Conférence Permanente des chargé·e·s de mission Egalité et Diversité

Guide conçu par
un groupe de travail interne à la CPED

Gestion des données sensibles

Recommandations de gestion et d'archivage des données liées aux signalements de violences sexuelles et sexistes, de harcèlement et de discriminations dans le cadre des dispositifs des établissements d'enseignement supérieur et de recherche

Première édition - 2023

Edito

Cinq années se sont écoulées, depuis la circulaire du 9 mars 2018 relative à la lutte contre les violences sexuelles et sexistes dans la fonction publique. Aujourd'hui, tous les établissements ont posé les principes de la prévention et des procédures liées au traitement des situations de Violences Sexistes et Sexuelles (VSS), de harcèlement et de discrimination. La CPED a, depuis cinq ans, multiplié ses actions sur le sujet des VSS, que ce soit à travers la formation, la communication, l'accompagnement des établissements, les enquêtes, la participation à et/ou la mise en place d'espaces d'échanges nationaux et internationaux. La prévention et le traitement des VSS reste un sujet majeur de préoccupation dans nos établissements. Des questions se posent quotidiennement en lien avec les enjeux de communication, de formation des étudiant·es et des personnels, de gestion des données, de procédures, de gestion des situations après sanction, de l'accompagnement des personnes ou encore du partage d'informations entre établissements.

Les rencontres de la CPED, organisées par l'Université d'Orléans en juin 2022, ont mené au constat collectif de difficultés liées à la gestion des données sensibles générées par nos dispositifs de signalement. Il émane, alors, la proposition de créer un groupe de travail sur le thème de la gestion et de l'archivage des données sensibles. Il est proposé à travers ce livrable un cadre et une méthode pour aider les établissements à établir leurs modalités et délais de conservation. Il définit d'abord « les données sensibles », avant d'aborder les ressources et réglementations existantes puis de proposer une méthode pour déterminer les durées de conservation et le devenir des documents. Enfin, le groupe de travail a souhaité mettre en lumière un certain nombre de bonnes pratiques et proposer des perspectives de travail.

Nous aimerions remercier très sincèrement les participant·es à ce groupe de travail pour leur expertise, leur assiduité, leur envie de partage et leur engagement au sein de la CPED et de leur établissement respectif sur cette question. Cela nous a permis de constater encore une fois la force du collectif pour élaborer des pistes de résolutions face à une problématique. Nous espérons que ce guide vous permettra de gagner du temps et surtout d'améliorer le fonctionnement de vos dispositifs. Nous avons hâte de vous retrouver dans un prochain groupe de travail.

Véronique Van De Bor, vice-présidente de la CPED en charge de la formation.
Aude Stheneur, cheffe de projet de la CPED.

I. Contexte

A. Les dispositifs de signalement

- **La création des dispositifs**

La circulaire du 9 mars 2018 relative à la lutte contre les violences sexuelles et sexistes (VSS) dans la fonction publique impose aux employeurs publics d'instaurer un plan de prévention et de traitement des VSS autour de trois axes principaux: prévenir, traiter et sanctionner tous faits de VSS à travers la mise en place de dispositifs de prévention, de signalement, de traitement et de suivi des VSS. L'article 80 de la loi sur la transformation de la fonction publique (LFTP) du 6 août 2019 prévoit, la mise en place obligatoire d'un dispositif au sein de l'ensemble des administrations et ajoute à son périmètre d'actions l'ensemble des discriminations et le harcèlement moral. Son fonctionnement et son périmètre sont précisés dans le décret n° 2020-256 du 13 mars 2020 relatif au dispositif de signalement, ainsi que l'arrêté du 17 mars 2021 portant application.

En pratique, les dispositifs de signalement doivent participer à la prévention, proposer une écoute, recueillir les signalements, mettre en place des moyens d'accompagnement et d'orientation, établir des procédures de traitement des situations, élaborer un bilan annuel et favoriser l'articulation avec les procédures disciplinaires. Ils doivent également assurer la confidentialité des données et des personnes, garantir la neutralité et l'impartialité ainsi que l'indépendance des dispositifs et le traitement rapide des signalements.

- **Des dispositifs différents en fonction des établissements**

Le mode de fonctionnement est à l'appréciation des établissements d'enseignement supérieur. Bien qu'ils soient tous tenus de mettre en place un dispositif, sa mise en pratique peut être très diverse et doit s'adapter aux spécificités de chaque établissement. Il n'existe pas de dispositif unique qui puisse fonctionner pour tous les établissements.

Certains établissements ont choisi d'internaliser leur dispositif, d'autres de l'externaliser complètement ou partiellement, en faisant, par exemple, appelle à un·e prestataire spécialisé·e dans la qualification juridique des faits, un partenaire associatif spécialisé dans l'écoute et l'accompagnement ou de mutualiser leurs

dispositifs avec d'autres établissements de l'ESR. Ainsi, chaque établissement pourra se saisir de ce guide pour l'adapter à son dispositif spécifique.

B. Enjeux en matière de gestion et archivage des données sensibles

En lien avec le déploiement des dispositifs d'écoute et de signalement, sont nées des interrogations concernant la gestion des données sensibles afférentes.

Quels moyens et durées de conservation pour les dossiers et documents qui contiennent des données sensibles ?

Comment garantir le droit des personnes tout en garantissant les besoins des dispositifs et des différentes procédures (signalement, enquête interne, section disciplinaire, procédure pénale) ?

Plusieurs établissements ont fait remonter la nécessité de définir un cadre juridique et réglementaire qui s'applique aux documents comportant des données sensibles issus des dispositifs de signalement des violences sexistes et sexuelles. En effet, il n'existe aujourd'hui aucun texte décrivant le temps de conservation de ces données ni le cadre de leur utilisation.

Pourtant, la question des données personnelles est essentielle : la confiance et le respect de la vie privée des personnes qui mobilisent les dispositifs sont en jeu.

Les conséquences de l'absence de référentiel sont doubles : premièrement dans de nombreux établissements, il existe un manque de transparence sur la conservation et l'archivage des données ; deuxièmement, il existe un manque d'harmonisation des pratiques entre tous les services concernés, au sein des établissements mais également avec les partenaires externes impliqués dans le fonctionnement du dispositif.

En matière de gestion et d'archivage des données sensibles, il est essentiel que l'établissement soit capable de :

- Retrouver l'information
- Garantir le respect des droits des personnes (victime comme agresseur présumé)
- Sécuriser juridiquement son dispositif de signalement et l'archivage des ses données

- Améliorer la confiance dans les procédures

C. Conception du guide

- **La CPED**

La Conférence Permanente des chargé·es de mission Egalité et Diversité, ou mission assimilée, des établissements d'enseignement supérieur et de recherche – CPED – s'est constituée en janvier 2011. Elle réunit les établissements représentés par leurs chargé·es de mission, référent·es ou vice-président·es égalité-diversité et les membres de leurs équipes autour de la mise en oeuvre de politiques visant l'égalité entre les femmes et les hommes, le respect de la diversité et la lutte contre les violences sexistes et sexuelles et les discriminations, qu'elles concernent le personnel ou les étudiant·es.

Suite au partage de difficultés communes par les établissements, la CPED constitue des groupes de travail afin d'échanger sur les enjeux identifiés et de produire des ressources mutualisables.

- **Fonctionnement du groupe de travail**

Suite aux échanges menés lors des rencontres de la CPED à Orléans en juin 2022, le groupe de travail (GT) concernant la gestion des données sensibles a été créé le 26 octobre 2022. Il était composé de chargé·es de mission égalité-diversité, ou mission assimilée, d'archivistes, de délégué·es à la protection des données, d'une référente déontologue et juriste. La liste des participant·es est à retrouver en annexe. Le GT s'est réuni une fois par mois jusqu'au 6 juin 2023.

Les membres du GT ont échangé sur les situations de leurs établissements en termes de VSS et partagé des retours d'expériences et des bonnes pratiques. Ils et elles ont mené des recherches collaboratives sur les documents concernés par les données sensibles, les cadres juridiques et réglementaires pouvant s'appliquer et les enjeux des décisions concernant les méthodes et durées de conservation des documents. Les membres du GT ont conjointement produit ce guide, contenant les obligations et recommandations en matière de gestion des données sensibles dans les dossiers issus des procédures de lutte contre les VSS et les discriminations dans l'Enseignement Supérieur et la Recherche.

II. Les documents qui contiennent des données sensibles

Selon la CNIL (voir CNIL, p.12), les données sensibles sont définies comme "*des informations qui révèlent la prétendue origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique*." Dans nos dispositifs de signalement, nous manipulons très fréquemment des informations sur les comportements sexuels d'individus identifiés, et/ou des informations concernant la santé des personnes que nous pouvons, selon la définition de la CNIL, considérer comme des données sensibles.

A quels documents faisons-nous référence lorsque nous parlons de données sensibles ?
Le groupe de travail a listé les documents issus des dispositifs d'écoute et de signalement contenant des données sensibles.

NB : Les documents de type "statistiques" ou "bilan" ne sont pas comptés comme données sensibles car ils sont anonymés.

A. Cellule / Dispositif

Typologie de document	**Descriptif et exemples**	**Utilisation**
Dossier de signalement qui déclenche le processus de traitement	- Plusieurs supports (physique, électronique) - Peut contenir par exemple : compte-rendu d'entretien, certificat médical, éléments probants écrits, photos, vidéos, enregistrement audio, fiche de signalement, plainte pénale, etc.	- Traitement du dossier de signalement (consultation du dossier pour lecture et analyse) - Orientation si besoin vers un autre dispositif - Transmission au service juridique après accord du signalant ou de la signalante

Rapport	Un compte-rendu d'entretien est rédigé à l'issu de chaque entretien, enrichi par le ou la signalante	Transmission au service juridique après accord du signalant ou de la signalante (rapport daté et signé)
Tableau de suivi des signalements	Tableau répertoriant les différents signalements, éventuellement les statuts des personnes et l'état d'avancement du traitement du signalement	Suivi des saisines et/ou des signalements en interne (ou en externe si demande du MESR par exemple)

B. Analyse / Enquête / Traitement

Typologie de document	**Descriptif et exemples**	**Utilisation**
Dossier d'enquête en vue d'une éventuelle procédure disciplinaire	Contient le dossier de signalement et le rapport (cf. tableau A), les PV d'audition et les éventuels nouveaux éléments apportés par les témoins directs ou indirects	Obligations légales, recours, réquisition judiciaire. Transmission éventuelle à la section disciplinaire
Rapport final de l'enquête préalable	Compte-rendu des membres de la commission d'enquête incluant éventuellement des recommandations	A destination du chef ou de la cheffe d'établissement. Permet de décider de la suite de la procédure par exemple la saisine ou non d'une commission disciplinaire
Registre des enquêtes internes préalables	Registre contenant le nombre de signalements, le suivi (dates et personnes ayant consulté les documents)	Suivi des enquêtes internes

C. Disciplinaire

Typologie de document	Descriptif	Utilisation
Dossier de procédure disciplinaire	Contient le dossier de signalement (cf. tableau A) et/ou le dossier d'enquête (cf. tableau B) et le rapport final d'enquête. Et si applicable, le signalement au procureur de la République.	- Dossier accessible aux membres de la section disciplinaire et au(x) mis en cause. - Réquisition en cas d'enquête pénale (uniquement sur demande)
Rapport d'examen	Document officiel qui rend décision de la procédure disciplinaire (anonymé ou non, selon la décision de la section disciplinaire)	- Document transmis au(x) mis en cause. - Affichage au sein de l'établissement - Réquisition en cas d'enquête pénale (uniquement sur demande)
Registre des décisions de la section disciplinaire	Registre contenant les décisions des sections disciplinaires.	Suivi des décisions de la section disciplinaire

D. Communication institutionnelle

Typologie de document	Descriptif et exemples	Utilisation
Communications par le président ou la présidente	Courriers envoyés par le président ou la présidente à destination du procureur de la république, ou informant des mesures conservatoires ou de la saisine de la commission d'enquête de la section disciplinaire ou de mise en demeure	Information des parties prenantes

III. Déterminer les durées de conservation et le devenir des documents

A. Cadres réglementaires et juridiques mobilisables[1]

Afin de déterminer les durées de conservation des données et le devenir des documents, il convient d'articuler plusieurs instruments juridiques principalement issus des instances et autorités compétentes qui animent la vie universitaire et les procédures de l'enseignement supérieur et de la recherche.

Ces références légales sont celles qui sont utilisées lors des procédures allant du signalement, à l'instruction jusqu'au jugement. Les dispositifs internes à un établissement dépendent de l'environnement juridique de l'enseignement supérieur et de la mission de service public. On y retrouve principalement des circulaires ministérielles, des normes et guides ainsi que des décrets d'application faisant suite à des réformes juridiques.

Cependant, outre les dispositifs et procédures internes, il est important de mesurer les besoins de conservation s'agissant de procédures de droit commun qui dépassent les compétences de l'établissement.

Ainsi, une instruction interne donnant lieu ou non à une sanction, peut tout à fait être poursuivie sur une échelle différente en dehors de l'établissement, avec par exemple le dépôt d'une plainte pénale. Les procédures pénales et disciplinaires sont distinctes et correspondent à des temporalités différentes. Néanmoins, les durées de conservation et le devenir des documents contenant des données sensibles doivent tenir compte des deux.

Les plaintes pénales amènent souvent à des enquêtes judiciaires menant à des réquisitions judiciaires (code de procédure pénale) de la part d'officier·es de police judiciaire ou de magistrat·es, impliquant une coopération de l'établissement.

Ce scénario implique de réfléchir à un format de conservation qui dépasse les besoins premiers de l'instruction menée par l'établissement. C'est pourquoi, pour déterminer une durée de conservation optimale, le jeu d'équilibre entre la vie privée des personnes concernées appelées tiers à la procédure, et la poursuite des obligations légales qui incombent à un établissement est primordiale. Pour ce faire,

[1] Les informations utilisées pour la rédaction de ce paragraphe ont été tirées des sites institutionnels des organismes et des autorités administratives compétentes : LegiFrance, Commission nationale de l'informatique et des libertés (CNIL), Service interministériel des archives de France (SIAF), ministère de l'Enseignement supérieur et de la Recherche, Commission d'accès aux documents administratifs (CADA), Défenseur des droits.

le présent chapitre a su référencer les instruments et instances juridiques clés, amenés par des années d'expériences et de convergences de pratiques de plusieurs établissements d'enseignement supérieur.

Cette liste non exhaustive, vous permettra d'identifier les textes potentiellement applicables aux dispositifs mis en œuvre au sein de votre institution.

- **Règlement général de protection des données (RGPD)**

Le RGPD est un texte réglementaire européen qui encadre le traitement des données de manière égalitaire sur tout le territoire de l'Union européenne (UE). Il est entré en application le 25 mai 2018.

Le RGPD s'inscrit dans la continuité de la loi française « Informatique et Libertés » de 1978, modifiée par la loi du 20 juin 2018 relative à la protection des données personnelles, établissant des règles sur la collecte et l'utilisation des données sur le territoire français. Il a été conçu autour de trois objectifs :

- renforcer les droits des personnes ;
- responsabiliser les acteurs et actrices traitant des données ;
- crédibiliser la régulation grâce à une coopération renforcée entre les autorités de protection des données.

- **LOI n° 2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique (1)**

La loi tend à poursuivre la démarche entreprise par la loi du 29 janvier 1993 relative à la prévention de la corruption et à la transparence de la vie économique et des procédures publiques ("loi Sapin"). Il s'appuie aussi sur les conclusions du rapport de Jean-Louis Nadal, président de la Haute Autorité pour la transparence de la vie publique (HATVP). Cette a été renforcée par la LOI n° 2022-401 du 21 mars 2022 visant à améliorer la protection des lanceurs d'alerte (1) et son Décret n° 2022-1284 du 3 octobre 2022 relatif aux procédures de recueil et de traitement des signalements émis par les lanceurs d'alerte et fixant la liste des autorités externes instituées par la loi n° 2022-401 du 21 mars 2022 visant à améliorer la protection des lanceurs d'alerte.

- **Code du patrimoine, Livre II : Archives, Articles L211 à L214-10**

Le Code du patrimoine fixe les principes généraux applicables à la gestion des archives. Il identifie la spécificité des archives publiques et reconnaît les responsabilités des organismes producteurs en termes de conservation, destruction, communication et restriction d'accès. Les articles du Code du patrimoine fixent

également le périmètre des responsabilités pénales des agents chargés qui interviennent tout au long des cycles de vie des documents.

- **Instruction n° 2005-003 du 22-2-2005 de tri et de conservation pour les archives reçues et produites par les services et établissements concourant à l'éducation nationale**

L'instruction n° 2005-003 propose un cadre de référence pour les documents produits par les établissements concourant à l'éducation nationale et l'enseignement supérieur. En particulier, elle définit les durées d'utilité administrative, les règles de tri et de conservation des archives. Cette instruction provisoire n'est pas exhaustive mais donne plusieurs indications de politique générale sur certaines typologies documentaires.

- **Code de l'éducation, Livre VIII : La vie universitaire, titre 1, section 2 : Discipline (Articles R811-10 à R811-42)**

Le code de l'éducation identifie le périmètre d'application du pouvoir disciplinaire au sein des établissements de l'enseignement supérieur et de recherche. Il identifie les responsabilités des usagers de l'université en cas de fraude et de tout fait de nature à porter atteinte à l'ordre, au bon fonctionnement ou à la réputation de l'université. Par ailleurs, il définit la composition et les pouvoirs des commissions de discipline compétentes à l'égard des usagers et qui sont chargés de l'instruction des dossiers afin de rendre une décision portant ou non une sanction.

- **Le Code des relations entre le public et l'administration est un code (CRPA)**

Le CRPA regroupe les dispositions régissant les relations entre le public au sens large et l'administration française. Il est issu de l'ordonnance nº 2015-1341 du 23 octobre 2015 et du décret nº 2015-1342 du même jour. Le CRPA encadre les conditions de communication des documents administratifs.

- **Code du travail (textes de référence)**

- Code du travail : articles L4121-1 et L4121-5 (Obligations de l'employeur)
- Code du travail : article L4122-1 (Obligation des travailleurs)
- Code du travail : articles L4131-1 à L4131-4 (Droit d'alerte et de retrait)
- Code du travail : article L1321-1 (Règlement intérieur)

- **Environnement du droit pénal (textes de référence)**

- Code de procédure pénale : article 7 (Prescription en cas de crimes)
- Code de procédure pénale : article 8 (Prescription en cas de délits)
- Code de procédure pénale : article 9 (Prescription en cas de contraventions),

- Code de procédure pénale : article 9-1 (Prescription des infractions occultes ou dissimulées)
- Code de procédure pénale : article 9-2 (Interruption de la prescription)
- Code de procédure pénale : article 9-3 (Suspension de la prescription)
- Code de procédure pénale : articles 706-47 (Infractions avec des délais allongés (pour les victimes mineurs))
- Loi du 29 juillet 1881 sur la liberté de la presse (Prescription des délits d'injure et de diffamation (articles 65 et 65-3)
- Code pénal : article 213-5 (Prescription des crimes contre l'humanité)
- Loi n°2021-478 du 21 avril 2021 visant à protéger les mineurs des crimes et délits sexuels et de l'inceste (Allongement du délai de prescription pour concernant certaines infractions commises sur une victime mineure)

Consulter les recommandations, guides, avis, délibérations et réglementations : Instances et autorités compétentes :

- **La Commission nationale de l'informatique et des libertés (CNIL)**

Créée par la loi Informatique et Libertés du 6 janvier 1978, la CNIL est chargée de veiller à la protection des données personnelles contenues dans les fichiers et traitements informatiques ou papiers, aussi bien publics que privés. Ainsi, elle est chargée de veiller à ce que l'informatique soit au service du citoyen et qu'elle ne porte atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques. La CNIL est une autorité administrative indépendante (AAI), c'est-à-dire un organisme public qui agit au nom de l'Etat, sans être placé sous l'autorité du gouvernement ou d'un ministre. Elle est composée de 18 membres élus ou nommés et s'appuie sur des services. Elle a un rôle d'alerte, de conseil et d'information vers tous les publics mais dispose également d'un pouvoir de contrôle et de sanction.

- **Le Service interministériel des Archives de France (SIAF)**

Service composant la direction générale des patrimoines et de l'architecture chargé de coordonner et évaluer l'action de l'Etat en matière de collecte, de conservation, de communication et de mise en valeur des archives publiques à des fins administratives, civiques, scientifiques et culturelles. Son action s'inscrit dans le cadre stratégique défini par le comité interministériel aux archives de France (CIAF). Elle s'appuie sur les avis et l'expertise du conseil supérieur des archives (CSA).

- **La Commission d'accès aux documents administratifs (CADA)**

Autorité administrative indépendante chargée de veiller à la liberté d'accès aux documents administratifs et aux archives publiques ainsi qu'à la réutilisation des informations publiques. Elle peut être saisie par les personnes (physiques ou

morales) qui se sont vues opposer une décision défavorable en matière d'accès aux documents administratifs ou de réutilisation des informations publiques. La commission peut aussi être saisie, à titre de conseil, par les administrations sollicitées en ces matières.

- **Le Défenseur des droits**

Nommé par le Président de la République après avis des commissions permanentes compétentes des assemblées parlementaires, pour un mandat de six ans non renouvelable, le Défenseur des droits est une autorité administrative indépendante chargée de veiller à la protection des droits et des libertés et de promouvoir l'égalité. Il intervient notamment dans les relations avec l'administration, les discriminations, la protection de l'intérêt de l'enfant, la déontologie des forces de police et, depuis 2016, la protection des lanceurs d'alerte.

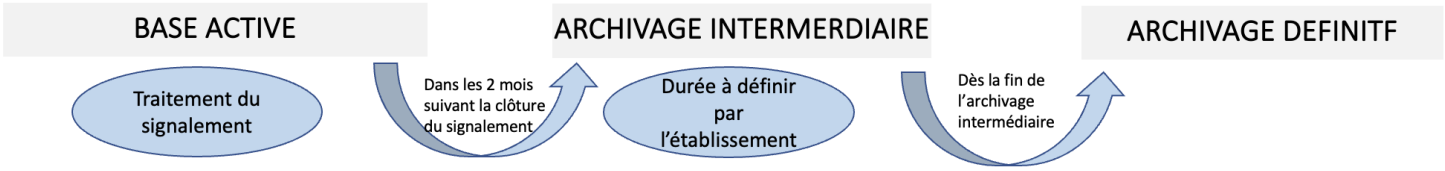
- **Ministère de l'enseignement supérieur, de la recherche et de l'innovation et son ou sa Ministre (Décret n° 2022-838 du 1er juin 2022 relatif aux attributions du ministre de l'enseignement supérieur et de la recherche) :**

Le ministre de l'enseignement supérieur et de la recherche prépare et met en œuvre la politique du Gouvernement relative au développement de l'enseignement supérieur. Il propose et, en liaison avec les autres ministres intéressés, met en œuvre la politique du Gouvernement dans le domaine de la recherche et de la technologie.

- Il est associé par le ministre de l'économie, des finances et de la souveraineté industrielle et numérique à la définition et au suivi de la politique en matière d'espace.
- Il prépare les décisions du Gouvernement relatives à l'attribution des ressources et des moyens alloués par l'Etat dans le cadre de la mission interministérielle « Recherche et enseignement supérieur ». A cet effet, les autres ministres lui présentent leurs propositions de crédits de recherche.
- Il contribue à la définition et à la mise en œuvre du programme des investissements d'avenir.
- Il est compétent pour la définition et la mise en œuvre de la politique de vie étudiante.
- Il est compétent, en lien avec les autres ministres intéressés, pour la définition et le suivi de la politique en matière d'innovation.
- Il prépare les décisions du Gouvernement relatives à la constitution d'universités de recherche à rayonnement international.
- Il participe à la promotion des sciences et des technologies, à la diffusion de la culture scientifique, technologique et industrielle ainsi qu'à la politique de transition écologique et énergétique.
- Il participe, conjointement avec les autres ministres intéressés, à l'élaboration et à la mise en œuvre de la politique du Gouvernement en faveur du

développement et de la diffusion des usages du numérique dans la société et l'économie.

B. Cycle de vie des documents contenant des données sensibles



Ce schéma représente les trois grandes étapes du cycle de vie des documents à caractère sensible.

- **Base active**

La base active correspond au traitement du signalement par les cellules, c'est-à-dire la période qui s'étend de la déclaration du signalement jusqu'au courrier du Président ou de la Présidente ou au jugement de la section disciplinaire.

- **Archivage intermédiaire**

L'archivage intermédiaire permet de conserver des documents durant un temps donné. Cette durée n'est pas fixée et doit être définie par l'établissement (voir III. C.). Il convient de définir le périmètre d'accès, c'est-à-dire les personnes habilitées à la consultation de l'archivage intermédiaire, ainsi que de s'assurer de la sécurité de la plateforme sur laquelle sont déposés les documents (voir IV. A.). L'extraction des données ne doit avoir lieu que pour les besoins du contentieux ou sur réquisition judiciaire.

- **Archivage définitif**

Les documents archivés définitivement pourront être utilisés pour des besoins statistiques ou des projets de recherche. Ils doivent être versés aux archives publiques.

C. Comment définir le délai d'archivage intermédiaire

Il n'y a pas de texte qui définisse la durée d'archivage intermédiaire. Chaque établissement est invité à établir son propre cadre, selon l'avis de son service juridique. Nous pouvons cependant formuler des préconisations.

Pour déterminer cette durée, il faut pondérer l'intérêt et les risques de conserver le dossier. L'enjeu est de trouver un équilibre entre le respect de la vie privée et de l'intégrité de la personne mise en cause et les possibilités pour la personne signalante de mener certaines procédures et la protection de potentielles autres victimes.

Ainsi, nous proposons plusieurs pistes de réflexion à explorer par l'établissement afin de déterminer le délai d'archivage intermédiaire.

- **A quelles fins les documents sont-ils archivés ?**

  ➔ Les données manipulées dans les dispositifs de signalement et de suivi des VSS concernent des faits susceptibles d'entraîner des poursuites judiciaires. Dans ce cas, se pose la question du délai de prescription. Pour rappel, la prescription désigne la durée au-delà de laquelle une action en justice, civile ou pénale, n'est plus recevable.

Tableau récapitulatif des délais de prescription pour les VSS

Acte	Type d'infraction	Délai de prescription
Injure à caractère sexiste ou sexuel	Contravention	1 an (art 9 CPP)
Outrage sexiste	Délit	6 ans (art 8 CPP)
Harcèlement sexuel	Délit	6 ans (art 8 CPP)
Agression sexuelle	Délit	6 ans (art 8 CPP)

Viol	Crime	20 ou 30 ans (art 7 CPP)

➔ L'accès au document peut être nécessaire si l'événement se répète, si la personne qui a signalé revient vers le dispositif afin d'obtenir des informations pour attester du signalement du problème à ce moment-là, ou qu'une enquête RH nécessite la récolte de témoignages pour la recherche de précédents.

➔ Un autre établissement d'enseignement supérieur pourrait demander des informations en cas de nouvel événement en son sein.

- **Quels sont les risques liés à la conservation des documents ?**

➔ La perte des documents.

➔ La fuite de données.

➔ Une plainte peut être déposée par la CNIL ou par une personne concernée pour conservation abusive (et non motivée) des informations. Dans tous les cas, il faut pouvoir fournir clairement les motifs de conservation des documents (se référer à "à quelles fins les documents sont-ils archivés ?").

➔ Le non-respect de la vie privée de la personne mise en cause et de la personne signalante.

NB : Il peut se poser la difficulté de la lisibilité des documents dans plusieurs années. Il convient de privilégier des formats standards, que ce soit pour les fichiers multimédia ou les écrits.

- **Quels sont les risques liés à une conservation trop courte ?**

➔ Le risque juridique est faible. Il n'y a jamais eu de sanction, dans le cadre d'une réquisition judiciaire, pour suppression d'informations sensibles. Les seuls cas d'obstruction à l'enquête concernent le fait de détenir une information que l'on refuse de donner.

➔ Il existe en revanche un risque moral. S'il manque des éléments lors d'une recherche de précédents par exemple, il pourrait y avoir un défaut d'assistance à la victime

- **Exemple : délais choisis par Université Côte d'Azur**

Des groupes de réflexion constitués d'expert·es (juristes, DPO, référente déontologue, DGS et membres de la gouvernance) ont été réalisés au sein de l'établissement de manière à trouver le meilleur cadre possible concernant la conservation des données sensibles. Il est apparu qu'un prérequis indispensable était notre capacité à garantir la conservation des données dans un espace sécurisé mais aussi de mettre en place un accès contrôlé aux données, permettant la journalisation de cet accès.

Les données sont considérées en base active pendant toute la durée du traitement. Cela peut aller de quelques semaines à une année selon les situations. Le nombre de personnes ayant accès aux données peut varier selon les situations, mais ce nombre est toujours restreint au maximum. Lorsque le traitement de la situation s'achève au sein de l'établissement, nous avons un délai de 2 mois pour transférer les données en archivage intermédiaire.

Les délais d'archivage intermédiaire ont été fixés à 20 ans pour notre établissement correspondant au délai de prescription du viol sur personne majeure, avec les modalités suivantes : seules quelques personnes habilitées y ont accès ; les données sont stockées sur une plateforme sécurisée permettant la journalisation des données ; l'extraction des données est possible uniquement pour les besoins du contentieux ou sur réquisition judiciaire par les personnes habilitées (direction juridique de l'établissement). Les fondements de ces modalités d'archivage intermédiaire sont l'art. 6.1 du RGPD, les besoins du contentieux, le concours éventuel aux services de police.

A l'issue de ces 20 ans, les données sont placées en archivage définitif et ne peuvent plus être consultées. Les modalités de transfert de ces données aux archives pour des besoins de recherche est à l'étude.

IV. Bonnes pratiques

A. Supports de conservation et dispositifs techniques qui portent les données

Les données manipulées dans les dispositifs de signalement et de suivi des VSS sont particulièrement sensibles car elles sont potentiellement nominatives et concernent des faits susceptibles d'entraîner des poursuites tant sur le plan disciplinaire que judiciaire. Dans ce dernier cas, et pour certains faits (viol sur mineur·e), les délais de prescriptions peuvent atteindre 30 ans à date de la majorité de la victime. Il est donc envisageable que les durées de conservation atteignent 30 ans. Il faut distinguer les étapes du cycle de vie des documents (CF III.B) et les documents ne seront en principe pas conservés sur des délais aussi importants en dehors d'un système d'archivage intermédiaire ou définitif, mais il faut, pour tous les établissements, être attentif aux dispositifs techniques qui portent les données collectées dans les dispositifs de signalement.

Le projet de recherche ANR Hubble s'est intéressé entre 2016 et 2019 à l'acquisition et au traitement de données d'apprentissage (Learning Analytics), souvent nominatives, pour la catégorisation ou l'évaluation d'étudiant·es ou d'élèves parfois mineur·es. Les données manipulées, jugées sensibles, ont soulevé des questions d'éthique et de sécurité des données et un Comité d'éthique en Learning Analytics (CELA) a été constitué. Il a proposé une grille questionnaire dont les questions (https://hubblelearn.imag.fr/wp-content/uploads/2019/03/FormulaireGuide_CELA.pdf) sont également pertinentes à notre contexte. La première question à se poser est celle des personnes ayant accès au stockage des données. Plus précisément, le CELA, en plus de demander d'identifier le responsable des traitements et le lieu de la collecte de données demandait à ce que ce responsable déclare ses éventuels conflits d'intérêt, les bénéfices et risques vis-à-vis de la réputation des personnes sur lesquelles on conservait des données et le traitement envisagé des données. Si ces premiers aspects sont très différents dans le contexte des cellules de signalement où il n'y a que des risques vis-à-vis de la réputation des personnes sans aucun bénéfice et en principe une neutralité des responsables des traitements, tout le questionnement sur le traitement des données reste semblable : quel est le procédé d'anonymisation (ici, le processus doit être réversible), quelles sont les personnes qui auront accès aux données : bien sûr la ou le responsable des données, mais aussi globalement les personnes associées d'un point de vue fonctionnel (cellule d'écoute et de traitement, administration) et d'un point de vue technique : il s'agit d'une part

des administrateur·rices du serveur, qui n'auront sans doute pas connaissance de ces données, mais auront dessus des accès complets. D'autre part, d'autres personnels des DSI auront certainement des facilités à accéder à ces données, même s'ils ne sont pas supposés administrer le serveur portant les données. Il est utile de faire un examen précis et complet, faire intervenir le ou la RSSI de l'établissement pour une analyse de sécurité du dispositif est une éventualité à envisager sérieusement. Enfin, les données sont en général sauvegardées (dupliquées) sur un système de sauvegarde de données (sur disque ou bandes). Ces sauvegardes sont effectuées régulièrement, typiquement tous les jours, mais avec des méthodes évitant de sauvegarder la totalité des données chaque jour (sauvegarde dite "différentielle" ou "incrémentale" par exemple). Sur des documents qui ne sont pas fréquemment modifiés, les copies ne sont sans doute que dans les sauvegardes dites complètes, qu'on ne fait que mensuellement voire moins. Les documents à surveiller ne sont donc en principe pas trop dupliqués, mais il faut aussi se poser la question des accès au système de sauvegarde et restauration des données du robot de sauvegarde.

D'un point de vue pragmatique, une analyse des possibilités d'accès pour différents dispositifs est utile pour mesurer le risque de fuite des données. Il faut suivre le processus dans son déroulé.

- **Formulaire de contact**

Tout d'abord, il y a un premier contact, souvent par le biais d'un formulaire en ligne permettant de faire le signalement. Selon les établissements, ce formulaire est libre d'accès ou situé sur un intranet. Nous ne pouvons que recommander qu'il soit d'accès libre car l'obligation de se connecter laisse planer le doute pour la personne effectuant la demande sur le réel anonymat proposé par ce type de formulaire. Souvent, ce formulaire en ligne abonde une adresse mail générique dans l'établissement. Il est utile de vérifier qui aura accès légitimement ou pour des raisons techniques au contenu de cette boite mail. Par ailleurs, certaines solutions de formulaire (MachForm par exemple) ne se limitent pas à l'envoi d'un mail à une adresse de contact ou générique, les données de chaque formulaire renseigné sont stockées dans une base de données. Via l'interface d'administration du formulaire, on accède à des informations complémentaires, notamment les adresses IP des utilisateur·rices qui ont envoyé chaque formulaire. Souvent dans nos établissements, l'adresse IP ne permet pas de remonter à un·e utilisateur·rice, mais ce n'est pas exclu. Les bases de données sont généralement stockées dans des SGBD (système de gestion de base de données) et il est de pratique courante que les SGBD soient accessibles à tous les développeurs d'application de la DSI. Les bases de données sont en principe sauvegardées (dump sql), il faut également se poser la question de qui a accès à ces sauvegardes.

- **Dossier de signalement, rapport, tableau de suivi des signalements**

Après ce premier contact, nous allons en général constituer le dossier de signalement, souvent sur un espace de partage entre collègues des missions égalité. A titre d'exemple, dans un établissement, un partage de fichier Windows avec contrôle d'accès par utilisateur·rice est disponible ainsi qu'un serveur NextCloud utilisé de façon limitée pour des projets de recherche et administré par le ou la référent·e égalité. En première intention, on peut imaginer que le partage de fichiers Windows présente davantage de sécurité et que moins de personnes sont susceptibles d'avoir accès aux données, mais un examen plus approfondi peut montrer le contraire :

- Le partage de fichiers est accessible légitimement à la ou le propriétaire du dossier (chargé·e de mission égalité), mais aussi aux personnes avec lesquelles les données sont partagées (membres de la cellule de traitement, administration). Nous ne dénombrons pas ici ces personnes car ce sont les mêmes qui auront légitimement accès à l'autre dispositif technique (NextCloud). En plus de ces personnes, les personnels de la DSI qui gèrent les partages Windows ont accès aux réglages du partage et peuvent temporairement s'octroyer des droits d'accès en cas de besoin technique (restauration de fichier, dépannage, etc.). Les administrateur·rices de la DSI ont un accès direct au serveur qui supporte le partage Windows et donc au système de fichier, ils et elles ont donc également potentiellement accès aux données. Le personnel de l'équipe support de la DSI a un système de prise en main à distance des postes du périmètre de l'administration. Ils et elles pourraient aussi, par l'intermédiaire d'un des postes des personnes ayant un accès légitime, voir ces données. Tous les personnels de DSI signent une charte d'administrateur·rice des systèmes d'information et savent qu'ils et elles ne doivent pas divulguer les informations auxquelles ils et elles auraient pu avoir accès dans le cadre de leurs fonctions, mais au total, en plus du dispositif de traitement, c'est une vingtaine de personnes qui peuvent avoir accès aux données.

- La solution NextCloud est hébergée sur les serveurs web de l'établissement. Trois administrateur·rices gèrent les serveurs. L'établissement utilise une architecture séparant production et qualification. Les développeur·ses n'ont d'accès direct que sur la qualification et les données sensibles ne sont qu'en production, ils n'y ont donc pas accès. Le RSSI de l'établissement a également accès aux serveurs. Le système de sauvegardes est géré par l'un·e des trois administrateur·rices système et au final, seules 4 personnes ont accès aux données et tous ont aussi signé la charte d'administrateur·rice système. De plus, mais c'est un cas particulier, le ou la référent·e égalité est l'un·e des trois administrateur·rices et comme le serveur qui

porte NextCloud est un serveur dédié à la recherche, l'un·e des administrateur·rices n'y accède jamais. Donc finalement, en plus des personnes du dispositif qui ont légitimement accès aux données, seules 2 personnes externes ont potentiellement accès aux données. Il faut toutefois rester prudent sur le fait que NextCloud est une application Web par nature directement exposée aux attaques externes, il faut donc être vigilant·e sur les mises à jour de cette plate-forme.

Cet exemple montre qu'une étude attentive est utile pour savoir où stocker les données avec un risque minimal de fuite et que, dans le cas présenté, l'utilisation de la plateforme NextCloud a été préconisée par le RSSI.

Pour des plateformes en ligne intégrées de type SOS de l'Université de Franche-Comté, en plus de la vérification des personnes ayant un accès pour des raisons techniques aux bases de données, il faut être attentif·ve à la fois aux sauvegardes de ces bases de données et au fait que l'application soit robuste vis-à-vis des injections SQL. En effet, les attaquant·es utilisent ce type de faille pour identifier la structure des bases de données et exécuter des requêtes pour récupérer la totalité de ces données.

- **Dossier d'enquête, rapport d'enquête**

Les utilisateur·rices de ces données sont principalement les services juridiques, voire la présidence de l'Université, plutôt qu'une mission égalité. Les services juridiques sont en général mieux formés à la gestion de ces données sensibles et les dispositifs techniques utilisés sont en principe davantage séparés de l'administration générale. Les données devraient y être mieux protégées.

Dans le cas d'une externalisation de l'enquête, un point de vigilance reste les moyens de transferts des données entre l'établissement et le prestataire, puis l'envoi du rapport d'enquête par le prestataire.

- **Archivage**

Enfin, après que les données aient été utilisées et partagées dans les cellules de signalement, missions égalité, services juridiques et services de la présidence, arrive le moment de leur archivage intermédiaire, puis définitif. Il faut prêter la même attention aux personnes ayant accès aux éventuelles copies de sauvegarde et aux personnes ayant l'accès au matériel et aux connaissances techniques pour y accéder.

Pour cet archivage, un stockage sur bandes, une mise hors ligne dans un stockage hors site dans des armoires sécurisées (anti-feu) assure à la fois la sécurité des données et limite considérablement tout risque d'accès non souhaité à ces données.

B. Copies locales et documents informels

Avec le besoin de se réunir et de gérer les dossiers, beaucoup des membres des cellules d'écoute et de traitement sont équipés d'ordinateurs portables. Le réseau informatique n'étant pas toujours disponible partout, la solution pour avoir sous la main les dossiers est d'en avoir fait une copie locale (sur le disque dur de l'ordinateur portable). Si cette pratique s'avère nécessaire pour travailler et disposer des pièces d'un dossier, nous pouvons préconiser de ne conserver en copie locale que le strict nécessaire et d'éliminer les copies locales dès que possible. Le risque vis-a-vis des copies locales de dossiers est essentiellement le vol de l'ordinateur. Si le disque dur de l'ordinateur est crypté comme le préconise le CNRS et un certain nombre d'établissements, le risque est toutefois très limité. Dans le cas où l'on ne gère pas soi-même des copies locales des dossiers, mais qu'on utilise un outil de type cloud interne (OwnCloud, NextCloud), il existe souvent une fonctionnalité de suppression à distance des données copiées sur un poste, en cas de vol : ceci ne fonctionne que si l'ordinateur est allumé et connecté au réseau, mais le serveur Cloud envoie alors l'ordre au client ou à la cliente présent·e sur le portable de supprimer les données locales.

Par ailleurs, lors d'une écoute d'une victime suite à un signalement ou des réunions pour le traitement d'un dossier ou encore pour des auditions de témoins ou de personnes mises en cause, il arrive souvent que l'on prenne des notes sur ordinateur ou manuscrites et/ou que l'on ait imprimé certains éléments du dossier pour pouvoir s'appuyer dessus. Ce type de documents n'a pas été mentionné dans ce guide jusqu'à présent car ils n'ont pas de rôle formel dans le processus de traitement, mais ils peuvent exister. Les préconisations que l'on peut donner pour ces documents informels sont d'une part d'en limiter très fortement l'existence : détruire (broyeuse) les éléments imprimés et les notes manuscrites dès qu'elles ne sont plus utiles, préférer des compte-rendus collaboratifs même imparfaits, où chacun·e retrouvera les informations dont il ou elle a besoin, à des compte-rendus officiels dont on gère le cycle de vie, accompagnés de compte-rendus individuels parallèles dont on ne gère pas le cycle de vie. Et d'autre part, dans la mesure où ces documents informels vont tout de même exister, mettre en place les moyens permettant de cadrer et limiter leur diffusion en prévoyant des serveurs internes maîtrisés, plutôt que de laisser chacun·e gérer ses notes individuelles.

C. Gestion humaine des documents

Il est important de constituer la liste des personnes habilitées à consulter les documents à caractère sensible. Par exemple, un·e référent·e chargé·e du dossier, et des personnes dédiées en charge du traitement ainsi que les membres de la gouvernance en particulier le ou la président·e qui prendront un certain nombre de décisions relatives au traitement de la situation. Ponctuellement, certaines personnes peuvent être amenées à consulter certaines pièces du dossier comme des membres des services des ressources humaines, la médecine du travail, certaines directions, des juristes.

Conclusion et perspectives

Ce groupe de travail sur la gestion des données sensibles à mis en relation des membres des dispositifs de signalement, avec un ensemble d'acteurs et d'actrices mobilisés au cours du traitement des dossiers au sein des établissements d'enseignement supérieur, de leur création à leur archivage, en passant par leur traitement. Des expert·es (archivistes, DPO, RSSI, etc.) ont également contribué à ce groupe en apportant leur expertise et par leurs échanges. La rédaction de ce guide résulte d'un besoin convergent des acteurs et actrices , qui, de par leurs rôles et fonctions, se sont vu·e·s confronté·es à un vide juridique, s'agissant de la conservation et de la destruction des données sensibles récoltées et traitées au sein de dispositifs, cellules et instances internes liées aux VSS et aux discriminations.

En effet, ces informations qui circulent au sein des différents dispositifs nous posent une question centrale : *Combien de temps pouvons-nous estimer nécessaire de conserver les informations récoltées et traitées pour répondre à l'objectif de ces traitements ?*

Afin de répondre à cette interrogation, une réflexion a été amorcée parmi ces acteurs et actrices qui, *in fine,* ont pu apporter une réflexion constructive, nourrie de références et d'expériences et ce, dans le but commun de trouver un équilibre pour qu'aucune procédure n'ait à pâtir de durées de conservation inadaptées, liées à un traitement isolé d'une procédure en particulier. En effet, certaines procédures sont liées entre elles, même si cela n'est pas toujours clairement établi. Cette imbrication doit être prise en compte pour que la gestion des données lié à une procédure n'impacte pas négativement une autre procédure.

Les réflexions de ce groupe de travail ont permis d'élargir la vision des acteurs sur les procédures existantes autour des sujets impliquant la récolte, le traitement et la conservation de données particulièrement sensibles.

Un travail de recensement des spécificités de chaque procédure, des typologies de données produites, des documents exploités et modifiés à des fins d'enquête, d'entretiens, de rapport de décision etc. a été conduit pour l'élaboration de ce guide. Ce travail a fait émerger le sujet de la conservation et de la destruction de ces données, pilotée par la recherche d'un équilibre entre les obligations légales de l'institution, le droit des usagères et usagers au respect de la vie privée et l'accès à la justice.

Néanmoins, il résulte des travaux du GT que le vide juridique qui entoure le sujet nécessiterait de définir son cadre légal auprès des autorités et instances qui ont la capacité de délibérer sur la démarche à suivre.

Par exemple, la Commission nationale de l'informatique et des libertés (CNIL), qui s'est saisie de la question des durées de conservation et du traitement des données

sensibles, est très attendue sur le sujet bien que la fixation du cadre légal applicable aux durées de conservation *stricto sensu,* ne soit pas de sa compétence directe même si la nécessité de définir une durée est prévue au sein du RGPD.

Applicable au sein de tout type d'établissement sous tutelle du Ministère de l'enseignement supérieur et de la recherche, une directive ministérielle, permettrait de guider les établissements sur le contexte juridique devant encadrer les dispositifs qui leur sont imposés. En effet, la création des dispositifs a multiplié les interlocuteurs et interlocutrices : les échanges de documents comportant notamment des données sensibles sont nombreux et doivent être sécurisés.

A l'échelle des établissements d'enseignement supérieur, la proposition de lieux de discussions concernant les données sensibles et les durées de conservation, notamment par la création d'espaces d'échange autour des situations VSS, discriminations par exemple, viserait à nourrir la réflexion commune et à prendre en compte les évolutions légales et contextuelles qui s'appliquent à la prise en charge de ces sujets et leurs dispositifs.

Ce guide a pour objectif d'ouvrir la réflexion sur le sujet, à l'échelle de tous les acteurs et actrices concerné·es au sein de l'enseignement supérieur. Il n'ést pas figé, sa vocation est humblement d'établir les principales bases de réflexions, le plus difficile étant souvent de savoir "*par où commencer ?*".

Ainsi, ce guide vise à proposer à toutes et tous la perspective d'une évolution de la réflexion, mûrie par vos apports, vos ressources, vos compétences mais surtout votre expérience au sein des missions Égalité et des services concernés par les dispositifs VSS en place au sein des établissements d'enseignement supérieur de l'ESR.

Annexes

A. Lexique

Notion	Définition
Outrage sexiste	Constitue un outrage sexiste le fait d'imposer à une personne tout propos ou comportement à connotation sexuelle ou sexiste qui soit porte atteinte à sa dignité en raison de son caractère dégradant ou humiliant, soit crée à son encontre une situation intimidante, hostile ou offensante
Harcèlement moral	Le harcèlement moral se manifeste par des agissements répétés pouvant entraîner, pour la personne qui les subit, une dégradation de ses conditions de travail pouvant aboutir à : une atteinte à ses droits et à sa dignité ou une altération de sa santé physique ou mentale. ou une menace pour son évolution professionnelle.
Harcèlement sexuel	Le harcèlement sexuel est le fait d'imposer à une personne, de façon répétée, des propos ou comportements à connotation sexuelle ou sexiste qui soit portent atteinte à sa dignité en raison de leur caractère dégradant ou humiliant, soit créent à son encontre une situation intimidante, hostile ou offensante
Violence	Les violences sont l'ensemble des infractions pénales ou circonstances aggravantes constituant une atteinte à l'intégrité des personnes
Discrimination	Une discrimination est un traitement défavorable qui doit généralement remplir deux conditions cumulatives : être fondé sur un critère défini par la loi (sexe, âge, handicap...) ET relever d'une situation visée par la loi (accès à un emploi, un service, un logement...).À ce jour, la loi reconnait plus de 25 critères de discrimination.
Document administratif	Le code définit la notion de document administratif de façon très large (art. L. 300-2) : dossiers, rapports, études, comptes rendus, procès-verbaux, statistiques, directives, instructions, circulaires... qu'ils se présentent sous forme écrite, sous forme d'enregistrement sonore ou visuel ou sous forme numérique ou informatique. Sont également concernées les informations contenues dans des fichiers informatiques et qui peuvent en être extraites par un traitement automatisé d'usage courant.

CRPA	Le Code des relations entre le public et l'administration est un code regroupant les dispositions régissant les relations entre le public au sens large et l'administration française. Il est issu de l'ordonnance nº 2015-1341 du 23 octobre 2015 et du décret nº 2015-1342 du même jour.
CADA	La Commission d'accès aux documents administratifs est une autorité administrative indépendante chargée de veiller à la liberté d'accès aux documents administratifs et aux archives publiques ainsi qu'à la réutilisation des informations publiques.
CNIL	La Commission nationale de l'informatique et des libertés est l'autorité administrative indépendante française chargée notamment maintenant de veiller au respect du RGPD
SIAF	Le service interministériel des Archives de France
SECTION DISCIPLINAIRE	La section disciplinaire est une formation juridictionnelle du conseil académique de l'université ou de l'un des autres établissements publics français d'enseignement supérieur placés sous la tutelle du ministre chargé de l'enseignement supérieur
CODE DU PATRIMOINE	Le patrimoine s'entend, au sens du présent code, de l'ensemble des biens, immobiliers ou mobiliers, relevant de la propriété publique ou privée, qui présentent un intérêt historique, artistique, archéologique, esthétique, scientifique ou technique.
RGPD	Le règlement général sur la protection des données (RGPD, ou encore GDPR, de l'anglais « General Data Protection Regulation »), officiellement appelé règlement UE 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE, est un règlement de l'Union européenne qui constitue le texte de référence en matière de protection des données à caractère personnel
RSSI	Désigne la ou le Responsable de la Sécurité des Systèmes d'Information
DPO	DPO est l'acronyme anglais de data protection officer - délégué·e à la protection des données
Anonymisation au sens RGPD	Source cnil.fr : L'anonymisation rend impossible l'identification d'une personne à partir d'un jeu de données et permet, ainsi, de respecter sa vie privée, voir technique : https://ec.europa.eu/justice/article-29/documentation/opinion-reco

	mmendation/files/2014/wp216_fr.pdf
Pseudonymisation au sens RGPD	Source cnil.fr : La pseudonymisation est un traitement de données personnelles réalisé de manière à ce qu'on ne puisse plus attribuer les données relatives à une personne physique sans information supplémentaire. En pratique, la pseudonymisation consiste à remplacer les données directement identifiantes (nom, prénom, etc.) d'un jeu de données par des données indirectement identifiantes (alias, numéro séquentiel, etc.). La pseudonymisation permet ainsi de traiter les données d'individus sans pouvoir identifier ceux-ci de façon directe. En pratique, il est toutefois bien souvent possible de retrouver l'identité de ceux-ci grâce à des données tierces : les données concernées conservent donc un caractère personnel. L'opération de pseudonymisation est également réversible, contrairement à l'anonymisation.
Anonymat	Pratique consistant à supprimer ou à ne pas mentionner le ou les prénom(s) et le ou les nom(s) des personnes, en outre il s'agit d'apprécier la qualité de ce qui est anonyme, de ce qu'on ignore le nom, dont on ne connaît pas l'identité directe.

B. Liste des participant·es au groupe de travail

Alan Boucher, responsable du service archives à Champ-sur-Marne, Université Gustave Eiffel
Anthony Nutten, directeur des données, service informatique Université Paul Valéry
Antoine Ruf, assistant en gestion administrative, Mission égalité Université Paul Valéry Montpellier 3
Aude Stheneur, cheffe de projets, CPED
Aymma Letellier, chargée de mission égalité, Université Caen Normandie
Isabelle Jacques, référente égalité, Université de Franche-Comté, responsable de la cellule SOS (Signalement Orientation Suivi)
Maëva Ballon, cheffe de projet de la mission égalité, Université Gustave Eiffel
Magali Boucaron Nardetto, référente déontologue-laïcité-alerte, Université Côte d'Azur
Nawale Lamrini, déléguée protection des données, Sciences Po Paris
Philippe Daubias, référent égalité, ENS de Lyon
Radouan Mounecif, archiviste, Sciences Po Paris
Romane Masternak, stagiaire, CPED
Rozenn Texier-Picard, ENS Rennes
Solen Lallement, référente égalité et lutte contre les violences sexistes et sexuelles, Sciences Po Paris
Sonia Grèze, référente RGPD, Université Paul Valéry
Sylvie Levillayer, archiviste, Université Gustave Eiffel
Véronique Van de Bor, vice-présidente politique sociale, égalité, diversité, Université Côte d'azur et vice-présidente de la CPED
Violette Zecchi, chargée de mission Egalité Femmes-Hommes au sein de la Vice-Présidence Egalité Femmes-Hommes, Université Grenoble Alpes
Yamina Meziani, Chargée de mission parité, égalité, diversité, Université de Bordeaux