Quelles démarches de conformité pour l'organisation d'un examen à distance et/ou en ligne ?

Synthèse :

Le recours au passage d'examen à distance sous forme numérique par les établissements d'enseignement supérieur publics et privés est de plus en plus répandu. Les dispositifs de télésurveillance utilisés dans ce cadre étant par nature intrusifs, les exigences de la réglementation sur la protection des données personnelles et la mise en œuvre de bonnes pratiques doivent permettre le bon déroulement des examens tout en assurant le respect de la vie privée des étudiants.

Le déroulement des examens à travers ces nouveaux usages pourrait porter atteinte au principe d'égalité de traitement entre les candidats ; à ce titre, la CNIL recommande expressément que le passage de certaines épreuves à distance soit une faculté offerte aux étudiants et non une obligation. Ainsi, lorsqu'un établissement décide de recourir au passage d'un examen à distance avec télésurveillance, une alternative en présentiel doit systématiquement être proposée aux candidats[1].

La mise en œuvre de ce type de traitement doit donc être strictement encadrée. Ainsi, les principes de proportionnalité et de sécurité permettront de déterminer les modalités du passage des examens à distance, notamment en cas de recours à la surveillance (signature d'un contrat de sous-traitance si recours à un prestataire, utilisation de l'ensemble des fonctionnalités ou pas, etc.), la durée de conservation et le respect des droits des personnes doivent être définis et mis en œuvre, …

Ce type de traitement fait obligatoirement l'objet d'une analyse de conformité approfondie au regard des grands principes de protection des données, en collaboration avec votre Délégué(e) à la protection des données (DPO).

1. Cadre juridique

Le décret n 2017-619 a créé les articles D611-10 et suivants qui prévoient la **possible validation des enseignements sous forme numérique**, assortie des conditions suivantes :

- La vérification que le candidat dispose des moyens techniques lui permettant le passage effectif des épreuves ;
- La vérification de l'identité du candidat ;
- La surveillance de l'épreuve et le respect des règles applicables aux examens.

S'y ajoute la règle selon laquelle « les conditions de la validation des enseignements, dispensés en présence des usagers ou à distance, le cas échéant sous forme numérique, sont arrêtées dans chaque établissement d'enseignement supérieur au plus tard à la fin du premier mois de l'année d'enseignement et elles ne peuvent être modifiées en cours d'année[2].

[1] Point 19 de la Délib. n 2023-058 du 8 juin 2023 portant adoption d'une recommandation relative aux modalités de mise en œuvre des dispositifs de télésurveillance pour les examens en ligne

[2] art. L611-8 et D611-12 du Code de l'éducation

2. Démarches préalables à réaliser par les services de l'établissement pour la mise en place d'un examen à distance

- Indiquer dans les plaquettes de formation le recours à l'examen à distance comme modalité de contrôle des connaissances, notamment en cas de télésurveillance, afin que l'étudiant puisse être informé lors du choix de sa formation ;

- Vérifier que l'examen entre dans le cadre des MCC (Modalités de Contrôle des Connaissances)[3] ou le règlement des études, selon la forme juridique de l'établissement (public ou privé) ;

- Vérifier auprès du service en charge de la mise en œuvre de l'examen et/ou du DPO[4] que les outils utilisés pour le déroulement de l'examen ont fait l'objet d'une analyse de conformité au RGPD ;

- Vérifier auprès du service en charge de la mise en œuvre de l'examen qu'il existe des mesures permettant de pallier certaines difficultés (prêt de matériel adapté par exemple) et prévoir aussi souvent que possible une possibilité de passage de l'examen en présentiel ; étant précisé que l'organisation d'un examen en mode hybride devra respecter le principe d'égalité de traitement entre les candidats ;

- Se référer à l'Analyse d'Impact relative à la Protection des Données (AIPD) produite par l'établissement concernant le traitement « examen à distance » afin d'apprécier les mesures organisationnelles et techniques à mettre en œuvre pour respecter les droits des étudiants ou candidats. En l'absence d'une telle analyse, rapprochez-vous de votre DPO afin qu'il vous accompagne dans la réalisation d'une telle analyse et vous oriente vers les bonnes démarches.

3. Principes[5] des règles de protection des données personnelles

L'organisation d'un examen à distance en lieu et place d'un examen en présentiel, notamment en cas de recours à la télésurveillance de l'examen, doit faire l'objet d'une analyse juridique et technique approfondie, adaptée aux risques associés aux opérations de traitement, et prendre en compte le contexte et les finalités du traitement.

En s'appuyant sur la recommandation en date du 8 juin 2023 de la Commission nationale de l'informatique et des libertés relative aux modalités de mise en œuvre des dispositifs de télésurveillance pour les examens en ligne[6] et les grands principes des règles de la protection des données personnelles, voici une première base d'analyse qui sera à **adapter par chaque établissement**.

- Sur l'obligation d'information :

L'obligation d'information doit être réalisée à différents stades du traitement :

- En amont, dans les MCC et dans les plaquettes ou supports de communication sur les différentes formations concernées ;

[3] Ici l'établissement joue son rôle de responsable du traitement (RT), en tant que représentant légal de l'établissement d'enseignement supérieur, il détermine les finalités et moyens du traitement mis en œuvre ;
[4] Cf. l'encart « Focus mission du DPO » en fin de document ;
[5] https://www.cnil.fr/fr/cnil-direct/question/quels-sont-les-grands-principes-des-regles-de-protection-des-donnees
[6] Délib. n 2023-058 du 8 juin 2023 portant adoption d'une recommandation relative aux modalités de mise en œuvre des dispositifs de télésurveillance pour les examens en ligne

- Au sein du règlement des études pour les établissements privés ;
- Au plus tard à la fin du premier mois de l'année universitaire, par tout moyen (e-mail, espace en ligne de la formation,) conformément à la réglementation sur les examens selon laquelle les modalités d'examen doivent être arrêtées dans chaque établissement d'enseignement supérieur au plus tard à la fin du premier mois de l'année d'enseignement[7].

  La CNIL encourage vivement les établissements à communiquer les modalités d'examen envisagées ainsi que les dispositifs susceptibles d'être employés pour la télésurveillance suffisamment à l'avance, aussi tôt que possible et avant l'inscription à la formation, afin de permettre aux étudiants de faire leur choix de formation en toute connaissance de cause.
- Des mentions d'information dont la rédaction doit reprendre précisément les obligations de l'article 13 du RGPD sont à prévoir sur les supports de communication et doivent être accessibles à tout moment par les étudiants (par exemple sur différents supports : site internet de la formation, mentions présentes sur l'outil d'examen en ligne). La communication de ces mentions est un préalable à toute mise en œuvre d'un examen en ligne/à distance.
- Prenez contact avec votre DPO concernant la rédaction de ces mentions d'information.

Toute opération de lecture/écriture sur l'équipement du candidat est soumis à son consentement sauf si ces opérations, qui demandent à accéder au service de communication en ligne permettant de passer l'épreuve à distance, sont strictement nécessaires à sa fourniture[8].
Une analyse de la solution technique est à réaliser par le responsable de traitement en cas de dépôt de cookies ou autres traceurs par la solution envisagée.

- Sur le principe de finalité :

On précise qu'il s'agit ici de déterminer l'objectif poursuivi par l'établissement dans la mise en œuvre des examens en ligne/à distance. Cet objectif s'intègre dans une **finalité plus générale de** la passation d'un examen pour la délivrance d'un diplôme. Ce traitement devrait déjà être inscrit au registre d'activités des traitements de l'établissement, soit en tant que traitement isolé, soit intégré à un traitement plus global de gestion de la scolarité des étudiants. Dès lors, une mise à jour du traitement pourrait être nécessaire pour documenter les nouvelles catégories de données personnelles traitées ainsi que les nouvelles mesures techniques et organisationnelles mises en œuvre, liées à l'utilisation d'un dispositif de passation d'examen en ligne, télésurveillé ou non.

Focus : existence de finalité(s) complémentaires

Attention : certains éditeurs conditionnent l'usage de leur solution à la mise en œuvre d'un traitement complémentaire sur la base de leur intérêt légitime à des fins de *machine learning. Ce machine learning* leur permet de faire évoluer leur outil grâce aux traitements des données des étudiants.
Cette finalité complémentaire doit être particulièrement encadrée, dans la négociation du contrat entre l'établissement et l'éditeur, mais également au regard du droit des personnes, qui doivent pouvoir consentir ou s'opposer au traitement, au risque de constituer un détournement de finalité.

[7] Art. D. 611-12, Code de l'éducation.
[8] Article 82 de la loi « Informatiques et libertés »

- Quelle base légale mobiliser ?

Déterminer la base légale du traitement permet de s'assurer que le traitement mis en œuvre est licite et autorise l'établissement à traiter les données personnelles.

Les principales bases à mobiliser dans le cadre de la passation d'un examen, quelles que soient les modalités mises en œuvre (à distance, en ligne, présentiel, hybride) sont les suivantes :

- La mission d'intérêt public poursuivie par l'établissement public et le cas échéant certains établissements privés ;
- L'exécution du contrat (pour les établissements privés) est mobilisable à condition que les modalités d'examen soient fixées dans le contrat avec l'étudiant.

Les autres bases légales apparaissent moins appropriées[9].

Focus : le consentement comme base légale

On rappelle que le consentement, pour être valide, doit être libre et éclairé.

Le consentement comme base légale paraît peu approprié ; en effet, cela nécessiterait :

- Qu'une alternative en présentiel soit proposée au candidat, sans conséquence négative pour lui s'il la choisit ;
- Que le consentement puisse être retiré à tout moment, ce qui n'est pas envisageable dans le cadre d'un examen.

- Sur le principe de proportionnalité et de pertinence :

Les données doivent être minimisées ; seules les données strictement nécessaires devront être collectées et traitées pour assurer l'identification du candidat, le déroulement de l'épreuve et la correction le cas échéant.

Ces données peuvent être identiques à celles traitées lors d'un examen sur table (nom et prénom de l'étudiant, INE, …), complétées de celles rendues nécessaires par l'usage de la solution technique (adresse électronique, …). Les fonctionnalités retenues déterminent l'étendue de la collecte des données et l'établissement doit être vigilant sur le caractère proportionné de l'ensemble des collectes de données personnelles.

S'agissant de la vérification de l'identité des candidats, celle-ci pourra s'opérer :

- Pour les examens à faible enjeu (contrôle continu, quizz de connaissances) :
  - par une authentification de la personne sur la plateforme
- Pour les examens à fort enjeu (examen de fin d'année, de diplomation)
  - par une vérification documentaire du candidat avec présentation d'une pièce d'identité valide

Focus :
Le recours à un dispositif de reconnaissance faciale qui induit un système biométrique nécessite un consentement et vous devez impérativement contacter votre DPO pour vérifier que l'ensemble des conditions complémentaires et obligatoires requises sont effectivement respectées.

[9] Point 25 la Délib. n 2023-058 du 8 juin 2023 portant adoption d'une recommandation relative aux modalités de mise en œuvre des dispositifs de télésurveillance pour les examens en ligne

S'agissant du déroulement de l'examen, la solution devra également permettre la gestion des étudiants en situation de handicap, avec la possibilité d'accepter une autre personne dans la salle pour le secrétariat, la possibilité d'un tiers-temps, ou encore la conformité des solutions au Référentiel général d'amélioration de l'accessibilité (RGAA).

S'agissant des modalités de surveillance, celles-ci sont à examiner au regard des questions de fracture numérique et d'expérience utilisateur (telle que la nécessité d'installer une application sur l'outil informatique, ou encore l'usage complémentaire d'une application installée sur le téléphone portable de l'étudiant pour un second angle de vue). Elles doivent aussi être mesurées en fonction de la proportionnalité des données collectées, par exemple en fonction des accès excessifs demandés par l'application sur le smartphone, et du risque de sécurité

Ces questions pourraient explicitement figurer dans le contrat signé avec le sous-traitant.

- Sur le principe d'une durée de conservation limitée :

Les durées de conservation des données figurent déjà dans le registre des traitements tenu par le Responsable du traitement.

Dans l'hypothèse d'une sous-traitance à un prestataire extérieur, il apparaît nécessaire de préciser ces durées si la dématérialisation les impacte, en particulier pour les captations de l'étudiant, et de s'assurer que la solution technique retenue permet effectivement de respecter ces durées de conservation. Dans tous les cas, une fois que l'examen est passé, notamment lorsqu'une solution technique externe est utilisée, il est nécessaire d'exporter les données afin que l'établissement puisse conserver les données en archivage intermédiaire selon les durées prévues dans le registre des traitements. Les données archivées donneront lieu à la mise en place d'une clef de hachage permettant d'attester que les données d'origine n'ont pas été altérées.

Cette durée devra tenir compte des délais probatoires et de la durée d'utilité administrative[10].

- Sur le principe de sécurité et de confidentialité :

Le sous-traitant (avec lequel un contrat doit nécessairement être signé[11]) doit présenter les garanties suffisantes permettant d'assurer la sécurité des données traitées.

Il peut s'agir en particulier d'expliciter les conditions de chiffrement des données, la gestion des habilitations et des droits des différents intervenants permettant de limiter au strict nécessaire l'accès aux données selon leurs fonctions, la mise en place d'une journalisation des accès[12], la politique de protection des données en vigueur, la gestion des mots de passe, les résultats des audits et tests d'intrusion, les conditions d'hébergement des copies, de l'authentification des étudiants et des administratifs, le recours à d'éventuels sous-traitants ultérieurs, etc.

[10] dans la Délibération n 2023-058 du 8 juin 2023, en point 49, la CNIL stipule « En cas de suspicion de fraude, la durée de conservation des données ne devrait pas excéder les délais légaux des procédures disciplinaire ou contentieuse qui pourraient être engagées, et qui est en principe de deux mois. »
[11] RGPD art. 28, notamment via la mise en œuvre avec les sous-traitants des Clauses contractuelles type de la décision d'exécution (UE) 2021/915
[12] dans la Délibération n 2023-058 du 8 juin 2023, en point 56, la CNIL stipule que « les journaux d'accès aux données doivent disposer d'une durée de conservation propre, généralement comprise entre six mois et un an. »

Il conviendra de vérifier que seuls les administrateurs du système peuvent modifier ou supprimer les données collectées par les outils de télésurveillance.

Vous devrez aussi vous assurer que l'installation d'outils sur le poste du candidat ne posera pas de problème d'instabilité ou de sécurité du poste et cela quel que soit le système d'exploitation utilisé sur ces postes étudiants. La désinstallation des outils de surveillance doit se faire facilement et sans poser de problème sur le poste du candidat.
En cas d'incident sur le poste candidat, une solution alternative doit pouvoir lui être proposée (examen papier, prêt d'un équipement pour le temps de l'examen à distance).

Le recours à des examinateurs-tiers doit aussi être analysé : certains prestataires contractent avec des sous-traitants ultérieurs pour identifier les suspicions de fraude. Le lieu et les modalités d'accès de ces examinateurs sont à étudier. Le recours à des examinateurs présents dans un local de l'établissement peut être à privilégier pour en assurer la sécurité le temps de l'examen.

En fonction des fonctionnalités utilisées (captation de l'étudiant, utilisation d'algorithmes de détection de fraudes, installation complémentaire d'une application, …), et au regard des différents critères prévus par le RGPD (notamment données hautement personnelles, collecte à large échelle, personnes vulnérables, usage innovant), une analyse d'impact sur la protection des données (AIPD)[13] devrait être menée par le responsable des traitements.

Un tel traitement devrait, enfin, faire l'objet d'une homologation au Référentiel général de sécurité (RGS) pour les établissements ayant une mission d'intérêt général ou de service public.

- <u>Sur le respect des droits des personnes</u> :

Comme rappelé dans le point 2 du présent document, les modalités d'examen sont à arrêter au plus tard à la fin du premier mois de l'année d'enseignement. Au-delà de ce délai, ces modalités ne peuvent plus être mises en place.
Ces modalités peuvent opportunément intégrer les mentions d'information utiles sur les conditions de traitement des données personnelles des usagers[14]. Ces informations « RGPD » doivent par ailleurs être largement diffusées pour assurer la meilleure transparence des conditions de traitement des données des étudiants. Pour les établissements privés, ces modalités d'examen sont à prévoir dans la contractualisation mise en place avec l'apprenant.

Enfin, un guide d'utilisation de la solution retenue devrait intégrer les bonnes pratiques afin d'éviter la collecte de données superflues telles que les éléments de l'environnement, photographies de famille, etc…

On rappelle que, même pour les traitements mis en œuvre dans le cadre de l'exécution d'une mission d'intérêt public, le droit d'opposition s'applique « *à moins que le responsable du traitement ne démontre qu'il existe des motifs légitimes et impérieux pour le traitement qui prévalent sur les intérêts et les droits et libertés de la personne concernée*[15] »

[13] Ex. d'AIPD du projet OP4RE : https://www.onlineproctoring.eu/fr/extrants-intellectuels/
[14] RGPD, art. 13"
[15] RGPD, art. 21

Enfin, et en complément de ces grands principes, il apparaît nécessaire d'avoir une attention particulière sur la question du recours à une solution algorithmique ou intelligence artificielle de détection de la fraude proposée par certains prestataires.

Ces innovations, particulièrement intrusives, ne doivent en effet pas permettre la prise de décision entièrement automatisée, a priori inapplicable du fait de l'existence d'un jury d'examen, et par ailleurs interdite selon la base légale retenue[16]. De plus, elles présentent des risques élevés de faux positifs pouvant nuire à la bonne tenue de l'examen et fixer l'attention des candidats sur leur comportement plutôt que sur le passage de l'examen.

- Analyse d'Impact relative à la Protection des Données

En fonction de la nature de l'examen et de l'impact qu'il va avoir au regard des libertés individuelles des candidats, le responsable de traitement, avec l'appui du délégué à la protection des données, le cas échéant, doit procéder à une réflexion et une analyse d'impact préalables à l'organisation d'un examen à distance avec télésurveillance, en tenant compte des risques réels de fraude et des conséquences de celle-ci, afin d'éviter de recourir à des outils excessivement intrusifs au regard de l'enjeu et des risques.

Focus : Missions du DPO

Les missions du délégué à la protection des données (DPO) sont prévues par le Règlement général sur la protection des données (RGPD) ; celles-ci sont notamment[17] de :

- Informer et conseiller le responsable du traitement ou le sous-traitant (ST) ainsi que les employés qui procèdent au traitement sur les obligations qui leur incombent en vertu du RGPD et des lois nationales ;
- Contrôler le respect du RGPD ;
- Dispenser des conseils, sur demande, en ce qui concerne l'analyse d'impact relative à la protection des données (AIPD) et vérifier l'exécution de celle-ci.

[16] RGPD, art. 22
[17] RGPD, art. 39