NEWSLETTER RGPD/DATA

NUMÉRO 68 ● 2025

ACTUALITÉS DU CABINET P. 10

FORMATION À LA PRÉPARATION À LA CERTIFICATION « DPO ».
DATE SUR DEMANDE

SOMMAIRE

PAS DE COMMUNICATION DE L'IDENTITE DU PLAIGNANT

L'autorité de contrôle grecque a prononcé un avertissement à l'encontre d'une commune ayant transmis l'identité et les coordonnées d'un plaignant à la personne contre laquelle la plainte était dirigée.

La transmission de données personnelles d'un plaignant

Un habitant d'une commune, constatant que la porte d'entrée d'un immeuble empiétait sur le trottoir, a signalé cet empiètement à la direction des services techniques de sa commune.

La direction des services techniques a pris en compte la plainte et a adressé, au propriétaire de l'immeuble, un courrier de mise en demeure de retirer l'élément empiétant sur le domaine public, dans lequel était mentionné l'identité et les coordonnées complètes de l'auteur de la plainte.

Ce dernier, apprenant que son identité et ses coordonnées ont été transmises au propriétaire de l'immeuble, a déposé une plainte auprès de l'autorité grecque de contrôle.

La transmission de données personnelles en violation du RGPD

Pour sa défense, la municipalité avançait plusieurs arguments. Elle affirmait :

- D'une part, avoir informé oralement le plaignant de la possible divulgation de ses données personnelles ;
- D'autre part, qu'il appartenait au plaignant d'indiquer, dans sa plainte, s'il souhaitait que ses données restent confidentielles, et ;
- Enfin, que la réglementation grecque permet à toute personne contre laquelle une plainte est dirigée, de demander d'accéder au texte de celle-ci ainsi qu'à l'identité et aux coordonnées du plaignant.

En réponse, l'autorité de contrôle a considéré que :

- Premièrement, la municipalité ne démontrait pas avoir effectivement informé oralement la personne concernée, faute de produire une preuve, un document ou une procédure attestant cette information. Cette absence d'information constitue une violation du principe de transparence, posé à l'article 5§1a), du RGPD ;
- Deuxièmement, et en tout état de cause, la municipalité avait violé le principe de minimisation posé à l'article 5§1c) du RGPD. En effet, compte tenu de la nature de l'infraction alléguée (un litige d'urbanisme), la communication de l'identité et des coordonnées du plaignant n'était pas utile pour régler le litige.

Compte tenu de ce qui précède, l'autorité de contrôle grecque a adressé un avertissement à la municipalité.

Source : ici

REPONSE A UNE DEMANDE DE DROIT D'ACCES : L'INCOHERENCE PEUT COUTER CHER !

L'autorité de contrôle maltaise a sanctionné une banque qui avait répondu de manière incohérente à une demande de droit d'accès.

L'exercice du droit d'accès et la réponse du responsable du traitement

Une personne concernée avait exercé son droit d'accès auprès de sa banque en vue d'obtenir une copie de l'intégralité de ses données à caractère personnel, y compris les courriels internes échangés entre les employés et tous les documents internes la concernant.

La banque a répondu favorablement à cette demande en transmettant la copie de nombreuses données. Toutefois, la réponse était, selon la requérante, incomplète dans la mesure où il manquait la copie des courriels internes échangés entre les employés et tous les documents internes la concernant.

Malgré l'insatisfaction de la requérante, la banque a refusé de transmettre ces éléments au motif que leur transmission porterait atteinte au secret professionnel et au secret bancaire (exception posée à l'article 15(4) du RGPD).

La personne concernée a réitéré sa demande, considérant que cette exception ne lui était pas opposable.

En réponse, la banque lui a indiqué avoir transmis l'intégralité des données personnelles dont elle disposait et qu'elle ne compléterait pas sa réponse initiale.

Face à cette incohérence, la personne concernée a déposé une plainte auprès de l'autorité de contrôle maltaise.

La sanction pour réponse incohérente à la demande de droit d'accès

L'autorité a considéré que la banque avait manqué au principe de transparence, posé à l'article 5(1)a du RGPD, en n'indiquant pas, dès la première réponse, qu'elle s'était fondée sur l'article 15(4) du RGPD pour refuser de transmettre certains éléments. En effet, si la personne concernée n'avait pas insisté, elle n'aurait jamais su que la réponse initiale était incomplète.

L'autorité de contrôle maltaise a également ajouté que la réponse de la banque était contraire au RGPD. En effet, selon l'autorité, le responsable du traitement ne peut pas, d'un côté, prétendre avoir fourni toutes les données à caractère personnel d'une personne et, de l'autre côté, invoquer l'article 15(4) du RGPD pour refuser l'accès à certaines données.

En conséquence, l'autorité de contrôle a adressé un avertissement à la banque et lui a ordonné de répondre à la demande de droit d'accès de la personne concernée.

Source : ici

DECISIONS AUTOMATISEES ET DROIT D'ACCES : LA CJUE CONSACRE UN « DROIT A L'EXPLICATION »

La prise de décisions automatisées, y compris le profilage, impose au responsable de traitement d'observer des règles plus strictes en matière de protection des données personnelles. La CJUE a récemment précisé le périmètre du droit d'accès des personnes concernées par de telles décisions[1].

Pour rappel, le RGPD (article 15 § 1 h)) prévoit que, en cas de prise de décisions automatisées, y compris un profilage[2], la personne concernée a, en vertu de son droit d'accès, le droit d'obtenir des informations supplémentaires et spécifiques à ce type de traitement, parmi lesquelles « *des informations utiles concernant la logique sous-jacente* » à une telle prise de décision. Mais que recouvrent véritablement ces informations ? La CJUE a récemment donné des éléments de réponse.

En l'espèce, une personne s'est vu refuser la conclusion d'un contrat avec un opérateur de téléphonie mobile au motif d'une insuffisante solvabilité. Ce refus a été basé sur une évaluation de crédit de la personne concernée, laquelle avait été réalisée de façon automatisée par une société spécialisée dans ce type d'évaluation.

Dans ce cadre, il a été reproché à la société d'évaluation de ne pas avoir respecté l'article 15 § 1 h) de la personne concernée parce qu'elle (i) n'avait pas fourni « *des informations utiles sur la logique sous-jacente* » à la prise de décision automatisée ; (ii) et, à tout le moins, n'avait pas suffisamment motivé pourquoi elle n'aurait pas pu fournir de telles informations.

A cette occasion, la CJUE a été interrogée sur le point de savoir ce que recouvre cette notion d'« *informations utiles sur la logique sous-jacente* ».

Pour la CJUE, il s'agit pour le responsable du traitement d'expliquer « *la procédure et les principes concrètement appliqués* » et ce, afin que la personne concernée comprenne quelles données à caractère personnel ont été utilisées et de quelle manière « *aux fins d'en obtenir un résultat déterminé* ». Cette explication doit être « *concise, transparente, compréhensible et aisément accessible* ».

A cet égard, la « *complexité des opérations* » ne décharge pas le responsable de traitement de son obligation d'explication, la CJUE ayant notamment précisé que la seule communication d'un algorithme ne saurait, être considérée comme suffisante. En revanche, informer « *de la mesure dans laquelle une variation au niveau des données à caractère personnel prises en compte aurait conduit à un résultat différent* » serait appropriée concernant le type de profilage réalisé en l'espèce.

La CJUE a ajouté que si le responsable de traitement estime que les explications à communiquer comportent des données de tiers protégées ou encore des secrets d'affaires, cela ne saurait suffire, par principe, à les exclure du droit d'accès. En pareil cas, le responsable de traitement doit communiquer ces données/informations protégées à l'autorité de contrôle ou la juridiction compétente. Ce sont alors elles qui évalueront si ces éléments doivent être communiqués en mettant en balance « *les droits et intérêts en cause* ».

Cette décision n'est pas sans conséquence pour les organismes utilisant des algorithmes, outils d'IA et autres systèmes conduisant à une prise de décision automatisée. En effet, ils doivent pouvoir expliquer, de façon simple, comment ces systèmes opèrent et comment les données y sont exploitées pour aboutir à la prise de décision automatisée.

[1] CJUE, 27 février 2025 (Affaire C-203/22).
[2] Au sens de l'article 22 du RGPD.

SANCTION D'UN PHOTOGRAPHE POUR DES PHOTOS DE NU NON CONSENTIES

L'autorité de contrôle autrichienne a sanctionné un photographe ayant outrepassé les souhaits de son modèle quant au sort des photographies réalisées.

Un photographe et une femme s'étaient donnés rendez-vous dans une piscine et s'étaient mis d'accord pour qu'une unique photographie de nu soit prise, avec le smartphone de cette dernière.

Outrepassant cet accord, le photographe a pris plusieurs photographies, puis se les est envoyées sur son propre téléphone.

Ayant eu connaissance de ces agissements, la femme a demandé au photographe de supprimer les photographies, ce qu'il a fait le jour même, expliquant les avoir transférées en vue de les retoucher.

Saisie de cette affaire, l'autorité de contrôle autrichienne a considéré que le photographe avait réalisé des opérations de traitements en s'adressant les photographies sur son téléphone et en les conservant.

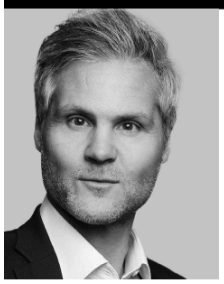
Se faisant, le photographe a violé :

- Le principe de licéité, le traitement ne reposant sur aucune base légale ;
- Le principe de loyauté du traitement, compte tenu du défaut d'information de la personne concernée ;
- Le principe de limitation des finalités, l'autorité autrichienne n'ayant pas été convaincue par le motif de retouche avancé par le photographe ;
- Le principe de minimisation des données, le traitement outrepassant ce qui était nécessaire au regard de sa finalité ;
- L'interdiction de traiter des données liées à la vie sexuelle de la personne concernée.

Compte tenu de ces manquements, l'autorité de contrôle autrichienne a infligé au photographe une amende administrative de 2.000 €.

Source : ici

DOCTRINE



DONNÉES PERSONNELLES

La liberté d'expression doit s'exprimer dans le respect du RGPD

Comme chaque mois, Alexandre Fievée tente d'apporter des réponses aux questions que tout le monde se pose en matière de protection des données personnelles, en s'appuyant sur les décisions rendues par les différentes autorités de contrôle nationales au niveau européen et les juridictions européennes. Ce mois-ci, il se penche sur la question de savoir si un média en ligne peut relayer dans un article une vidéo initialement publiée sur un réseau social.

En application de l'article 85.1 du RGPD, il appartient aux États membres de concilier, par la loi, le droit à la protection des données à caractère personnel et le droit à la liberté d'expression et d'information, y compris le traitement à des fins journalistiques. L'article 85.2 précise les principes, les droits et autres obligations sur lesquels les Etats membres peuvent prévoir des « *exemptions* » ou des « *dérogations* ».

Le législateur français a, dans ce cadre, prévu quelques dérogations au régime de droit commun de la protection des données personnelles. Ainsi, en application de l'article 80 de la loi « *Informatique et libertés* », et lorsque ces dérogations sont nécessaires pour concilier le droit à la protection des données personnelles et la liberté d'expression et d'information, plusieurs principes et droits ne s'appliquent pas, tels que : le principe de limitation de la conservation des données ; le principe d'interdiction de traiter les données dites « *sensibles* » et les données relatives aux condamnations pénales et aux infractions ; le principe de transparence ; le droit d'accès ; le droit de rectification et le droit à la limitation du traitement.

Aucune dérogation au principe de minimisation n'est prévue. C'est vrai en droit français, c'est également vrai en droit espagnol, comme en témoigne l'affaire ci-après, initiée par un particulier espagnol qui reprochait à un média d'avoir publié plus d'informations le concernant que nécessaire.

L'affaire[1]

Un utilisateur du réseau social Twitter avait posté, sur son profil, une vidéo consistant en un montage de prises de vue successives, dans lequel le visage et la voix d'une tierce personne étaient facilement identifiables. Cette vidéo est devenue virale. La personne concernée, qui n'avait jamais donné son autorisation pour une telle publication, a, par la suite, constaté que le site internet d'actualité, El Español, avait mis en ligne un article portant sur la diffusion de cette vidéo sur les réseaux sociaux, article dans lequel il était fait mention de son nom. Cet article, qui contenait un lien vers la vidéo en question, était par ailleurs illustré d'une photographie représentant cette

personne (tirée de la vidéo). Dans cet article, le média faisait état du contenu de la vidéo (en soulignant certains dialogues), mais aussi de sa large diffusion sur les réseaux sociaux et des milliers de commentaires auxquels elle avait donnés lieu (certains commentaires étant retranscrits dans l'article).

La personne concernée a déposé une plainte auprès de l'autorité espagnole de protection des données (l'AEPD). Cette dernière a rappelé que l'entité qui effectue un traitement – en l'occurrence « *l'inclusion de l'image d'une personne ou d'une vidéo contenant son image et sa voix dans des publications journalistiques* » - est tenue de respecter les principes du RGPD et les obligations en matière de protection des données personnelles, précisant, à cet égard, que « *ces principes et obligations ne sont pas diminués par le fait que le responsable du traitement des données est un média* ».

Ainsi, le média aurait dû, selon l'AEPD, tenir compte du principe de minimisation, ce qu'il n'a pas fait : « *El Español aurait dû examiner si la finalité de l'information exigeait la diffusion de l'image et de la voix du plaignant contenues dans la vidéo sans y avoir appliqué un quelconque processus d'anonymisation, ou si l'indication du nom dans le texte de l'article publié était réellement nécessaire, ou si cette finalité, au contraire, était parfaitement réalisable sans l'identification de la personne concernée.* »

Pour l'autorité, la circonstance selon laquelle le média n'aurait fait qu'insérer dans un article une vidéo déjà publiée par un tiers sur son compte Twitter est indifférente : « *L'existence d'éventuelles violations antérieures par des tiers n'exempte pas les médias de l'obligation d'effectuer une analyse de risque avant la publication d'articles. El Español, en tant que média et responsable du traitement, décide de ce qu'il publie et de la manière dont il le fait. Il peut décider de publier la vidéo telle quelle, de ne pas la publier ou de déformer l'image et la voix du plaignant afin qu'il ne soit pas reconnaissable par des tiers.* »

Enfin, l'AEPD a souligné, en réponse à l'argument du média selon lequel il ne pourrait être responsable de la publication d'une vidéo qui a pu initialement être diffusée par la personne concernée elle-même, que « *même si une telle diffusion intentionnelle a pu avoir lieu, elle ne peut être interprétée dans le sens voulu par El Español dans ses allégations* » car, en tout état de cause, « *seule la personne concernée a le droit de décider de l'utilisation de ses données personnelles (...) et cela ne change pas que les données personnelles soient accessibles via internet, et ce quelle que soit leur origine.* »

Partant, l'autorité espagnole de protection des données a estimé que « *le traitement effectué par El Español dans le cadre de la liberté d'expression a été excessif, car il n'y avait pas d'intérêt public dans la diffusion de l'image et de la voix du plaignant, avec l'indication de son nom.* ». Une amende administrative d'un montant de 10 000 euros a été prononcée à l'encontre du média.

Quelles recommandations ?

Jusqu'à présent, pour mettre en cause un média, il fallait généralement démontrer que le contenu litigieux est injurieux, diffamatoire ou qu'il porte atteinte à la vie privée. ÀA l'appui de cette décision (mais aussi d'autres que nous avons eu l'occasion de commenter), il semble désormais acquis qu'une contestation de la licité d'un article est possible sur un autre fondement que la loi de 1881 (loi sur la liberté de la presse) ou l'article 9 du cCode civil (droit au respect de la vie privée). Ce nouveau fondement est le principe de minimisation, tel que visé à l'article 5.1.c) du RGPD.

Mais qu'on se le dise, la liberté d'expression n'est pas menacée. Un juste équilibre doit être trouvé entre ce droit fondamental et celui de la protection des données à caractère personnel, afin d'éviter la diffusion excessive de données non pertinentes au regard de la finalité poursuivie.

Alexandre FIEVÉE
Avocat associé
DERRIENNIC ASSOCIES

Notes

(1) AEPD, EXP202309208, 19 juin 2024.

(2) « Oui, les organes de presse sont bien soumis au RGPD ! », Expertises, juillet 2024, Alexandre FIEVEE.

Vous avez envie de vous exprimer sur un sujet qui vous tient à cœur, de partager votre analyse avec la communauté des lecteurs d'Expertises, d'exposer un point de vue différent sur un article déjà publié, de lancer un débat sur un thème émergent, ou simplement de commenter l'actualité du droit du numérique ?

Contactez la rédactrice en chef d'Expertises Sylvie Rozenfeld sr@expertises.info

DOCTRINE

DONNÉES PERSONNELLES

Cloud non-souverain et données de santé : *le Conseil d'Etat au secours de la Cnil*

Le Conseil d'Etat a récemment rendu plusieurs décisions[1], par lesquelles il confirme la possibilité pour le Groupement d'intérêt public Plateforme des données de santé (le « Health Data Hub ») de recourir à Microsoft pour l'hébergement d'un entrepôt de données de santé. Est-ce que cela signifie qu'il est donc possible d'héberger des données de santé sur des cloudnon-souverains ?

Le Health Data Hub, « *chargé par la loi de recueillir les bases de données de santé les plus importantes du pays* », a conclu un contrat de services avec l'Agence européenne du médicament (EMA). Ce contrat porte notamment sur « *la constitution d'un entrepôt de données de santé visant à permettre des recherches, études et évaluations en pharmaco-épidémiologie* ». « *Un appariement entre une fraction des données de la base principale du système national des données de santé (SNDS) et les dossiers médicaux fournis par quatre établissements partenaires en France* » y est prévu. Ce projet est dénommé « *EMC2* ».

Le cas de l'entrepôt de données de santé « EMC2 » du Health Data Hub

Pour mémoire, la Cnil a publié un référentiel relatif « *aux traitements de données à caractère personnel mis en œuvre à des fins de création d'entrepôts de données de santé dans le domaine de la santé* ». Ce référentiel concerne uniquement les traitements « *nécessaire[s] à l'exercice d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable de traitement* ». Ainsi, un organisme, responsable de traitement, souhaitant mettre en œuvre un entrepôt de données de santé doit, par principe, s'assurer de sa conformité à ce référentiel. Dans le cas où l'organisme considère être en stricte conformité avec le référentiel, il peut alors se contenter d'une déclaration de conformité auprès de la Cnil. Dans l'hypothèse, en revanche, où il existe des écarts avec les exigences prévues au référentiel, il appartient à l'organisme de saisir la Cnil d'une demande d'autorisation spécifique préalable. Dans la mesure où le projet « *EMC2* » ne répondait pas à toutes les exigences prévues dans ledit référentiel, en particulier celles relatives au sous-traitant, le Health Data Hub avait saisi la Cnil d'une demande d'autorisation.

À noter, en particulier, que le projet « *EMC2* » prévoyait de recourir à l'hébergeur Microsoft Ireland Ltd (avec la solution Microsoft Azure), société irlandaise, dont la maison mère est située aux Etats-Unis. Le risque d'accès par des tiers à des données personnelles sensibles a été un des points d'attention de la Cnil.

Une analyse de la Cnil sujette à débats

Dans sa décision[2], la Cnil a relevé plusieurs éléments semblant pencher pour un refus d'autorisation. Tout d'abord, la Cnil a estimé qu'il existe – en dépit du « *Data Privacy Framework* » (à savoir la décision d'adéquation du 10 juillet 2023 reconnaissant que le cadre de transfert des données à caractère personnel « *Etats-Unis/UE* » assure un niveau de protection adéquat) - bien un risque d'accès aux données par les autorités américaines puisque la maison mère de la société Microsoft Ireland Ltd est située aux Etats-Unis (et donc soumise au droit de cet Etat).

La Cnil a ensuite rappelé sa recommandation « *pour les bases de données les plus sensibles* », selon laquelle il appartient à l'organisme de ne faire appel qu'à un hébergeur exclusivement soumis au droit européen et certifié « *SecNumCloud* ». À cet égard, la Cnil a indiqué que les entrepôts de données de santé appariés avec le SNDS doivent faire l'objet d'une vigilance particulière (« *malgré le fait que ces données soient pseudonymisées* »), dans la mesure où « *la CNIL a toujours demandé aux porteurs de projet, publics et privés, de s'assurer que l'hébergeur des données n'est pas soumis à une législation extra-européenne* ». La circulaire de la Première Ministre du 31 mars 2023 demandait d'ailleurs, comme l'a souligné la Cnil, que les autorités publiques s'assurent que « *les données 'd'une sensibilité particulière' hébergées dans le cloud ne soient pas soumises à des lois extra-européennes* ». La Cnil en a conclu que le choix du Health Data Hub « *apparaît en très nette contradiction avec [ces] éléments* ».

Mais d'autres éléments ont conduit la Cnil à refaire pencher la balance... La Cnil a, d'une part, déploré qu'aucun prestataire, susceptible de répondre actuellement aux besoins exprimés par le Health Data Hub, « *ne protège les données contre l'application de lois extraterritoriales de pays tiers* » (alors que, selon la Cnil, « *le projet EMC2 aurait pu être retenu par le [Health Data Hub] pour préfigurer la solution souveraine vers laquelle il doit migrer* »), et, d'autre part, souligné « *qu'il est nécessaire que les engagements pris vis-à-vis de [l'Agence européenne du médicament] puissent être honorés* ».

La Cnil a alors décidé d'autoriser la mise en œuvre de l'entrepôt de données de santé « *EMC2* » avec un hébergement chez Microsoft pour une durée de 3 ans (durée de la migration de la plateforme).

Cette décision a fait l'objet de plusieurs critiques dans la mesure où elle reconnaît notamment le non-respect du projet « *EMC2* » à des exigences nationales de souveraineté tout en validant ce projet, tandis que d'autres projets similaires hébergés par Microsoft avaient été refusés par la Cnil. Plusieurs organismes ont saisi le Conseil d'Etat en annulation pour excès de pouvoir de la décision de la Cnil, notamment l'association Internet Society France[3]. À cette occasion, plusieurs requérants ont remis en cause la légalité du « *Data Privacy Framework* ».

La position de la Cnil, validée par le Conseil d'Etat

Dans un premier temps, le Conseil d'Etat a souligné que l'objet de l'autorisation de la Cnil portait sur « *la création d'un entrepôt de données de santé, hébergées dans des centres de données situés en France* » et non pas sur « *un transfert de données personnelles vers les Etats-Unis* », sachant que seules les « *données techniques d'usage de la plateforme* » sont susceptibles de faire l'objet d'un tel transfert. Ce faisant, le Conseil d'Etat a considéré que les critiques portant sur l'illégalité du « *Data Privacy Framework* » et la méconnaissance par la Cnil de textes encadrant le transfert de données à caractère personnel vers des pays tiers[4], en l'occurrence les Etats-Unis, n'avaient pas lieu d'être.

Dans un deuxième temps, le Conseil d'Etat a analysé la critique selon laquelle la décision de la Cnil méconnaîtrait l'article 28.1 du RGPD, en application duquel le sous-traitant – ici Microsoft Ireland Ltd – doit présenter des « *garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du présent règlement et garantisse la protection des droits de la personne concernée* ». Sur ce point, la Haute Juridiction a jugé que, certes, le risque « *ne peut être totalement exclu* » que les autorités américaines, « *sur le fondement des lois de ce pays, par l'intermédiaire de la société-mère de l'hébergeur* », puissent faire des demandes d'accès aux données du traitement autorisé, données qualifiées « *d'une sensibilité particulière eu égard à leur nature de données de santé mais aussi au potentiel scientifique et économique de leur exploitation* ». Pour autant, le Conseil d'Etat a relevé plusieurs éléments permettant de justifier le respect des dispositions de l'article 28.1 du RGPD, à savoir : (i) la pseudonymisation multiple des données par la Caisse nationale d'assurance maladie et par le Health Data Hub « *avant toute mise à disposition au sein de l'entrepôt « EMC2* », (ii) la certification « *HDS* » de Microsoft Ireland Ltd « *qui implique un audit régulier par un organisme accrédité* » (en ayant, par ailleurs, relevé que Microsoft Ireland Ltd « *ne peut bénéficier de la certification « SecNumCloud* » délivrée par (...) [l'ANSSI] dès lors qu'elle est la filiale d'une société soumise au droit des Etats-Unis ») et (iii) la durée de l'autorisation de la Cnil, limitée à 3 ans.

En troisième lieu, le Conseil d'Etat a estimé que, au regard des éléments et des finalités d'intérêt public poursuivies par le traitement, il n'y avait pas « *d'atteinte disproportionnée au droit à la vie privée* ».

Enfin, la Haute Juridiction a relevé notamment que la « *méconnaissance des prescriptions de la doctrine d'utilisation de l'informatique en nuage par l'Etat* » - à savoir la circulaire de la Première Ministre susvisée – par la Cnil étant sans incidence. La Cnil n'est effectivement pas contrainte de respecter une telle doctrine.
En conséquence, le Conseil d'Etat a rejeté les recours.

Que peut-on en retenir ?

La Haute Juridiction a validé la décision de la Cnil admettant donc la possibilité d'un hébergement temporaire de données de santé sur un cloud non-souverain, faute de mieux.

Des garanties telles que la pseudonymisation, la certification HDS (bien que moins exigeante que la certification « *Secnumcloud* ») et ce, pour des finalités spécifiques d'intérêt public et une durée limitée du traitement concerné peuvent permettre de « *légaliser* », dans une certaine mesure, un hébergement de données de santé sur un cloud non-souverain.

La prudence reste toutefois de mise compte tenu du contexte particulier du traitement objet du projet « *EMC2* » et des travaux gouvernementaux à venir sur la mise en place / l'exigence d'un cloud souverain.

À suivre...

Alexandre FIEVEE
Avocat associé

Alice ROBERT
Avocate of Counsel

Derriennic Associés

Notes

(1) Conseil d'Etat, 13 novembre 2024, décision n°475297 ; Conseil d'Etat, 13 novembre 2024, décision n°492895 ; Conseil d'Etat, 19 novembre 2024, décision n°491644.

(2) Délibération Cnil 21 décembre 2023, publiée le 31 janvier 2024.

(3) À noter que d'autres recours ont été formés devant le Conseil d'Etat sur la même problématique, en l'occurrence concernant la décision de refus du ministère des solidarités et de la santé de prendre « les mesures propres à éliminer la violation du (...) (RGPD) résultant de l'hébergement des données de la Plateforme des données de santé par la société Microsoft ».

(4) À savoir les articles 44 à 48 du RGPD sur les transferts de données à caractère personnel vers des pays tiers et l'article R.1461-1 du code de la santé publique qui dispose en son dernier alinéa « Les données du système national des données de santé sont hébergées au sein de l'Union européenne. Aucun transfert de données à caractère personnel ne peut être réalisé en dehors de l'Union européenne, sauf dans le cas d'accès ponctuels aux données par des personnes situées en dehors de l'Union européenne, pour une finalité relevant du 1° du I de l'article L.1461-3 ».

ACTUALITÉS DU CABINET

DERRIENNIC ASSOCIÉS PROPOSE UN PROGRAMME DE FORMATION DE 35 HEURES POUR LA PRÉPARATION À LA CERTIFICATION DPO

OBJECTIFS

1/ Acquérir les compétences, les connaissances et le savoir-faire attendus par la CNIL et permettre au collaborateur de se présenter à l'examen de certification en maximisant ses chances de succès.
2/ Indépendamment de la certification, la formation permet à l'apprenant de se familiariser avec la matière et d'acquérir les compétences, les connaissances et le savoir-faire pour :

- analyser une situation impliquant un traitement de données personnelles ;
- définir et appréhender les problématiques, les enjeux et les risques qui en découlent ;
- prendre les décisions qui s'imposent en concertation avec l'équipe « DPO ».

CONTENU DE LA FORMATION

Partie 1 : Réglementation générale en matière de protection des données et mesures prises pour la mise en conformité
Partie 2 : Responsabilité (Application du principe d'« Accountability »)
Partie 3 : Mesures techniques et organisationnelles pour la sécurité des données au regard des risques

COÛT

4.000 € HT/personne

INTERVENANT

Alexandre FIEVEE
Avocat Associé
01.47.03.14.94
afievee@derriennic.com

CLASSEMENTS
Alexandre Fievee figure dans le classement BestLawyers dans la catégorie « *Information Technology Law* » (2024).

Il a également fait en 2020 son entrée dans le classement Legal 500 dans la catégorie *« Next* Generation Partners ».

Enfin, en 2025, il fait son entrée dans le classement Chambers France, se positionnant en Band 3 dans le classement individuel Data Protection.

RENSEIGNEMENTS PRATIQUES
Prochaine session en 2025 :
Sur demande.
Lieu de la formation :
Au cabinet Derriennic Associés (5 avenue de l'opéra - 75001 Paris) ou en visio-conférence.
Inscription et informations :
afievee@derriennic.com