mise en œuvre

- Les services internes chargés du déploiement des questionnaires
- Prestataires de services tiers des établissements pourvoyeurs de service – devant se conformer à l'article 28 du Règlement Général sur la Protection des Données. (Pour en savoir plus voir le guide du sous-traitant de CNIL)

Fondement juridique

Le service est proposé à titre facultatif à chaque étudiant qui le souhaite, sur la base de son consentement.

Le refus de consentement de l'étudiant ne lui permet pas de bénéficier de ce service. À tout moment en cours d'année, l'étudiant peut retirer son consentement.

Finalités

Analyse des données des questionnaires dans le cadre des activités de recherche de l'établissement d'enseignement supérieur

Données personnelles concernées

- Données d'identification (nom, prénom, numéro d'étudiants…)
- Données d'ouverture d'un compte ENT /plateforme : identifiant, mot de passe
- Données de connexion,
- Information sur la vie personnelle
- Informations d'ordre économique
- Opinions personnelles pouvant conduire à la collecte de données sensibles à l'exception des données de santé, biométriques et génétiques, selon les réponses pouvant être apportées par l'étudiant aux questions posées, avec un facteur non négligeable de sérendipité[5]

Durée de conservation des données

Les données à caractère personnel sont collectées à des fins de recherche sont conservées pour la durée du cursus de l'étudiant au sein de l'établissement d'enseignement supérieur puis sont anonymisées.

Destinataires des données

- Personnels enseignants
- Personnels administratifs

Mesures de sécurité et de confidentialité

Au vu de la sensibilité des données traitées dans le cadre de ce service, des mesures techniques et organisationnelles appropriées doivent être mises en place afin de garantir un niveau de sécurité adapté aux risques.

Mesures organisationnelles

Un document formalisant la gestion des habilitations permettant de consulter les réponses aux différents types de questionnaire en fonction de la matière concernée et de l'équipe pédagogique en charge des étudiants concernés afin d'assurer la confidentialité des réponses afin d'exclure tout accès illégitime aux réponses effectuées.

Un journal permettant la traçabilité des accès ainsi que l'historique des actions effectuées, devra permettre d'effectuer des analyses a posteriori.

Chaque jeu de réponse devra faire l'objet d'une empreinte à la validation du questionnaire par l'étudiant, afin d'assurer l'intégrité des réponses a posteriori, pour exclure toute altération des réponses effectuées.

L'ensemble des questionnaires devront également être redondé sur une sauvegarde physiquement distincte, pour assurer la disponibilité.

[5] La notion de sérendipité désigne le fait de collecter des données, sans que ces dernières n'aient été requises ni anticipées.

2.11. Système d'alerte et d'information des populations universitaires

Dans le cadre des projets de modernisation des parcs d'autocommutateurs téléphoniques, les DSI d'établissement de l'ESR étudient depuis un certain temps, la possibilité d'acquérir et d'utiliser des plateformes d'envoi massif de SMS/mail à destination des téléphones mobiles/des adresses mails des agents, enseignants et étudiants. (Voir https://www.esup-portail.org/wiki/display/PROJSMSU/ESUP-SMS-U)

Les DSI disposent en partie des numéros de téléphone mobile personnel et des adresses mails des agents, des enseignants et des étudiants.

Les DSI souhaitent être en mesure de pouvoir s'appuyer sur des bonnes pratiques pour leur permettre d'utiliser ces numéros/ces adresses mail pour la diffusion de SMS/mail d'alerte ou d'information, dans le respect des règles relatives à la protection des données à caractère personnel.

Responsables de traitement concernés

- Etablissements d'enseignement supérieur

Services chargés de la mise en œuvre

- Tous les services internes en charge de la communication
- Prestataires de services tiers des établissements pourvoyeurs de service – devant se conformer à l'article 28 du Règlement Général sur la Protection des Données. (Pour en savoir plus voir le guide du sous-traitant de CNIL)

Finalités

Finalité 1 : Information des agents, enseignants et étudiants par SMS/mail en lien avec la vie de l'établissement d'enseignement supérieur.

Finalité 2 : Alerte des agents, enseignants et étudiants par SMS/mail en lien avec leur sécurité physique.

Fondement juridique

Le service d'information est proposé à titre facultatif à chaque personne concernée qui le souhaite, sur la base de son consentement (finalité 1)

Le refus de consentement de la personne concernée ne lui permet pas de bénéficier de ce service d'information. À tout moment, elle peut retirer son consentement.

Le service d'alerte repose sur la sauvegarde de la vie humaine, dans des situations d'urgence (finalité 2).

Données personnelles concernées

- Données d'identification (nom, prénom, numéro de téléphone portable, adresse mail)
- Données d'ouverture d'un compte ENT /plateforme : identifiant, mot de passe

Durée de conservation des données

L'ensemble des informations inhérentes à ce service est conservé pour la durée du cursus de l'étudiant ou de la relation contractuelle du personnel avec l'établissement d'enseignement supérieur puis est supprimé.

Destinataires des données

- Tous les services internes en charge de la communication

Mesures de sécurité et de confidentialité

Au vu de la sensibilité des données traitées dans le cadre de ce service, des mesures techniques et organisationnelles appropriées doivent être mises en place afin de garantir un niveau de sécurité adapté aux risques.

www.infhotep.com