CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

Décision n° MED-2025-048 du 22 avril 2025 mettant en demeure la société EDUSIGN

(N°MDM251031)

La Présidente de la Commission nationale de l'informatique et des libertés,

Vu le 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 ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, notamment son article 20 ;

Vu le décret n° 2019-536 du 29 mai 2019 modifié pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

Vu la délibération n° 2013-175 du 4 juillet 2013 portant adoption du règlement intérieur de la Commission nationale de l'informatique et des libertés ;

Vu la décision n° 2023-172C du 26 juin 2023 de la Présidente de la Commission nationale de l'informatique et des libertés de charger le Secrétaire général de procéder ou de faire procéder à une mission de vérification des traitements de données mis en œuvre par la société EDUSIGN;

Vu le procès-verbal de contrôle sur audition n° 2023-172/1 du 26 septembre 2023 ;

Vu les autres pièces du dossier ;

I. La procédure

La société EDUSIGN (ci-après « la société ») est une société par actions simplifiée créée en mars 2020 dont le siège social est situé 1 rue du Prieuré à Saint-Germain-en-Laye (78100) et qui emploie environ vingt salariés. La société a réalisé un chiffre d'affaires d'environ [redacted] en 2022 pour un résultat net de [redacted] euros.

La société EDUSIGN est spécialisée dans le conseil en systèmes et logiciels informatiques. La société a environ [redacted] clients, qui sont des établissements d'enseignement supérieur, des organismes de formation et des entreprises. Elle fournit aux organismes de formation une plateforme afin d'automatiser la gestion des présences d'apprenants, la signature de documents, le remplissage de questionnaires et fournit des alertes et statistiques concernant l'assiduité des apprenants.

L'application proposée par la société comprend environ [redacted] utilisateurs qui ont un compte administrateur, et plus [redacted] utilisateurs qui ont un compte spécifique aux apprenants.

En application de ma décision n° 2023-172C du 26 juin 2023, une délégation a procédé à une mission de contrôle sur audition du président de la société EDUSIGN le 26 septembre 2023 dans les locaux de la CNIL, afin de vérifier la conformité des traitements mis en œuvre par la société à l'ensemble des dispositions de la loi n° 78-17 du 6 janvier 1978 relative à

l'informatique, aux fichiers et aux libertés modifiée et du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (ci-après le « Règlement » ou le « RGPD »).

Des pièces complémentaires ont été reçues par la CNIL le 5 octobre 2023.

II. Sur la qualité de la société EDUSIGN vis-à-vis du traitement en question

En droit, en vertu de l'article 4, paragraphe 7, du RGPD, est responsable du traitement, « *la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement* ».

L'article 4, paragraphe 8, du RGPD définit le sous-traitant comme « *la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement* ».

En l'espèce, la société EDUSIGN fournit à ses clients (des organismes de formation, des établissements d'enseignement supérieur ou des entreprises) une plateforme afin d'automatiser la gestion de présence des apprenants, la signature de documents, le remplissage de questionnaires, et la fourniture d'alertes et de statistiques concernant l'assiduité des apprenants. Dans ce cadre, en fournissant une application afin que ses clients puissent mettre en œuvre leur traitement de suivi de présence des apprenants, elle agit pour le compte des clients, responsables de traitement qui déterminent les finalités et les moyens de leur traitement. Dès lors, elle doit être regardée comme sous-traitante de ces derniers au sens de l'article 4, paragraphe 8 précité. La société a elle-même déclaré, lors du contrôle de la Commission, qu'elle était sous-traitante de ses clients.

En revanche, EDUSIGN est responsable du traitement des données de ses salariés en ce qu'elle détermine les finalités et les moyens de ce traitement.

III. <u>Les manquements au RGPD</u>

A. Un manquement à l'obligation d'assurer la sécurité et la confidentialité des données (article 32 du RGPD)

En droit, l'article 32 du RGPD impose au responsable de traitement « *Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, [de mettre] en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque* ».

En outre, il résulte des mêmes dispositions, lu à la lumière du considérant 75 du RGPD que, lorsque le traitement en cause porte sur des catégories particulières de données à caractère personnel, comme des données de santé, le traitement doit bénéficier de mesures de sécurité renforcées.

S'agissant de la sécurité des ordinateurs, je relève que le fait de ne pas rendre obligatoire l'utilisation d'un ordinateur chiffré par les salariés lorsqu'ils utilisent un équipement nomade crée un risque d'atteinte à la sécurité des données à l'extérieur des locaux, dont le vol ou la perte des équipements mobiles fournis aux salariés. Dans sa fiche « Sécurité : sécuriser l'informatique mobile[1] » du 14 mars 2024, la CNIL préconise le chiffrement des postes nomades : « *L'employeur est responsable de la sécurité des données personnelles de son*

[1] https://www.cnil.fr/fr/securite-securiser-linformatique-mobile

entreprise, y compris lorsqu'elles sont stockées sur des terminaux dont il n'a pas la maîtrise physique ou juridique, mais dont il a autorisé l'utilisation pour accéder aux ressources informatiques de l'entreprise. Les risques contre lesquels il est indispensable de se prémunir vont de l'atteinte ponctuelle à la disponibilité, l'intégrité et la confidentialité des données, à la compromission générale du système d'information de l'entreprise (intrusion, virus, chevaux de Troie, etc.) ». Afin de limiter ces risques, il est notamment recommandé de mettre en place des moyens de chiffrement des postes nomades et des supports de stockage mobiles, tels que le chiffrement de disque dur, le chiffrement fichier par fichier, ou la création de conteneurs chiffrés.

De la même manière, il ressort de la mesure 4 du guide d'hygiène informatique de l'agence nationale de la sécurité des systèmes d'information (ANSSI) qu'après avoir déterminé les données sensibles d'une entité et sur quels composants du système d'information elles sont localisées, il est nécessaire que ces composants fassent l'objet de mesures de sécurité spécifiques. La mesure 31 du même guide précise que le chiffrement des postes informatiques des personnels est exigé lorsque les postes permettent l'accès à des données sensibles.

Il résulte de l'ensemble de ce qui précède que lorsque le responsable de traitement autorise l'utilisation d'équipement nomades, notamment des ordinateurs portables, pour traiter un volume important de données sensibles ou dont la divulgation porterait une atteinte grave à la vie privée des personnes, il doit mettre en place des mesures de sécurité spécifiques de nature à protéger la confidentialité des données en cas de perte ou de vol de l'équipement. Le chiffrement constitue en principe la mesure la plus adaptée à mettre en place.

En l'espèce, la délégation a été informée que si la société propose à chaque salarié la mise à disposition d'un ordinateur professionnel, celui-ci n'est pas chiffré. Les ordinateurs personnels des salariés, dont l'employeur autorise l'emploi, ne le sont pas davantage. Or, la délégation a été informée qu'une partie des salariés avait accès à un volume important de données à caractère personnel relatives à la santé des personnes, précisément aux arrêts maladie des apprenants permettant de justifier leurs absences.

Dans ces conditions, pour assurer la sécurité des données à caractère personnel traitées par la société et accessibles depuis ces équipements, les ordinateurs doivent être chiffrés, que ceux-ci soient ou non fournis par la société. Il n'a pas été justifié de mesures de sécurité permettant d'atteindre une protection équivalente.

L'ensemble de ces faits constitue un manquement aux obligations de l'article 32 du RGPD. La société devra d'une part, mettre en place un chiffrement de l'ensemble des équipements informatiques nomades de ses salariés.

B. Un manquement aux conditions de désignation du délégué à la protection des données (articles 37 et 38 du RGPD)

En droit, l'article 37 du RGPD impose la désignation d'un délégué à la protection des données dans certaines hypothèses. L'article 38 délimite les contours de ses fonctions. En particulier, le paragraphe 38.6 dispose que *« Le délégué à la protection des données peut exécuter d'autres missions et tâches. Le responsable du traitement ou le sous-traitant veillent à ce que ces missions et tâches n'entraînent pas de conflit d'intérêts ».*

Les lignes directrices concernant les délégués à la protection des données adoptées le 13 décembre 2016 et révisées le 5 avril 2017 par le groupe de travail « Article 29 » sur la protection des données précisent que le délégué à la protection des données « *ne peut exercer au sein de*

l'organisme une fonction qui l'amène à déterminer les finalités et les moyens du traitement de données à caractère personnel ». Il est ajouté : « *En règle générale, parmi les fonctions susceptibles de donner lieu à un conflit d'intérêts au sein de l'organisme peuvent figurer les fonctions d'encadrement supérieur (par exemple, directeur général, directeur opérationnel, directeur financier, médecin-chef, responsable du département marketing, responsable des ressources humaines ou responsable du service informatique), mais aussi d'autres rôles à un niveau inférieur de la structure organisationnelle si ces fonctions ou rôles supposent la détermination des finalités et des moyens du traitement* ».

En outre, dans son guide du délégué à la protection des données, accessible sur le site web de la CNIL, la Commission appelle l'attention des organismes sur le fait que, si le délégué à la protection des données peut occuper d'autres fonctions au sein de la structure, « *toutefois, dans le cadre de ses autres fonctions, il ne doit pas avoir de* ***pouvoir décisionnel sur la détermination des finalités et moyens des traitements*** *: le DPO ne doit donc pas être « juge et partie »* (voir fiche 2 : « Qui peut être désigné DPO »). A titre d'exemples, sont notamment citées les fonctions de directeur général des services, direction des opérations et responsable des ressources humaines.

En l'espèce, la délégation de contrôle de la CNIL a été informée qu'a été désigné comme délégué à la protection des données le directeur général de la société, [redacted] désignation qui a été notifiée à la CNIL en août 2021.

Or la fonction de directeur général fait partie des fonctions « *susceptibles de donner lieu à un conflit d'intérêts* », dès lors qu'il s'agit d'une fonction d'encadrement et qu'à ce titre, il intervient dans la prise de décision sur les traitements de données à caractère personnel.

Or une telle situation peut créer un conflit d'intérêts, en méconnaissance des dispositions de l'article 38.6 du RGPD, dans la mesure où le délégué à la protection des données ne doit pas avoir de pouvoir décisionnel sur la détermination des finalités et des moyens du traitement, ce qui est le cas en l'espèce au vu de ses autres fonctions.

La désignation du représentant légal de la société comme délégué à la protection des données constitue ainsi un manquement aux articles 37 et 38-6 du RGPD. La société devra donc désigner un délégué à la protection des données qui pourra accomplir les missions visées à l'article 39 du RGPD en dehors de tout conflit d'intérêts.

En conséquence, la société EDUSIGN, sise 1, rue du prieuré à Saint-Germain-en-Laye (78100), est mise en demeure sous un délai de 3 (trois) mois à compter de la notification de la présente décision et sous réserve des mesures qu'elle aurait déjà pu adopter, de :

- **prendre les mesures permettant de préserver la sécurité des données et empêcher que des tiers non autorisés y aient accès. L'établissement pourrait :**

  - chiffrer les équipements nomades utilisés par les salariés ;

- **désigner un délégué à la protection des données dont les fonctions permettent d'éviter tout conflit d'intérêts.**

Cette mise en demeure n'appelle pas de réponse de votre part auprès de la CNIL. En revanche, si la persistance ou la réitération des manquements visés dans la mise en demeure était constatée à l'occasion de vérifications ultérieures, je pourrais désigner au sein de la CNIL un rapporteur et saisir la formation restreinte de la CNIL, sans qu'une nouvelle mise en demeure ne vous soit adressée préalablement, afin que soit prononcée, le cas échéant, l'une ou plusieurs des mesures correctrices prévues par les articles 20 et suivants de la loi du 6 janvier 1978.