NEWSLETTER RGPD

NUMÉRO 33 • JUIN 2021

ACTUALITE DU CABINET

FORMATION A LA PREPARATION A LA CERTIFICATION «DPO».

Le cabinet organise régulièrement des programmes de formation visant à la préparation des apprenants à l'examen de certification «DPO».

Retrouvez notre programme à la fin de notre newsletter. **P13**

SOMMAIRE

COOKIES :

LA CNIL MET EN DEMEURE 20 ENTITES

LA CNIL A ADRESSE, LE 18 MAI 2021, UNE VINGTAINE DE MISES EN DEMEURE A L'ATTENTION D'ORGANISMES N'OFFRANT PAS AUX INTERNAUTES LA POSSIBILITE DE REFUSER DES COOKIES AUSSI FACILEMENT QUE DE LES ACCEPTER.

Pour rappel, la CNIL a, le 1er octobre 2021, fait évoluer sa position en matière de cookies par l'adoption de nouvelles recommandations et lignes directrices. La CNIL exige notamment que le consentement à l'utilisation des cookies réponde aux conditions posées par le RGPD, et que les internautes soient en mesure de refuser les cookies aussi facilement que de les accepter.

Suite à une série de contrôles, la CNIL a constaté que la politique d'utilisation des cookies d'un certain nombre d'organismes ne répondait pas aux exigences susvisées. Elle a, en conséquence, adressé des mises en demeure à l'attention de ces organismes.

Parmi les entités visées figurent principalement d'importantes sociétés de l'économie numérique, ainsi que des « acteurs publics ».

La CNIL annonce que ces entités ont un mois pour se mettre en conformité, et encourent des sanctions pécuniaires allant jusqu'à 2% de leur chiffre d'affaires dans l'hypothèse où ce délai ne serait pas tenu.

La CNIL a également rappelé que dans le cadre de ses décisions récentes de sanction concernant Google et Amazon, elle avait informé ces entités de la nécessité de rendre aussi facile le refus des cookies que leur acceptation.

Lien vers la publication de la CNIL : https://www.cnil.fr/fr/cookies-une-vingtaine-organismes-mis-en-demeure

COOKIES :

LA CNIL CLOTURE L'INJONCTION PRONONCEE A L'ENCONTRE DE GOOGLE

PAR UNE DELIBERATION DU 30 AVRIL 2021 (ACCESSIBLE ICI), LA CNIL A CLOTURE L'INJONCTION PRONONCEE A L'ENCONTRE DES SOCIETES GOOGLE LLC ET GOOGLE IRELAND LIMITED (CI-APRES, « GOOGLE »).

Par une délibération du 7 décembre 2020, la CNIL avait condamné GOOGLE à des amendes de 60 et 40 millions d'euros en raison de manquements à la législation applicable en matière de cookies.

La CNIL avait notamment relevé les manquements suivants :

- Des cookies publicitaires étaient automatiquement déposés sur le terminal de l'utilisateur sans recueil préalable de son consentement ;
- Aucune information n'était fournie à l'utilisateur concernant les cookies qui étaient déposés sur son terminal ;
- Le mécanisme d'opposition était partiellement défaillant puisque, malgré l'opposition de l'utilisateur, un des cookies publicitaires demeurait stocké sur son ordinateur et continuait de lire les informations à destination du serveur auquel il était rattaché.

Tirant les conséquences de ces manquements, la CNIL avait prononcé des amendes administratives, accompagnées d'injonctions de correction sous trois mois desdits manquements, assorties d'une astreinte de 100.000 euros par jour de retard.

GOOGLE demanda, sans succès, au juge des référés du Conseil d'Etat d'ordonner la suspension de l'exécution de la délibération de la CNIL concernant l'injonction qui avait été prononcée.

Des échanges sont ensuite intervenus entre la CNIL et GOOGLE.

Dans sa délibération du 30 avril dernier, la CNIL a indiqué que, dans le délai de trois mois imparti, GOOGLE lui a adressé des éléments justifiant sa mise en conformité puisque *« les personnes se rendant sur le site google.fr sont désormais informées, de manière claire et complète, de toutes les finalités des cookies soumis au consentement et des moyens mis à leur disposition pour les refuser, par le biais du bandeau d'information s'affichant à leur arrivée sur le site ».*

Par conséquent, la CNIL a clôturé l'injonction, sans qu'il n'y ait lieu à liquidation d'astreinte.

A noter que dans le communiqué qui accompagne la publication de la délibération, la CNIL a averti que dans la mesure où elle s'est prononcée avant la fin de la période d'adaptation laissée aux acteurs pour se mettre en conformité avec les nouvelles règles en matière de cookies, elle n'a pas examiné la conformité du bandeau d'information fourni sur le site « google.fr » avec lesdites règles.

Ainsi, l'autorité de contrôle a souligné que « cette décision de clôture ne préjuge donc pas de l'analyse de la CNIL quant à la conformité de google.fr à ces exigences, selon lesquelles l'utilisateur doit désormais être en mesure de refuser les cookies aussi facilement qu'il peut les accepter. La CNIL se réserve désormais la possibilité de contrôler ces modalités de refus et, si nécessaire, de mobiliser l'ensemble de sa chaîne répressive ».

RECLASSEMENT DE SALARIES :

LE COMPTE-RENDU D'ENTRETIEN DOIT ETRE OBJECTIF

METTANT NOTAMMENT EN CAUSE LE CARACTERE OBJECTIF DES DONNEES RETRANSCRITES DANS UN COMPTE RENDU, UN EMPLOYE A CONTESTE LE TRAITEMENT DE SES DONNEES PAR UN CABINET DE CONSULTANTS DILIGENTE PAR SON EMPLOYEUR, DANS LE CADRE D'UNE RESTRUCTURATION.

La société CER Haute-Savoie, association de gestion et de comptabilité, a décidé, en 2015, de mutualiser son service informatique avec d'autres entités, au sein d'une société dénommée « Agil'it ».

La société Agil'it, ainsi nouvellement créée, a fait appel à un cabinet de consultants en vue de procéder à l'intégration des salariés et de leur proposer le poste le plus adapté.

Dans le cadre de sa mission, le cabinet de consultants a réalisé un entretien avec le personnel afin d'analyser le positionnement de chacun par rapport au projet de transfert de chaque contrat de travail.

Se fondant sur l'article L 1224-1 du Code du travail, la société Agil'it a proposé à l'un des comptables, employé par la société CER Haute-Savoie, un contrat de travail en qualité d'analyste programmeur. Estimant ne pas avoir les compétences pour exercer ces fonctions, il a refusé cette proposition, ainsi que plusieurs autres propositions de reclassement.

Le comptable a été convoqué à un entretien préalable en vue d'envisager son licenciement économique, puis a été licencié.

Il a saisi, sans succès, le conseil de prud'hommes d'Annecy qui a estimé que la procédure de transfert de contrat de travail était fondée, de même que la rupture dudit contrat.

C'est, dans ce contexte, que l'ex-comptable a interjeté appel de la décision.

Outre ses demandes tenant au licenciement en tant que tel, l'ex-comptable se prévalait de l'irrégularité du traitement de ses données personnelles dans le cadre de l'intervention du cabinet de consultants, dès lors qu'aucune information ne lui avait été communiquée préalablement au traitement de ses données personnelles par ce cabinet, notamment, en ce qui concerne la finalité de sa mission.

Par ailleurs, l'ex-comptable faisait valoir que le compte-rendu d'entretien contenait des mentions subjectives, puisqu'il était fait état de son état d'esprit et comportait la mention suivante : « M. X dit les choses de manière franche et honnête dans la mesure où cela sert ses intérêts », ce qui constituerait, selon lui, une évaluation subjective, contraire aux dispositions du RGPD.

Invoquant un « fichage illégal », il a demandé à la Cour d'appel de Chambéry une indemnisation à hauteur de 10.000 euros.

La juridiction du second degré a relevé que le RGPD n'était pas applicable au cas d'espèce, puisque l'entretien s'était tenu avant sa date d'entrée en application. Néanmoins, la Cour d'appel a fait application de l'article 32 de la loi « Informatique et libertés » (en vigueur au moment des faits), et a conclu :

« En l'espèce, aucune information n'a été donnée à M. X. Le document remis lors de la rencontre d'information du 24 octobre 2017 ne contient aucun élément d'information concernant le cabinet Accile, la finalité de sa mission. »

Pour la Cour, les informations recueillies se devaient également d'être objectives, c'est-à-dire uniquement en rapport avec les compétences professionnelles de l'ex-comptable et son positionnement professionnel. Or, le compte-rendu contenait « *des appréciations purement subjectives sur son état d'esprit qui n'avaient pas à figurer dans ce rapport* ».

Si la Cour a, *in fine*, estimé que le licenciement reposait bien sur une cause réelle et sérieuse, elle a néanmoins condamné la société Agil'it à payer au particulier la somme de 2.000 euros à titre de dommages-intérêts pour « *fichage illégal* ».

Référence de la décision : Cour d'appel de Chambéry, chambre sociale prud'hommes, 4 mai 2021, n° 20/00419

Lien vers la décision : https://bit.ly/35Tc2Um

ACTUALITE EUROPEENNE :

PANORAMA DE QUELQUES DECISIONS RENDUES PAR DES AUTORITES NATIONALES DE CONTROLE

Accès illicites à un fichier de crédits

AEPD (BELGIQUE), 23 AVRIL 2021

Une plainte avait été déposée par une citoyenne belge contre un établissement financier, dont l'un des employés, son ex-mari, avait reconnu avoir consulté une vingtaine de fois des informations de son ex-femme dans la « Centrale des crédits aux particuliers » (CCP), fichier dans lequel sont enregistrés tous les crédits conclus par des personnes physiques ainsi que les éventuels défauts de paiement de ces personnes.

L'Autorité de contrôle belge (APD) a considéré que l'établissement financier n'avait pas respecté son obligation de sécurité, en permettant de tels accès, alors qu'il aurait fallu qu'il mette en place des règles d'accès, un registre-journal des accès, ainsi qu'un système de contrôle de ces accès.

Pour motiver le montant de l'amende de 100 000 euros prononcée contre l'établissement, l'APD a notamment mentionné le fait que l'accès portait sur des données sensibles.

Lien vers la décision en français : https://bit.ly/3oOsfma

Cookies : la CJUE épinglée par le CEPD

AEPD (ESPAGNE), 3 MAI 2021

Un particulier a envoyé une plainte le 2 octobre 2019 au CEPD (Contrôleur européen à la protection des données) au sujet du site internet de la CJUE et de deux sites vers lesquels le site de la CJUE renvoyait.

Le Contrôleur observe que plusieurs manquements ont été commis par la CJUE.

Au sujet des cookies, le CEPD estime d'abord que l'internaute n'est pas correctement informé de l'utilisation de cookies. Plus précisément, il considère que la CJUE ne prévient pas l'internaute que des cookies YouTube peuvent être placés. Ensuite, le CEPD estime que le site de la CJUE n'offre pas la possibilité à l'internaute de refuser les cookies aussi facilement qu'il ne les accepte. En particulier, il eût fallu qu'à côté du bouton « accepter » figure le bouton « rejeter ».

Le dispositif des cookies ayant été corrigé aussitôt que la plainte a été déposée, aucune sanction n'a été prononcée contre la CJUE.

Lien vers la décision en anglais : https://bit.ly/34jIw9k

Sanction d'un employeur pour avoir publié une lettre de démission sur un groupe WhatsApp

ANS (ROUMANIE), 7 MAI 2021

Un employeur roumain a publié sur le groupe WhatsApp sur lequel se trouvait une grande partie des employés de la société une lettre de démission d'un de ses anciens salariés. Cette lettre de démission contenait des données personnelles telles que le nom, le prénom, l'adresse, le numéro de carte d'identité et des informations relatives aux raisons de son départ.

L'autorité de contrôle roumaine a prononcé une sanction de 2.000 euros contre l'employeur pour manquement à l'obligation de confidentialité des données.

Lien vers la décision en roumain : https://bit.ly/3yHHnGG

Les échanges de données de santé par e-mail doivent être cryptés et protégés par mot de passe.

NAIH (HONGRIE), 14 MARS 2021

Les agents d'un établissement public hongrois avaient envoyé, par courriel, à un médecin, un fichier Excel contenant des données de santé de plus de 1.000 patients, dont des données relatives aux résultats de tests de dépistage contre la COVID. Ce fichier n'avait été protégé par aucun mot de passe. Par la suite, ce courriel a été forwardé plusieurs fois par le médecin destinataire à d'autres praticiens tiers. Une personne, qui n'était pas médecin et ayant reçu le courriel, a informé l'autorité de contrôle hongroise (NAIH) d'une possible violation des données personnelles.

La NAIH a considéré que la possession par un tiers de ce fichier Excel constituait une violation de données, ces données étant, de surcroit, sensibles. L'autorité de contrôle a ensuite rappelé que ces données de santé auraient dû être chiffrées et le mot de passe de déchiffrement aurait dû être transmis aux destinataires par un moyen différent. La NAIH a enfin précisé que l'urgence liée à la gestion de la pandémie de COVID-19 ne peut en aucun cas exonérer le responsable de traitement de ses obligations au titre du RGPD. En conséquence, l'établissement public hongrois a été sanctionné d'une amende administrative d'un montant de 30.000€.

Lien vers la décision en portugais : *https://bit.ly/3uDTxNL*

VUE DANS LA PRESSE :

QUELLE DUREE DE CONSERVATION DES MESSAGERIES ELECTRONIQUES PROFESSIONNELLES ?

LA QUESTION DE LA DUREE DE CONSERVATION DE LA MESSAGERIE ELECTRONIQUE N'EST PAS AISEE, MAIS DEVIENT FONDAMENTALE LORSQU'UN SALARIE QUITTE L'ENTREPRISE.

L'employeur peut-il conserver tout ou partie du contenu de la boîte électronique du salarié ayant cessé ses fonctions dans l'entreprise ? Si oui, pour quelle durée ?

Rappel du principe

Conformément au principe de limitation de la conservation visé à l'article 5-1-e) du RGPD, les données à caractère personnel ne doivent être conservées par l'organisme qui les traite que le temps strictement nécessaire à la réalisation des finalités poursuivies. Au-delà, elles doivent être anonymisées, supprimées, ou archivées (archivage intermédiaire ou archivage public).

Ce principe s'applique quelle que soit la nature ou la finalité du traitement. Ainsi, dans le cadre de la relation de travail, les données pourront être conservées en base active pendant toute la durée de cette relation notamment s'agissant des données du registre unique du personnel. En revanche, au terme de la relation de travail, l'employeur ne pourra les conserver, « sous forme d'archives intermédiaires distinctes de la base active, avec accès restreint » [1], que parce qu'il doit tenir compte des dispositions législatives ou règlementaires qui lui sont applicables (comme des obligations comptables, sociales, fiscales ou parce que les données présentent un « intérêt » en cas de contentieux. Pour aider les entreprises à encadrer leurs traitements « mis en oeuvre aux fins de gestion du personnel », la Cnil a adopté un référentiel dans lequel sont données des « illustrations pratiques » de durées de conservation pouvant, selon le contexte, être retenues par les organismes concernés. Ainsi, des durées de conservation sont proposées pour trois activités de traitement : (i) la gestion de la paie, (ii) le registre unique du personnel et (iii) la gestion des mandats des représentants du personnel. Aucune indication n'est en revanche donnée concernant les autres activités de traitement pourtant visées dans ce référentiel, comme la gestion des rémunérations, le suivi des carrières et de la mobilité, la formation, la gestion aides sociales ou encore la mise à disposition du personnel d'outils informatiques. Il appartient donc aux organismes de définir eux-mêmes les durées de conservation applicables à ces activités de traitement, en fonction de ce qui est strictement nécessaire à la réalisation des finalités poursuivies.

Vaste et délicat programme… Prenons l'exemple de l'activité de traitement portant sur la mise à disposition d'outils informatiques, telle que la messagerie électronique professionnelle. Quelle durée de conservation retenir pour l'employeur ? Peut-il maintenir l'adresse électronique active ? Peut-il conserver tout ou partie du contenu de la boîte électronique du salarié ayant cessé ses fonctions dans l'entreprise ? Si oui, pour quelle durée ?

La Cnil n'a jamais pris une position officielle sur ces questions. C'est pourquoi, nous nous sommes tournés vers d'autres autorités nationales de contrôle. Par chance, l'autorité belge de protection des données (l'« APD ») a eu l'occasion de se prononcer sur le sujet.

L'affaire belge

Dans cette affaire[2], les faits remontaient à 2019, lorsque le plaignant, ancien administrateur d'une société spécialisée dans la commercialisation de dispositifs médicaux, constata, après avoir cessé ses activités dans cette société, que cette dernière continuait d'utiliser ses anciennes adresses électroniques. Après un courrier recommandé resté sans réponse par lequel le plaignant demandait à la défenderesse de fermer les boîtes e-mails, le plaignant déposa une requête auprès de l'autorité de contrôle belge.

Lors de l'audition, la défenderesse expliqua que seuls les messages « entrant » étaient redirigés vers une personne unique de l'entreprise, sans utilisation de l'adresse de messagerie du plaignant pour des envois de messages à des tiers. Le maintien de ces adresses se justifiait, selon la défenderesse, par la volonté, d'une part, de ne pas perdre des messages professionnels importants et, d'autre part, de pallier l'absence de transmission de dossiers. Quant à la consultation des archives des e-mails, celle-ci était faite à des fins exclusivement professionnelles.

La chambre contentieuse a considéré que l'absence de suppression des adresses de messagerie du plaignant est constitutive de manquements aux principes du RGPD, à savoir les principes de licéité, de finalité, de minimisation et de conservation proportionnée des données. Selon l'autorité de contrôle, il incombait au responsable du traitement « de bloquer la messagerie électronique » du titulaire de celle-ci au plus tard le jour effectif de son départ. Ce blocage aurait dû intervenir après information de la personne et après y avoir fait insérer un « message automatique » avertissant tout correspondant ultérieur du fait que la personne concernée n'exerce plus ses fonctions au sein de l'entreprise, et ce « pendant une période raisonnable (a priori 1 mois) ». L'APD ajoute qu'en fonction du contexte et, en particulier du degré de responsabilité exercée par la personne concernée, « un délai plus long peut être admis ne pouvant idéalement dépasser 3 mois ».

Une telle façon de procéder est, selon l'autorité, à privilégier « par rapport au transfert automatique des mails à une autre adresse électronique de l'entreprise comme cela avait été mis en place par la défenderesse ».

Au-delà de cette période, l'APD précise que la messagerie électronique doit être supprimée, car « la finalité de traitement de cette donnée à caractère personnel [l'adresse électronique] est alors sans objet ». Elle ajoute que si l'adresse peut en effet rester active un certain délai aux fins d'assurer « le bon fonctionnement de l'entreprise et la continuité des prestations », au-delà de ce délai « plus aucune base de légitimité ne permet que le traitement se poursuive ». Or, à défaut d'intérêt légitime, « plus aucune base de licéité ne permettait de fonder la poursuite du traitement de cette donnée ».

Par conséquent, si l'employeur souhaite récupérer tout ou partie du contenu de la messagerie, il doit le faire avant que la messagerie ne soit bloquée. C'est d'ailleurs ce qu'indiquait le Comité des ministres du Conseil de l'Europe dans une recommandation CM/Rec (2015)5, à laquelle fait référence l'autorité belge de contrôle : « Lorsqu'un employé quitte son emploi, l'employeur devrait prendre des mesures techniques et organisationnelles afin que la messagerie électronique de l'employé soit désactivée automatiquement. Si le contenu de la messagerie devait être récupéré pour la bonne marche de l'organisation, l'employeur devrait prendre des mesures appropriées afin de récupérer son contenu avant le départ de l'employé et si possible en sa présence. » Cette récupération du contenu de la messagerie pour assurer la bonne marche de l'entreprise devrait se faire, selon l'APD, « avant le départ du salarié et en sa présence ». Quant au salarié, la Chambre contentieuse estime qu'il doit être mis en mesure « de reprendre ou d'effacer ses communications électroniques d'ordre privé avant son départ », étant précisé qu'en cas de situation litigieuse, « l'intervention d'une personne de confiance est recommandée ».

En l'espèce, la Chambre contentieuse a prononcé à l'encontre de l'organisme un ordre de mise en conformité par l'adoption d'une politique réglant la question de la clôture des messageries électroniques, ainsi qu'une amende administrative d'un montant de 15 000 euros.

Quelles recommandations ?

L'employeur doit fixer les règles dans la charte informatique en précisant le sort de la messagerie électronique à compter du départ du salarié : blocage et insertion d'un message automatique avertissant tout correspondant ultérieur du fait que le salarié a quitté ses fonctions. La charte doit également indiquer que le salarié peut, avant son départ effectif, récupérer ou effacer ses courriels d'ordre privé, étant précisé que l'employeur peut se réserver la possibilité de conserver, pendant une durée à définir dans le cadre d'un archivage intermédiaire, le contenu restant, et ce pour la bonne marche de l'entreprise. En cas de situation conflictuelle entre les parties, il est recommandé d'organiser ces opérations sous le contrôle d'un huissier de justice.

Alexandre FIEVEE, *Expertises Juin 2021*

Notes

[1] Cnil, « Référentiel relatif aux traitements de données à caractère personnel mis en œuvre aux fins de gestion du personnel », 21 novembre 2019.

[2] Autorité de protection des données belge, chambre contentieuse, 64/2020, 29 septembre 2020.

ACTUALITE DU CABINET

DERRIENNIC ASSOCIES PROPOSE UN PROGRAMME DE FORMATION DE **35 HEURES** POUR LA PRÉPARATION A LA CERTIFICATION DPO

OBJECTIF

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

COUT

3000€ HT/personne

INTERVENANT

Alexandre FIEVEE
Avocat Associé
Tél : 01.47.03.14.94
afievee@derriennic.com

Classements
Alexandre Fievee figure dans le classement BestLawyers dans la catégorie « Information Technology Law » (2020).
Il a également fait en 2020 son entrée dans le classement Legal 500 dans la catégorie « Next Generation Partners ».

RENSEIGNEMENTS PRATIQUES

Prochaine session 2021 :
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