La Newsletter dédiée à la mise en conformité au RGPD

par @DerriennicParis

DERRIENNIC ASSOCIÉS

Conformité RGPD

#NewsDerriennicRGPD 16

Madame, Monsieur,

Nous vous proposons, en cette période estivale, une lettre RGPD composée des actualités suivantes :

- La poursuite de la navigation ne vaut plus consentement à l'utilisation des cookies ;
- Défaut de sécurité et non-respect des durées de conservation : 400.000 € d'amende ;
- DPO : Le profil type ;
- Les moteurs de recherche peuvent-ils traiter des données relatives aux infractions ? ;
- 180 000 euros pour atteinte à la sécurité des données.

Nous vous en souhaitons une bonne lecture.

La poursuite de la navigation ne vaut plus consentement à l'utilisation des cookies

Le 18 juillet 2019, la CNIL a publié une délibération n° 2019-093 portant adoption de lignes directrices relatives à l'application de l'article 82 de la loi du 6 janvier 1978, lequel concerne l'utilisation des cookies et autres traceurs.

Comme elle l'a annoncé le 28 juin dernier, la CNIL a actualisé ses cadres de référence sans attendre le futur règlement « vie privée et communications électroniques » actuellement en discussion au niveau européen.

Pour rappel, jusqu'alors, la position de la CNIL consistait à recommander l'usage d'un « bandeau cookie » assorti d'une page « en savoir plus » permettant de paramétrer les cookies et autres traceurs. Lorsque l'utilisateur, informé par le bandeau cookie conformément aux recommandations de la CNIL, décidait de poursuivre sa navigation sur le site internet, la CNIL considérait que son consentement avait été valablement donné.

En application de cette nouvelle délibération :

- d'une part, la simple poursuite de la navigation sur un site ne peut plus être regardée comme une expression valide du consentement au dépôt des cookies ;
- d'autre part, les opérateurs exploitant des traceurs doivent être en mesure de prouver qu'ils ont bien recueilli le consentement des internautes.

Cette délibération sera suivie d'une nouvelle recommandation, qui précisera les modalités pratiques de recueil du consentement. Ce projet de recommandation, élaboré à l'issue d'une concertation avec les professionnels et la société civile, devrait faire l'objet d'une publication définitive au premier trimestre 2020.

A l'issue de cette publication, les acteurs bénéficieront d'une période d'adaptation de 6 mois pour se plier aux nouvelles règles.

Lien vers les résultats de l'enquête :

https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000038783337

Défaut de sécurité et non-respect des durées de conservation : 400.000 € d'amende

La CNIL a prononcé une sanction de 400.000 € à l'encontre de la société SERGIC pour avoir insuffisamment protégé les données des utilisateurs de son site internet et n'avoir pas mis en œuvre des modalités de conservation des données appropriées.

Le 12 août 2018, la CNIL a été saisie d'une plainte d'un utilisateur du site de www.sergic.com, édité par la société SERGIC, spécialisée dans la promotion immobilière, l'achat, la vente, la location et la gestion immobilière.

Le plaignant indiquait qu'une modification d'un caractère dans l'adresse url du site permettait, sans authentification préalable, d'accéder aux pièces justificatives mises en lignes par des candidats à la location. Ces allégations ont été confirmées par un contrôle en ligne, puis sur place, de la CNIL, les 7 et 13 septembre 2018.

Le correctif mettant fin à la vulnérabilité a été mis en production par la société SERGIC le 17 septembre 2018, étant toutefois précisé que cette dernière avait connaissance de ladite vulnérabilité dès le 8 mars 2018. La société SERGIC a également procédé à la notification de la violation de données aux personnes concernées.

A l'issue du contrôle sur place, deux manquements sont constatés par la CNIL, l'un concernant la sécurité des données (1.), l'autre l'obligation de conserver les données pour une durée proportionnée (2.).

1. S'agissant du manquement à l'obligation d'assurer la sécurité des données, la CNIL relève que le libre accès aux documents conservés par la société traduisait « *une conception défectueuse du site, caractérisée en l'espèce par l'absence de mise en place d'une procédure d'authentification des utilisateurs.* » et que l'exploitation de la vulnérabilité « *ne requérait pas de maîtrise technique particulière en matière informatique* »

Elle estime que la société SERGIC n'a pas « *mis en œuvre les mesures techniques et organisationnelles appropriées afin de garantir la sécurité des données personnelles traitées, conformément à l'article 32 du Règlement* ». Ce manquement est, selon elle, « *aggravé au regard de la nature des données à caractère personnel rendues accessibles* ».

2. S'agissant du manquement à l'obligation de conserver les données pour une durée proportionnée, le rapporteur « *reproche à la société SERGIC de conserver les documents transmis par les candidats n'ayant pas accédé à la location au-delà de la durée nécessaire à l'atteinte de la finalité pour laquelle les données personnelles ont été collectées et traitées – à savoir la location d'un bien immobilier - et ce sans que cette conservation ne soit encadrée par des garanties appropriées.* »

La société SERGIC justifie la durée de conservation des données en indiquant que les personnes concernées étaient susceptibles de saisir le Défenseur des droits en alléguant d'une discrimination, pendant un délai de prescription de six ans.

La formation restreinte de la CNIL lui rétorque que la durée de conservation des données personnelle doit être déterminée en fonction de la finalité poursuivie par le traitement, et que « *lorsque cette finalité est atteinte, les données doivent soit être supprimées, soit faire l'objet d'un archivage intermédiaire lorsque leur conservation est nécessaire pour le respect d'obligations légales ou à des fins précontentieuses ou contentieuses. Ces données doivent alors être placées en archivage intermédiaire, pour une durée n'excédant pas*

celle nécessaire aux finalités pour lesquelles elles sont conservées, conformément aux dispositions en vigueur. Ainsi, après avoir opéré un tri des données pertinentes à archiver, le responsable de traitement doit prévoir, à cet effet, une base de données d'archives dédiée ou une séparation logique dans la base de données active. Cette séparation logique est assurée par la mise en place de mesures techniques et organisationnelles garantissant que seules les personnes ayant un intérêt à traiter les données en raison de leurs fonctions, comme par exemple les personnes du service juridique, puissent y accéder. Au-delà de ces durées de conservation des données versées en archives intermédiaires, les données personnelles doivent être supprimées. »

En l'espèce, la formation restreinte rappelle que la collecte a pour finalité l'attribution de logement et que « *dès lors que cette finalité est atteinte, les données personnelles des candidats n'ayant pas accédé à la location ne peuvent plus être conservées au-delà de trois mois, au sein de la base de données active et au-delà faire l'objet d'une séparation logique voire d'un archivage intermédiaire.* »

La CNIL relève un manquement à l'obligation de conservation des données, pour les raisons suivantes : « *la société SERGIC conservait en base active les données à caractère personnel des candidats n'ayant pas accédé à la location pour une durée excédant dans des proportions importantes celle nécessaire à la réalisation de la finalité du traitement, à savoir l'attribution de logements, sans qu'aucune solution d'archivage intermédiaire n'ait été mise en place*. »

En défense, la société SERGIC argue que les manquements qui lui étaient reprochés auraient pu être corrigés dans le cadre d'une mise en demeure, or, en l'espèce la CNIL a engagé une procédure de sanction, sans mise en demeure préalable, ce qui l'aurait privée de la possibilité de se mettre en conformité.

La CNIL répond à cela que le prononcé d'une sanction n'est pas subordonné à l'adoption préalable d'une mise en demeure :

« *La décision de désigner un rapporteur et de saisir la formation restreinte est un pouvoir appartenant au Président de la CNIL, qui dispose de l'opportunité des poursuites et peut donc déterminer , en fonction des circonstances de l'espèce, les suites à apporter à des investigations en clôturant par exemple un dossier, en prononçant une mise en demeure ou en saisissant la formation restreinte en vue du prononcé d'une ou plusieurs mesures correctrices.* »

Lien vers la délibération de la CNIL :

https://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000038552658&fastReqId=119744754&fastPos=1

DPO : Le profil type

Le ministère du Travail a confié à l'Agence pour la Formation Professionnelle des Adultes (l'AFPA) la réalisation d'une enquête en ligne ayant pour objet de mieux comprendre les conditions d'exercice, les formes d'emploi ou d'activité, les parcours ou compétences détenues ou attendues pour l'exercice du métier de délégué à la protection des données (ou data privacy officer, « DPO »). Les résultats de cette enquête, réalisée en mars et avril 2019, dressent le profil type du DPO.

Selon les résultats de l'enquête, le DPO type est une femme ou un homme de plus de 40 ans, cadre ou cadre supérieur, ayant reçu une formation supérieure et ayant un parcours professionnel dans le domaine de l'informatique ou du juridique. Le DPO interne d'une entreprise exerce typiquement cette fonction en CDI.

Il est rattaché à la direction générale 49% du temps (contre 16,5% pour la DSI, 12,9% pour la direction juridique et 10,4% pour la direction conformité-risque-qualité), avec un positionnement hiérarchique de N-1 par rapport au responsable du traitement, dans 53,40% des cas.

Le DPO type a moins de 2 ans d'expérience dans le domaine « Informatique et Libertés » et n'a pas été « Correspondant Informatique et Libertés ». Il exerce ses missions de DPO à temps partiel, en complément de son activité initiale

Il n'a pas d'équipe ni de budget dédié.

Les principales missions de ce DPO type, outre la gestion des contrats de sous-traitance et de co-responsabilité, sont les suivantes :

- cartographier les traitements et établir le registre (23,4% du temps dédié) ;
- sensibiliser le responsable de traitement et les directions (14,2% du temps dédié) ;
- mettre en conformité les traitements existants (13,9% du temps dédié) ;
- veiller à la conformité des nouveaux traitements (11,9% du temps dédié) ;
- assurer une veille, intégrer les nouveautés légales et doctrinales (11,6% du temps dédié)

Les DPO se répartissent quasiment à part égale, s'agissant de leur domaine d'expertise d'origine, entre l'informatique (34%) et le juridique (31%).

Les entreprises ont généralement recours aux DPO externes lorsque les données personnelles concernent moins de 10 000 personnes, alors que les DPO internes mutualisés sont majoritaires lorsque les données personnelles concernent plus de 10 000 personnes.

Lien vers les résultats de l'enquête :

https://travail-emploi.gouv.fr/IMG/pdf/rgpd-metier-dpo-premiers-resultats-072019.pdf

Les moteurs de recherche peuvent-ils traiter des données relatives aux infractions ?

La première chambre civile de la Cour de cassation a, le 5 juin 2019, rendu un arrêt par lequel elle a posé une question préjudicielle à la CJUE sur le point de savoir si l'exploitant d'un moteur de recherche est soumis à l'interdiction de traiter des catégories particulières de données, au sens de l'article 8 de la directive du 24 octobre 1995, ainsi que des données relatives aux infractions, aux condamnations pénales et aux mesures de sûreté.

Un particulier exerçant la profession d'expert-comptable et de commissaire aux comptes a été déclaré coupable d'escroquerie et de tentative d'escroquerie par jugement du tribunal correctionnel de Metz, confirmé par un arrêt de la Cour d'appel de Metz rendu le 9 octobre 2013.

Par la suite, ce particulier a demandé à la société Google LLC de supprimer des liens redirigeant vers deux comptes rendus d'audience relatant cette condamnation pénale, publiés sur le site internet du journal « Le Républicain lorrain ».

Après que la société Google LLC lui ait opposé une fin de non-recevoir, le particulier a assigné cette dernière en référé, en se fondant sur son droit d'opposition, aux fins de déréférencement desdits liens.

Le particulier faisait ici grief à la décision de référé d'avoir rejeté sa demande de déréférencement alors même que l'article 9 de la loi n°78-17 du 6 janvier 1978, dans sa rédaction applicable en l'espèce, restreignait la mise en œuvre des traitements de données à caractère personnel relatives aux infractions, condamnations et mesures de sûreté, à une liste de personnes limitativement énumérées, parmi lesquelles ne figurent pas les exploitants de moteur de recherche.

La Cour de cassation a sursis à statuer jusqu'au prononcé de la décision de la CJUE, laquelle a été saisie par le Conseil d'Etat, le 24 février 2017, de plusieurs questions préjudicielles, parmi lesquelles :

> « Eu égard aux responsabilités, aux compétences et aux possibilités spécifiques de l'exploitant d'un moteur de recherche, l'interdiction faite aux autres responsables de traitement de traiter des données relevant des paragraphes 1 et 5 de l'article 8 de la directive du 24 octobre 1995, sous réserve des exceptions prévues par ce texte, est-elle également applicable à cet exploitant en tant que responsable du traitement que constitue ce moteur? »

D'autres questions étaient également posées par le Conseil d'Etat, notamment sur le point de savoir si, en cas de réponse positive à cette première question, l'exploitant d'un moteur de recherche devait faire systématiquement droit aux demandes de déréférencement portant sur des liens menant vers des pages web qui traitent de telles données.

A l'inverse, en cas de réponse négative à la première question, le Conseil d'Etat s'est interrogée sur le point de savoir quelles exigences spécifiques l'exploitant d'un moteur de recherche devait satisfaire, compte tenu de ses responsabilités, de ses compétences et de ses possibilités. De plus, le Conseil d'Etat a interrogé la CJUE afin de savoir si, lorsqu'un exploitant de moteur de recherche constate que des pages web vers lesquelles mènent les liens dont le référencement est demandé comportent des données dont la publication, sur lesdites pages, est illicite, les dispositions de la directive du 24 octobre 1995 doivent-elles être interprétées en ce sens :

- qu'elles imposent à l'exploitant d'un moteur de recherche de

supprimer ces liens de la liste des résultats affichés à la suite d'une recherche effectuée à partir du nom du demandeur ?

- ou qu'elles impliquent seulement qu'il prenne en compte cette circonstance pour apprécier le bien-fondé de la demande de déréférencement ?

- ou que cette circonstance est sans incidence sur l'appréciation qu'il doit porter ?

Lien vers la décision de la Cour de cassation :

https://www.legifrance.gouv.fr/affichJuriJudi.do?oldAction=rechJuriJudi&idTexte=JURITEXT000038629608&fastReqId=240051588&fastPos=1

180 000 euros pour atteinte à la sécurité des données

Par délibération du 18 juillet 2019, la formation restreinte de la CNIL a prononcé, une nouvelle fois, une sanction à l'encontre d'une société n'ayant pas mis en œuvre les mesures nécessaires afin d'assurer un niveau de sécurité adéquate des données à caractère personnel.

ACTIVE ASSURANCES est une société ayant une activité d'intermédiaire en assurance, concepteur et distributeur de contrats d'assurance automobile à des particuliers, en vente directe ou en vente en ligne. Pour les besoins de son activité, la société édite le site web www.activeassurances.fr, sur lequel les personnes peuvent demander des devis ou souscrire des contrats d'assurance automobile.

Après avoir été alertée par un client d'ACTIVE ASSURANCES, la CNIL a, au cours d'une mission de contrôle en ligne en date du 28 juin 2018, constaté qu'une requête effectuée à partir des mots clés « client.activeassurances.fr » et « site:client.activeassurances.fr » faisait apparaître des liens hypertextes permettant d'accéder librement à certains comptes de clients de la société, sans authentification préalable. La CNIL a ainsi pu avoir accès aux nom, prénom, adresse postale, adresse électronique et numéro de téléphone des personnes concernées et a été en mesure de télécharger plusieurs documents PDF concernant ces personnes.

La société a été informée par téléphone le même jour, par la CNIL, de l'existence du défaut de sécurité sur son site, sans que cette information ne constitue une mise en demeure. Un courrier électronique contenant le type d'adresses URL concernées lui a également été adressé. Il était demandé à la société de prendre les mesures correctives nécessaires pour y remédier dans les plus brefs délais afin d'éviter tout accès aux données personnelles par des tiers non autorisés. A la suite de cette information, ACTIVE ASSURANCES a assuré que des mesures avaient été prises afin de remédier au défaut de sécurité.

Le 12 juillet suivant, lors de la mission de contrôle dans les locaux de la société, cette dernière a, en effet, informé la délégation qu'elle avait pris des mesures dès le 29 juin afin que les documents de ses clients ne soient plus accessibles à des tiers non autorisés. Elle a ainsi précisé « avoir modifié le code source du site web ne générant pas d'authentification des personnes pour accéder à leur espace client, ainsi que le paramétrage des documents stockés sur le service Microsoft Azure, celui-ci étant, avant l'alerte de la CNIL, configuré de telle sorte que les fichiers étaient accessibles publiquement depuis internet ». La CNIL a, suite à ces déclaration, effectué une requête à partir des mots clés client.activeassurances.fr site:client.activeassurances.fr dans les moteurs de recherche Bing, Qwant et Yahoo. Elle a constaté qu'une liste de liens hypertextes renvoyant vers les comptes clients était toujours affichée dans les résultats de recherche mais que ceux-ci renvoyaient vers la page de connexion à l'espace client ou vers un message d'erreur « ResourceNotFound ».

La CNIL a également constaté que les mots de passe de connexion des clients à leur espace personnel, dont le format était imposé par la société, correspondaient à leur date de naissance et que ce format était indiqué sur les formulaires de connexion. Il a également été constaté que, après la création de leur compte, l'identifiant et le mot de passe de connexion étaient transmis aux clients par courriel et indiqués en clair dans le corps du message.

Ainsi, tout en soulignant la diligence de la société ACTIVE ASSURANCES qui a réagi rapidement après la révélation de l'incident pour le corriger, la formation restreinte a relevé que les mesures élémentaires de sécurité n'avaient pas été prises en amont du développement de son site web, ce qui a rendu possible la survenance de la violation de données à caractère personnel.

Elle a ainsi relevé que la violation de données à caractère personnel aurait pu être évitée si, par exemple :

- la société avait mis en œuvre une mesure d'authentification et une gestion des droits d'accès permettant de s'assurer que chaque utilisateur souhaitant accéder à un document était habilité à le consulter ;
- la société avait mis en place de mesures permettant de limiter l'indexation des documents par les moteurs de recherche, au moyen, par exemple, d'un fichier robot.txt ;
- la société avait imposé aux utilisateurs l'utilisation de mots de passe plus robustes et ne les avait pas transmis en clair par courriel.

Par ailleurs, la CNIL a souligné que l'accès aux données ne nécessitait aucune opération complexe ni aucune maitrise technique particulière en matière informatique et a concerné un nombre « particulièrement important » de données à caractère personnel et de documents concernant les clients de la société.

De surcroit, « le formulaire de connexion des clients à leur espace personnel indiquait expressément le format des mots de passe de connexion, à savoir la date de naissance des personnes, ce qui facilitait considérablement une attaque par force brute, ce d'autant que le format des mots de passe était indiqué sur le formulaire de connexion au compte client. La formation restreinte relève également que les clients désirant renforcer la sécurité de leurs données et modifier leur mot de passe en étaient empêchés par la société qui avait imposé le format relatif à la date de naissance ».

La CNIL a également constaté qu'« aucune mesure complémentaire pour l'authentification des personnes, telle qu'une limitation du nombre de tentatives en cas de mots de passe erronés, n'avait été mise en place ».

Le manquement à l'article 32 du RGPD étant établi, la CNIL a prononcé à l'encontre d'ACTIVE ASSURANCES une amende administrative d'un montant de 180.000 €.

Lien vers la décision :
https://www.legifrance.gouv.fr/affichCnil.do?id=CNILTEXT000038810992