NEWSLETTER RGPD/DATA

NUMÉRO 47 ● OCTOBRE 2022

ACTUALITES DU CABINET P. 20

MATINALE
LE DPO : DANS L'ŒIL DU CYCLONE ?

FORMATION A LA PREPARATION A LA CERTIFICATION « DPO ».
DATE SUR DEMANDE

SOMMAIRE

ACTUALITE NATIONALE

- Traitement de l'orientation sexuelle des candidats aux dons du sang : la France condamnée **P.2**
- Une violation dont le responsable du traitement a été informé par la CNIL n'a pas à être notifiée à cette dernière **P.4**
- INFOGREFFE sanctionné pour non-respect d'une « précaution élémentaire de sécurité » **P.5**
- Données sensibles : éclairages de la CJUE **P.6**
- Règlement DSA : la procédure d'adoption touche à sa fin **P. 7**
- Fiches Google My Business : un traitement illicite ? **P.8**
- ACCOR condamnée à 600.000 € d'amende pour plusieurs manquements **P. 10**
- Autorité de la concurrence : un nouveau gendarme du RGPD ? **P.12**
- Mises en demeure de designer un DPO : le bilan **P. 13**

VU DANS LA PRESSE

- Analyse de l'état émotionnel des appelants (IA) **P.14**

ACTUALITE EUROPEENNE

- Panorama de quelques décisions rendues par des autorités nationales de contrôle **P. 16**

ACTUALITES

TRAITEMENT DE L'ORIENTATION SEXUELLE DES CANDIDATS AUX DONS DU SANG : LA FRANCE CONDAMNÉE

La France a été condamnée par la Cour européenne des droits de l'homme, dans le cadre de la collecte et du traitement de données révélant l'orientation sexuelle des candidats aux dons du sang.

La Cour européenne des droits de l'homme (« CEDH ») a rendu, le 8 septembre 2022, une décision dans laquelle elle a eu à déterminer si la collecte et le traitement de l'orientation sexuelle des candidats aux dons du sang était compatible avec l'article 8 de la convention européenne des droits de l'homme, qui a pour objet de préserver la vie privée des individus et les prémunir contre les ingérences des autorités publiques.

En 2004, un homme a souhaité réaliser un don du sang auprès de l'établissement français du sang (« EFS »), établissement public de l'Etat. Au cours de l'entretien préalable au don, il a refusé de répondre à la question consistant à savoir s'il avait déjà eu des rapports sexuels avec un autre homme.

Ce silence a entrainé le rejet de sa candidature et l'inscription, dans son dossier, de la mention « FR08 », signifiant qu'il avait déjà eu des rapports sexuels avec un autre homme, ce qui constituait, à l'époque, une contre-indication au don du sang.

En 2006, le même individu s'est présenté pour réaliser de nouveau un don du sang et il lui a été opposé, en tant que motif du refus de sa candidature, ladite contre-indication. Précision lui a été donnée que l'interdiction de don le frappant demeurerait valable jusqu'en 2278.

En 2016, au cours d'une troisième tentative de don, l'individu a produit des analyses biologiques attestant de sa séronégativité. Il lui a néanmoins été opposé un nouveau refus, sur les mêmes fondements que les précédentes fois.

L'individu a porté plainte avec constitution de partie civile, arguant d'une violation de l'article 226-19 du Code pénal prohibant la conservation de données à caractère personnel relative à la santé ou à l'orientation sexuelle.

La plainte a abouti sur un non-lieu, la chambre de l'instruction ayant estimé que le législateur, par l'adoption d'un arrêté et d'un article du Code de la santé publique prévoyant la classification des contre-indications au don du sang, avait entendu créer une dérogation à l'interdiction de l'article 226-19 du Code pénal.

La Cour de cassation, saisie à l'issue de la décision de non-lieu, a rejeté le pourvoi de l'individu, estimant, pour sa part, que le traitement en cause était couvert par les dispositions de la Loi du 6 janvier 1978 autorisant un tel traitement, lorsqu'il est réalisé par des professionnels de santé à des fins médicales.

Source : ici

L'individu, ayant saisie la CEDH, a argué d'une ingérence des autorités publiques contraire à l'article 8 de la Convention européenne des droits de l'homme, en raison :

- du caractère discriminatoire de l'exclusion permanente du don du sang des homosexuels ;
- du caractère sensible de ses données personnelles ;
- de la collecte sur le seul fondement de son refus de répondre à des questions portant sur sa sexualité ;
- de l'absence de possibilité d'effacer ou de rectifier ses données.

Le gouvernement français a, pour sa part :

- admis qu'il y avait eu une ingérence, mais que celle-ci était prévisible compte tenu des dispositions de la loi du 6 janvier 1978 et de l'article 226-19 Code pénal ;
- avancé que le mécanisme de contre-indication au don était clair et impliquait que l'EFS se dote d'un système de traitement de l'information permettant sa mise en œuvre ;
- argué que le traitement en cause était nécessaire à la protection de la santé publique.

La CEDH a rappelé que les ingérences dans la vie privée doivent être prévues par la loi et être nécessaires et proportionnée au but légitime poursuivi, ainsi que reposer sur des motifs « *pertinents et suffisants* ».

S'agissant du caractère nécessaire de l'ingérence constituée par le traitement en cause, la CEDH a indiqué que la collecte et la conservation des données à caractère personnel relatives aux résultats de procédure de sélection des candidats au don du sang contribuent à garantir la sécurité transfusionnelle.

Cependant, pour la CEDH, le requérant s'est vu appliquer une contre-indication propre aux hommes ayant eu un rapport sexuel avec un autre homme, au seul motif de son refus de réponse à la question concernant sa sexualité, alors qu'« *aucun des éléments soumis à l'appréciation du médecin ne lui permettait de tirer une telle conclusion sur ses pratiques sexuelles* ».

La CEDH a rappelé qu'il incombe aux autorités de démontrer l'exactitude des données à caractère personnel collectées. Elle relève, également, que les données à caractère personnel n'ont pas été mises à jour suite aux protestations et à la plainte du requérant.

De plus, la CEDH a considéré que le simple refus de répondre à la question aurait pu être conservé, celui-ci motivant à lui seul un refus de la candidature au don du sang.

La CEDH a relevé, enfin, que la durée de conservation était excessive (274 ans annoncés, au moins 12 ans en pratique).

Il y a donc bien eu violation de l'article 8 de la convention européenne des droits de l'homme, ce qui a conduit la CEDH à condamner la France au paiement de 3.000 € du requérant pour préjudice moral, ainsi que 9.000 € pour frais et dépens.

Source : ici

UNE VIOLATION DONT LE RESPONSABLE DU TRAITEMENT A ÉTÉ INFORMÉ PAR LA CNIL N'A PAS Á ETRE NOTIFIÉE A CETTE DERNIÈRE

Le 22 juillet 2022, le Conseil d'Etat a rendu un arrêt, selon lequel un responsable du traitement, averti par la CNIL de l'existence d'une violation de données, n'a pas à notifier ladite violation à la CNIL.

Suite à l'ouverture des ports réseaux de sa box internet par un chirurgien orthopédiste, des milliers d'images médicales ont été rendues accessibles librement sur internet.

La CNIL a eu vent de cette violation par le biais d'un signalement sur le site « 01net.com », ce qui a déclenché un contrôle en ligne. Suite à ce contrôle, la CNIL a informé le chirurgien du libre accès des images et de l'existence dudit contrôle.

La CNIL a, *in fine*, rendu une décision de sanction condamnant le chirurgien au paiement d'une amende de 3.000 € pour défaut de sécurisation des données (article 32 du RGPD) et manquement à l'obligation de notification de la violation (article 33 du RGPD).

Le chirurgien a exercé un recours devant le Conseil d'Etat afin d'obtenir l'annulation de la décision de la CNIL.

Si le Conseil d'Etat a confirmé la décision de la CNIL s'agissant du défaut de sécurisation des données, il a néanmoins indiqué que les circonstances d'espèces justifiaient l'absence de notification à la CNIL de la violation :

> « *l'obligation de notifier à la CNIL une violation de données à caractère personnel susceptible de faire naître un risque pour les droits et libertés des personnes physiques ne s'impose pas au responsable du traitement dans le cas où la CNIL l'a elle-même informé de cette violation et a engagé son contrôle sur la base des informations portées à sa connaissance par ailleurs* ».

En conséquence, le Conseil d'Etat, dans sa décision rendue le 22 juillet 2022, a réduit de 500 € le montant de l'amende prononcée à l'encontre du chirurgien.

Source: ici

INFOGREFFE SANCTIONNÉ POUR NON-RESPECT D'UNE « *PRÉCAUTION ÉLÉMENTAIRE DE SÉCURITÉ* »

Saisie d'une plainte d'une personne indiquant que l'organisme INFOGREFFE lui avait transmis son mot de passe par téléphone en donnant simplement son nom, la CNIL a sanctionné l'organisme pour non-respect de l'obligation de sécurité et non-respect du principe de limitation de la conservation.

A la suite d'une plainte adressée à l'encontre d'INFOGREFFE, (l'organisme permettant de consulter des informations légales sur les entreprises), la CNIL a diligenté une enquête auprès de ce dernier.

Au terme de son enquête, la CNIL a dressé un rapport détaillant deux manquements au RGPD.

En premier lieu, INFOGREFFE n'a pas respecté les durées de conservation des données personnelles. Effectivement, bien qu'indiquant dans sa « *Charte de confidentialité* » qu'il gardait les données personnelles pendant « *36 mois à compter de la dernière commande* », INFOGREFFE a fourni à la CNIL un fichier contenant des données personnelles bien plus anciennes.

En second lieu, INFOGREFFE n'a pas mis en œuvre les mesures de sécurité adéquates. En effet, selon l'article 32 du RGPD, il incombe au responsable de traitement de prendre des *« mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque* ».

Or, la CNIL a constaté que les mots de passe (i) étaient limités à 8 caractères, (ii) n'exigeaient aucun critère de complexité, (iii) étaient transmis en clair par courriel et (iv) étaient conservés en clair par INFOGREFFE. De plus, la modification du mot de passe n'était pas confirmée à l'utilisateur. Après avoir rappelé que la protection des mots de passe est une « *précaution élémentaire de sécurité correspondant à l'état de l'art* », la CNIL en a conclu que « *la faiblesse extrême des règles de complexité des mots de passe, ainsi que les mesures de sécurité en matière de communication conservation et renouvellement des mots de passe* [rendaient] *l'ensemble des comptes vulnérables* ».

En conséquence de ces deux manquements la CNIL a infligé à INFOGREFFE une amende de 250 000 €.

Source : ici

DONNÉES SENSIBLES : ÉCLAIRAGES DE LA CJUE

Par un arrêt rendu le 1er août dernier, la CJUE a apporté des précisions sur la notion de « données sensibles » au sens du RGPD. Retour sur cette décision aux conséquences pratiques non négligeables.

La CJUE a été saisie de deux questions préjudicielles dans le cadre d'un litige lituanien relatif à la légalité d'une disposition nationale exigeant la publication d'une déclaration d'intérêts privés par le directeur d'un établissement percevant des fonds publics.

La 1ère question portait en particulier sur le point de savoir si le RGPD s'oppose à une disposition nationale prévoyant la mise en ligne de données à caractère personnel contenues dans les déclarations d'intérêts privés que tout directeur d'un établissement percevant des fonds publics est tenu de déposer auprès de l'autorité nationale chargée de collecter ces déclarations et d'en contrôler la teneur.

La CJUE a répondu par l'affirmative, dans la mesure où la publication en cause comporte notamment des données nominatives relatives au conjoint, concubin ou partenaire du déclarant ainsi qu'aux personnes proches ou connues de lui susceptibles de donner lieu à un conflit d'intérêts. Pour ce faire, la CJUE s'est notamment basée sur le principe de minimisation des données : l'objectif général poursuivi (garantir l'impartialité des décisions des personnes travaillant dans le service public/lutter contre la corruption) pourrait être atteint en faisant uniquement référence à l'expression générique de conjoint, concubin ou partenaire selon le cas, reliée à l'indication pertinente des intérêts détenus par ces derniers en relation avec leurs activités.

La seconde question était la suivante : est-ce que la publication sur le site internet de l'autorité publique concernée de données à caractère personnel susceptibles de divulguer indirectement les opinions politiques, l'appartenance syndicale ou l'orientation sexuelle d'une personne physique constitue un traitement de données sensibles au sens du RGPD ?

La CJUE a relevé que si les données concernées ne constituent pas par leur nature des données sensibles au sens de ces textes, elles sont de nature à révéler, par une opération intellectuelle de rapprochement ou de déduction, l'orientation sexuelle d'une personne physique et, de ce fait, rentrent dans la catégorie de données sensibles.

Cette position des juges européens apporte des clarifications à la qualification de données sensibles : sont concernées, au-delà des données sensibles par nature, les données révélant des données sensibles par simple rapprochement ou déduction intellectuels.

Une telle décision invite ainsi les responsables de traitement et sous-traitants à la plus grande vigilance dans leurs traitements de données, les cas de qualification de données sensibles étant particulièrement larges. A suivre la CJUE, de simples données de géolocalisation ou de consommation et d'habitude alimentaires pourraient effectivement permettre de déduire la religion d'une personne et pourraient être qualifiées de données sensibles.

Source : ici

REGLEMENT DSA : LA PROCEDURE D'ADOPTION TOUCHE A SA FIN

Ce mois-ci, le DSA a été approuvé définitivement par le Conseil de l'UE puis signé par ce dernier et le Parlement européen, marquant ainsi la fin d'un long processus d'adoption et le début d'une nécessaire mise en conformité pour de nombreuses plateformes.

Pour mémoire, le DSA pour « Digital Service Act » est un règlement européen, dont le nom officiel est « *règlement relatif à un marché unique des services numériques et modifiant la Directive 2000/31/CE (Règlement sur les services numériques)* », proposé par la Commission européenne le 15 décembre 2020.

Ce règlement encadre principalement le fonctionnement des « intermédiaires en ligne » afin de réguler davantage les contenus illicites en ligne et ce, en adaptant l'actuelle Directive dite « E-commerce » (directive n°2000/31/CE sur le commerce électronique, transposée dans notre « LCEN »), aux évolutions du marché numérique. Ce texte met à jour les obligations et responsabilités des plateformes d'e-commerce mais aussi et, plus largement, définit les obligations et responsabilités des fournisseurs de services intermédiaires en ligne tels que les réseaux sociaux, les places de marchés en ligne, les plateformes de partage de contenus, les services cloud et les FAI.

Des obligations supplémentaires sont également prévues pour les « *très grandes plateformes en ligne* » et les « *très grands moteurs de recherche* », c'est-à-dire ceux comptant plus de 45 millions d'utilisateurs actifs chaque mois au sein de l'UE.

Le Conseil de l'UE et le Parlement européen avait trouvé un accord provisoire sur le texte le 23 avril dernier. Le 4 octobre 2022, le Conseil de l'UE a approuvé définitivement le texte. Aussi, le 19 octobre 2022, le texte final a été signé par le Conseil de l'UE et le Parlement européen. Sa publication au Journal Officiel de l'UE ne devrait plus tarder.

Le règlement DSA sera applicable dans un délai de 15 mois à compter du 20ème jour suivant cette publication, sauf pour les « *très grandes plateformes* » et les « *très grands moteurs de recherche* » qui disposeront d'un délai réduit de 4 mois à compter de la notification de leur désignation conformément au DSA.

Les acteurs concernés sont donc invités à commencer, dès à présent, leur démarche de mise en conformité, dont l'ampleur peut être importante (revue des processus de traitement des réclamations/litiges et des documents contractuels dont les CGV, etc.), étant rappelé qu'une non-conformité peut être passible d'une amende pouvant aller jusqu'à 6% de leur chiffre d'affaires mondial total.

Source : ici

FICHES GOOGLE MY BUSINESS : UN TRAITEMENT ILLICITE ?

Le tribunal judiciaire de Chambéry, dans une décision du 15 septembre 2022, a condamné Google à supprimer une fiche Google My Business, en raison du défaut d'intérêt légitime de Google à traiter les données de la personne concernée.

Une dentiste a découvert l'existence d'une fiche « Google My business » la concernant, affichant son nom, son domicile et une notation et des avis liés à son activité professionnelle.

Cette dentiste a mis en demeure Google France de supprimer l'intégralité de la fiche, ce que Google France a refusé. La dentiste a assigné Google France, Google LLC et Google Ireland Limited devant le Tribunal judiciaire de Chambéry afin d'obtenir l'effacement de ses données, sous astreinte.

La dentiste a soutenu qu'une notation et un avis attribué à une personne constituent des données personnelles et a argué de la violation de plusieurs principes fondamentaux, caractérisés notamment par l'absence de formalités préalables (1.) et le caractère illicite du traitement (2.)**.**

1. La demanderesse a invoqué l'absence de déclaration CNIL, le traitement ayant débuté en 2014, au moment où le régime déclaratif était encore en vigueur.

Sur ce point, les sociétés défenderesses ont invoqué l'article 112-1 du Code pénal, lequel affirme, en substance, le caractère rétroactif de la loi pénale plus douce..

Cet argument a été retenu par le Tribunal judiciaire qui considère que « *l'action pénale ne peut plus être ouverte* », mais, qu'en revanche, cette absence de déclaration demeurait une faute civile

Néanmoins, la sanction de l'effacement des données, demandée par la dentiste, n'étant pas encourue, la demande d'effacement formulée par la dentiste au titre de l'absence de respect des formalités préalable a été rejetée.

2. La demanderesse affirmait que le traitement était illicite, en raison de l'absence de recueil du consentement et d'intérêt légitime.

Le tribunal judiciaire, constatant que la dentiste n'avait pas consenti au traitement, a cherché à savoir si les sociétés défenderesses pouvaient se fonder sur l'intérêt légitime. La juridiction de premier degré a affirmé que cette base légale supposait, pour le responsable du traitement, d'avoir procédé à une pondération entre son intérêt légitime et les droits et intérêts des personnes concernées, leurs « *attentes raisonnables* ».

Le tribunal judiciaire a relevé :

- que les avis ont « *nécessairement des conséquences pour la future clientèle d'un professionnel* » ;
- que « *l'internaute anonyme derrière son écran a une fâcheuse tendance à oublier tout sens de la modération, voire tout sens commun* » ;

- que les sociétés défenderesses n'ont mis en place « *aucune mesure permettant d'identifier si besoin la source de l'information et de vérifier sa fiabilité* » ; et
- qu'il est compliqué pour le professionnel de répondre à des avis anonymes, d'autant plus lorsque ledit professionnel est soumis au secret médical.

Le tribunal judiciaire en a conclu qu'il existait un « *déséquilibre patent entre le professionnel et l'utilisateur du service* » et que les sociétés défenderesses « *ne justifient pas d'un intérêt légitime leur permettant de passer outre le consentement de la personne à voir publiées ses données personnelles et des avis accolés à ces données personnelles* ».

En conséquence, en raison de l'absence d'« *intérêt légitime impérieux et nécessaire au traitement* », et à défaut de démonstration que le traitement était « *nécessaire au nom du droit à l'information* », la dentiste était fondée à exercer ses droits d'opposition et d'effacement.

Le Tribunal judiciaire a également relevé un non-respect du principe de loyauté et de transparence, étant donné qu'il n'existe « *aucune notification visant à signaler aux professionnels l'existence de ces fiches* ».

Les sociétés défenderesses ont, en conséquence, été condamnées à :

- supprimer la fiche de la demanderesse sous astreinte de 100 euros par jour à l'issu d'un délai de deux mois ;
- payer à la demanderesse 20.000 euros au titre du préjudice subi et 20.000 euros supplémentaires au titre de l'article 700.

Source : TJ Chambéry, 15 sept. 2022, n° 19/01427

ACCOR CONDAMNÉE A 600.000 € D'AMENDE POUR PLUSIEURS MANQUEMENTS

Dans une décision du 3 août 2022, la CNIL a condamné la société ACCOR au paiement d'une amende de 600.000 €, notamment pour avoir procédé à des opérations de prospection commerciale sans recueillir le consentement des personnes concernées et avoir méconnu les droits conférés auxdites personnes par le RGPD.

Entre 2018 et 2019, la CNIL a été saisie de plusieurs plaintes faisant état d'une absence de prise en compte satisfaisante de la part de la société d'hôtellerie ACCOR, (i) du droit d'opposition à la réception de courriels de prospection commerciale et (ii) du droit d'accès exercé par les personnes concernées.
Ces éléments ont déclenché un contrôle de la CNIL en ligne, puis dans les locaux d'ACCOR.

La CNIL a, dans un premier temps, relevé sa compétence en tant qu'autorité chef de file concernant les traitements transfrontaliers menés par ACCOR, ayant considéré que l'établissement principal d'ACCOR se trouvait en France.

1. La CNIL reprochait à ACCOR d'avoir réalisé des opérations de prospection commerciale concernant ses clients, pour des produits et services proposés par des sociétés « partenaires ». Le consentement était recueilli au moyen d'une case pré-cochée par défaut.

La CNIL a considéré que le consentement aurait dû être libre, spécifique et informé. Or, compte tenu du pré-cochage de la case, ce consentement à la prospection commerciale pour des sociétés tierces ne pouvait être considéré comme valablement donné par l'utilisateur.

Par ailleurs, cette case pré-cochée était également proposée aux utilisateurs du site se créant un compte client, quand bien même ces utilisateurs n'avaient pas acheté de produits ou services.

ACCOR ne pouvait donc se prévaloir de l'exception de l'article L 34-5 du Code des postes et communications électroniques (CPCE) s'agissant de la prospection de ses clients pour des « *produits et services analogues* » à ceux déjà achetés.

Il y avait donc là, à plusieurs titres, manquements aux obligations de l'article L 34-5 du CPCE.

2. Par ailleurs, la CNIL a considéré que les mentions d'information n'étaient « *pas "aisément accessibles" pour [les personnes concernées], en ce que, lors de la création d'un compte, l'accès à la "charte de protection des données personnelles" de la société n'était organisé que via un lien hypertexte disponible tout en bas des pages du site internet, ce qui nécessitait que l'internaute fasse défiler la page dans son intégralité et recherche l'information, en méconnaissance de l'article 12 du RGPD* ».

La CNIL y a vu un manquement aux articles 12 et 13 du RGPD.

3. Le défaut de réponse satisfaisante apportée par ACCOR à plusieurs demandes d'exercice des droits d'accès émanant de clients a également été relevé par la CNIL, en violation de l'article 15 du RGPD. Le dysfonctionnement du lien de désinscription à la newsletter d'ACCOR, pendant plusieurs mois, a également caractérisé un manquement à l'article 21 du RGPD sur le droit d'opposition.

4. Enfin, la CNIL, lors de son contrôle sur place, a constaté que « *l'utilisation d'un mot de passe composé de huit caractères contenant seulement deux types de caractères (sept lettres majuscules et un caractère spécial) permettait d'accéder à l'outil de gestion l'envoi des communications aux clients* », ce qui constitue des mesures « *insuffisantes* » et qui « *ne permettent pas d'assurer la sécurité des données à caractère personnel* ».

De plus, lorsque le compte d'un client était suspendu en raison d'une suspicion de connexion frauduleuse, le service client invitait la personne concernée à transmettre la copie de sa pièce d'identité en pièce jointe d'un courriel. Cet envoi par mail ne permet pas, pour la CNIL, de se « *prémunir contre son interception par un tiers* ». Elle estime, en effet « *que la pratique consistant en la transmission de données non chiffrées par courriel électronique génère un risque important pour la confidentialité des données transmises* ».

La CNIL a qualifié ces pratiques de manquements à l'article 32 du RGPD.

Malgré (i) la mise en conformité d'ACCOR avec « *l'ensemble des manquements relevés* », (ii) l'absence de « *caractère structurel* » de certains de ces manquements, (iii) la pleine coopération d'ACCOR avec la CNIL, (iv) la baisse du chiffre d'affaires d'ACCOR en 2020 et 2021 et (v) le contexte économique lié à la crise sanitaire de la Covid-19, la CNIL a prononcé une amende administrative de 600.000 € à l'encontre d'ACCOR, dont 100.000 € au titre des manquements à l'article L34-5 du CPCE.

Source : ici

AUTORITE DE LA CONCURRENCE : UN NOUVEAU GENDARME DU RGPD ?

Le 20 septembre dernier, l'avocat général près la CJUE a conclu qu'une autorité de la concurrence peut, dans certaines conditions, examiner la conformité de pratiques commerciales avec le RGPD.

Le litige oppose Meta Platforms, exploitant le réseau social Facebook, à l'autorité de la concurrence allemande. Cette dernière reproche au réseau social une exploitation abusive de sa position dominante du fait de la non-conformité d'un traitement de données personnelles au RGPD.

La juridiction allemande saisie de l'affaire s'est tournée vers la CJUE afin notamment de savoir si une autorité de la concurrence nationale peut apprécier la conformité d'un traitement de données personnelles avec le RGPD.

Dans ses conclusions, l'avocat général près la CJUE a considéré que « *si une autorité de la concurrence n'est pas compétente pour constater une violation du RGPD* », elle peut « *dans l'exercice de* [ses] *propres compétences et pouvoirs (…) tenir compte, à titre incident, de la compatibilité d'un comportement avec le RGPD* ».

A cet égard, l'avocat général a, en particulier, estimé que « *la conformité ou la non-conformité dudit comportement aux dispositions du RGPD, non en lui-même, mais compte tenu de toutes les circonstances de l'espèce, peut constituer un indice important pour établir si ce comportement constitue un recours à des moyens qui gouvernent une compétition normale* ».

Aussi, l'avocat général a précisé que cet examen doit notamment tenir compte des décisions ou enquêtes de l'autorité de contrôle compétente au titre du RGPD, informer cette dernière voire mener une consultation avec elle.

Quelle sera la position de la CJUE ?

Les données personnelles étant au cœur de l'activité des GAFA et la jurisprudence ayant déjà ouvert la voie des actions pour manquement au RGPD par différents biais (pour mémoire : Associations de consommateurs – La CJUE ouvre la voie des recours pour violation du RGPD), c'est une décision est particulièrement attendue.

Source : ici

MISES EN DEMEURE DE DESIGNER UN DPO : LE BILAN

En mai 2022, la CNIL avait annoncé avoir adressé des mises en demeure à des communes de plus de 20.000 habitants n'ayant pas encore désigné de DPO, afin qu'elles remédient à cette situation. Dans une publication d'octobre 2022, la CNIL dresse un premier bilan de ces mises en demeure.

Pour rappel, l'article 37 du Règlement général sur la protection des données (RGPD) impose la désignation d'un délégué à la protection des données (DPO) aux autorités publiques et aux organismes publics procédant à des traitements de données à caractère personnel en qualité de responsable du traitement ou de sous-traitant.

Dans une publication du 31 mai 2022, la CNIL avait annoncé :

- avoir mis en garde, en juin 2021, des communes de plus de 20.000 habitants qui ne s'étaient pas pliées à leur obligation de désigner un DPO ;
- puis, le 5 mai 2022, avoir mis en demeure 22 de ces communes n'ayant pas tenu compte de cette mise garde.

Le 4 octobre 2022, la CNIL a publié un bilan de ces mises en demeure, dont il ressort que :

- 18 communes ont procédé à la désignation d'un DPO, ce qui a entrainé la clôture de leur mise en demeure ;
- 2 communes sont « *en cours de désignation* » d'un DPO ;
- 2 communes n'ont pas répondu à la CNIL, ni désigné de DPO.

La CNIL a annoncé que, s'agissant des communes qui ne se sont pas conformées à la mise en demeure, celles-ci pourront faire l'objet d'une procédure afin que soient prononcées, le cas échéant, « *d'autres mesures correctrices telles qu'une amende ou une injonction sous astreinte* ».

Source : ici

ANALYSE DE L'ETAT EMOTIONNEL DES APPELANTS (IA)

La « *base légale* » d'un traitement est ce qui autorise légalement sa mise en œuvre, permettant ainsi à l'organisme de traiter licitement des données à caractère personnel. On parle également de « *fondement juridique* » ou de « *base juridique* » du traitement.

En application de l'article 6 du RGPD, il existe six bases légales : le consentement (la personne a consenti au traitement de ses données) ; le contrat (le traitement est nécessaire à l'exécution ou à la préparation d'un contrat avec la personne concernée) ; l'obligation légale (le traitement est imposé par des textes légaux) ; la mission d'intérêt public (le traitement est nécessaire à l'exécution d'une mission d'intérêt public) ; la sauvegarde des intérêts vitaux (le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée, ou d'un tiers) ; l'intérêt légitime (le traitement est nécessaire à la poursuite d'intérêts légitimes de l'organisme qui traite les données ou d'un tiers, dans le strict respect des droits et intérêts des personnes dont les données sont traitées).

Pour fonder un traitement sur l'intérêt légitime, l'organisme doit respecter certaines exigences.

Il doit opérer une pondération entre son propre intérêt au traitement et les intérêts ou libertés et droits fondamentaux des personnes concernées par le traitement (en intégrant notamment dans son analyse les « *attentes raisonnables* » de ces personnes).

Selon la CNIL, « *cette "mise en balance" des droits et intérêts en cause doit être réalisée pour chaque traitement fondé sur l'intérêt légitime, au regard des conditions concrètes de sa mise en œuvre*. »[1]

L'autorité française de protection des données ajoute que « *l'intérêt légitime ne peut donc être considéré comme une base légale "par défaut" : il requiert au contraire un examen attentif de la part de l'organisme et le suivi d'une méthodologie rigoureuse.* »[2]

La prise en compte des « *attentes raisonnables*» des personnes dans l'exercice de pondération est essentielle afin de ne pas les surprendre dans les modalités de mise en œuvre comme dans les conséquences du traitement.

Ainsi, selon la CNIL, « *la démonstration d'un intérêt légitime sera plus aisée pour un dispositif qui peut être raisonnablement anticipé, dans un contexte donné (par exemple, la réalisation d'actions de fidélisation de personnes déjà clientes de la société), que pour un traitement divergeant des attentes des personnes (par exemple, l'utilisation d'un réseau social implique la mise en relation d'individus, mais le profilage de leurs actions en vue de leur adresser de la publicité ciblée peut dépasser leurs attentes raisonnables)*. »[3]

Dans cette optique de prise en compte des « *attentes raisonnables* », la CNIL recommande à l'organisme de prévoir des « *mesures compensatoires ou additionnelles* » visant à limiter les impacts du traitement sur les personnes concernées, et ce afin d'atteindre un équilibre entre les droits et intérêts en cause. « *Par exemple, il peut être prévu, pour un traitement de ciblage fin des comportements d'achats en ligne des individus, susceptible de révéler de nombreuses préférences et habitudes touchant à leur intimité, un droit d'opposition inconditionnel des personnes, afin de leur permettre de faire cesser le profilage intrusif dont ils font l'objet*. »[4]

L'affaire[5]

A la suite d'une plainte, l'autorité hongroise de protection des données a enquêté sur les pratiques d'une banque qui avait recours à un dispositif (i) d'enregistrement des conversations téléphoniques du service clientèle et (ii) d'analyse automatique de l'état émotionnel des appelants, ainsi que qu'autres caractéristiques de la conservation et ce, aux fins d'identifier et de rappeler les clients mécontents.

La seule mention d'information portée à connaissance des clients de la banque était celle figurant sur le site internet de cette dernière, rédigée comme suit : « *[La banque] effectue un profilage fondé sur l'intérêt légitime et sélectionne les appels par décision automatique afin qu'un employé de la banque plus qualifié puisse résoudre le problème ou la plainte soulevée dans l'appel au moyen d'un rappel* ».

Après instruction du dossier, l'autorité hongroise de protection des données a identifié plusieurs manquements de la banque au RGPD.

L'autorité a, tout d'abord, rappelé qu'un tel dispositif basé sur l'intelligence artificielle doit être déployé sous réserve de garanties appropriées parce que les personnes concernées sont bien souvent incapables d'évaluer l'impact du traitement sur leurs droits individuels, une telle technologie permettant « *d'obtenir des données dont le client n'a même pas conscience* » faisant passer la personne concernée « *du statut de sujet de la procédure à celui d'objet* ».

Or, en l'espèce, l'autorité, relevant que non seulement « *l'information préalable adéquate* » faisait défaut, mais que le droit d'opposition n'était pas assuré, a considéré que la banque, qui se fondait sur l'intérêt légitime comme base légale du traitement, a seulement établi que le traitement est « *nécessaire aux fins de l'intérêt qu'elle cherche à atteindre* » sans jamais véritablement prendre en compte « *les intérêts des personnes concernées* ».

Dès lors que « *la mise en balance des intérêts effectuée par la banque ne fournit pas un résultat équitable fondé sur l'analyse requise par le Règlement général sur la protection des données* » et qu'en conséquence, « *la primauté de l'intérêt légitime qui la fonde sur les droits et libertés de la personne concernée ne peut être établie* », la banque n'a pas respecté les dispositions du RGPD.

En raison de l'invalidité de la mise en balance des intérêts, l'autorité a considéré que le traitement d'analyse automatique des enregistrements audio ne reposait sur aucune base légale, et ce en violation des dispositions de l'article 6 du RGPD. Compte tenu de ce qui précède, l'autorité a prononcé à l'encontre de la banque une amende d'un montant de plus de six millions d'euros.

Quelles recommandations ?

En cas de déséquilibre, il est indispensable pour le responsable du traitement de mettre en œuvre des mesures compensatoires permettant d'atteindre un équilibre effectif entre son intérêt légitime et les droits et intérêts des personnes concernées par le traitement.

Si la pondération apparaît ainsi équilibrée, il peut fonder son traitement sur la base légale de l'intérêt légitime. Dans le cas contraire, une autre base légale, comme le consentement, doit être envisagée.

Alexandre Fievée

(1) https://www.cnil.fr/fr/les-bases-legales/interet-legitime

(2) https://www.cnil.fr/fr/les-bases-legales/interet-legitime

(3) https://www.cnil.fr/fr/les-bases-legales/interet-legitime

(4) https://www.cnil.fr/fr/les-bases-legales/interet-legitime

(5) Autorité hongroise pour la protection des données, NAIH-85-3/2022,8 février 2022.

ACTUALITÉS EUROPÉENNES

PANORAMA DE QUELQUES DECISIONS RENDUES PAR DES AUTORITÉS NATIONALES DE CONTRÔLE

La collecte de données sur la séropositivité d'un patient est illicite si elle a pour but de refuser des soins

GPDP (Italie), 10 juin 2021

L'autorité de contrôle italienne a été saisie d'une plainte d'un patient reprochant à son dentiste de lui avoir fait remplir un questionnaire de santé préalable. Après avoir indiqué sa séropositivité dans ledit questionnaire, le patient s'est vu refuser les soins.

Un dentiste a fait remplir à ses patients un questionnaire de santé demandant explicitement d'indiquer les maladies infectieuses dont les patients souffraient et a refusé de prodiguer des soins à un patient faisant état de sa séropositivité, au motif que « *le diagnostic de séropositivité ne lui permettait pas de prévenir une éventuelle contagion du personnel et des autres patients* ».

Saisie d'une plainte, l'autorité de contrôle a ouvert une enquête et demandé au dentiste « *les raisons qui rendraient indispensable la collecte, au moment de l'admission d'un nouveau patient, d'informations concernant sa séropositivité* ».

Dans ses développements, l'autorité de contrôle a rappelé l'existence d'une loi italienne de 1990 qui prévoit des dispositions spécifiques pour la protection des professionnels de santé contre l'infection par le VIH : face à l'impossibilité d'identifier avec certitude tous les patients infectés par le VIH, la loi oblige à prendre des précautions à l'égard de l'intégralité des patients, et non uniquement ceux séropositifs.

Partant de cette loi, l'autorité de contrôle, dans une précédente affaire, avait jugé contraire au RGPD « *la collecte d'informations relatives à la séropositivité de tout patient qui se présente pour la première fois dans un cabinet médical, indépendamment du traitement à réaliser* ». Autrement dit, un professionnel de santé ne peut pas utiliser des données relatives à la séropositivité d'un patient pour refuser des soins, en revanche, il peut légitimement recueillir lesdites données si ces informations sont nécessaires « *compte tenu du type d'intervention médicale ou du plan de traitement à effectuer* », c'est-à-dire compte tenu de la finalité de diagnostic et de soins.

En l'espèce, l'autorité de contrôle reproche au dentiste d'avoir traité les données relatives à la séropositivité pour refuser des soins (finalité de refus de soin) et non pour améliorer le diagnostic et les soins. En conséquence, le dentiste a, selon l'autorité de contrôle, « *effectué un traitement de données à caractère personnel en violation de l'article 5 du RGPD* » dès lors que « *les données traitées n'étaient pas pertinentes au regard des finalités pour lesquelles elles étaient traitées* ».

Compte tenu de tout ce qui précède, l'autorité de contrôle a infligé au dentiste une amende de 20 000 €.

Source : ici

Le profilage opéré par une banque doit se fonder sur le consentement de ses clients

Die Landesbeauftragte für den Datenschutz (LfD) Niedersachsen (Allemagne), 28 juillet 2022

L'autorité de contrôle de Basse-Saxe a constaté que de nombreuses banques détournaient l'utilisation de données personnelles de leurs clients, initialement traitées de manière licite, afin d'effectuer du profilage publicitaire illicite.

Une banque a fait appel à un prestataire externe afin de réaliser un profilage de ses clients (actuels et anciens). Dans les faits, la banque utilisait le « *comportement numérique* » de ses clients (achats en ligne ou sur des « stores » d'applications, virements auprès de banques en ligne, etc.) pour enrichir ses données à l'aide d'une agence tierce et leur proposer des publicités ciblées sur des services numériques.

Au cours de son enquête, l'autorité de contrôle a, certes, constaté que les personnes concernées avaient été informées de l'existence du profilage, conformément à l'article 13 du RGPD, mais qu'en dépit de cette information, le traitement ne reposait sur aucune base légale valide.

Effectivement, l'autorité de contrôle reproche à la banque d'avoir effectué ledit profilage en utilisant l'intérêt légitime comme base légale, alors que le consentement des personnes concernées aurait dû être recueilli.

Il était impossible d'utiliser l'intérêt légitime de la banque car (i) les intérêts et les libertés et droits fondamentaux des personnes concernées prévalaient sur les intérêts légitimes poursuivis par la banque et (ii) les clients ne pouvaient pas raisonnablement s'attendre à ce que leur banque utilise à grande échelle les bases de données des clients pour établir des profils.

Die Landesbeauftragte für den Datenschutz Niedersachsen

Selon l'autorité de contrôle, l'intérêt légitime est d'autant plus difficile à justifier lorsque la banque fait appel à des organismes externes qui concatènent les données afin d'établir des profils encore plus précis des personnes concernées, comme ce fut le cas en l'espèce.

Pour toutes ces raisons, face à l'absence de consentement, seule base légale acceptable, l'autorité de contrôle a infligé à la banque une amende de 900 000 €.

Source : ici

Les dossiers médicaux des patients ne doivent pas être accessibles à tous les professionnels de santé

GPDP (Italie) 26 mai 2022

L'autorité de contrôle italienne a sanctionné un établissement de santé pour avoir permis aux professionnels de santé non impliqués dans le processus de traitement d'accéder aux dossiers médicaux des patients.

Après avoir reçu une plainte et deux notifications de violations de données, l'autorité de contrôle a ouvert une enquête à l'encontre d'un établissement de santé qui permettait l'accès aux dossiers médicaux de patients par des professionnels de santé qui n'étaient pas impliqués dans le processus de traitement.

Interrogé, l'établissement de santé a détaillé les critères d'accès aux dossiers médicaux par les professionnels de santé :

- Si le patient est « en cours de traitement » (c'est-à-dire qu'il est présent dans un des services de l'établissement), son dossier médical est accessible à tout le personnel de santé.
- Si le patient n'est pas en cours de traitement, l'accès à son dossier médical est réservé aux seuls personnels de santé qui déclarent qu'ils ont le droit de consulter lesdites données. En l'absence de déclaration (engageant la responsabilité du professionnel de santé), le système se bloque et l'accès au dossier est refusé.

Au cours de son enquête, l'autorité de contrôle a reproché à l'établissement de santé :

- d'une part, de permettre à tout professionnel de santé d'accéder aux dossiers médicaux des patients en cours de traitement sans limiter l'accès « *au seul personnel soignant qui traite effectivement le patient* », et ;
- d'autre part, comme en témoignent les notifications de violation de données et la plainte reçue, de ne pas suffisamment empêcher l'accès aux dossiers médicaux des patients qui ne sont pas en cours de traitement aux seuls professionnels de santé autorisés, notamment en omettant d'installer un système d'alerte permettant de « *détecter toute anomalie pouvant constituer un traitement illicite* ».

Rappelant le principe selon lequel « *l'accès au dossier médical doit être limité aux professionnels de santé impliqués dans le processus de soins du patient* », l'autorité de contrôle a considéré que l'établissement de santé avait violé (i) les principes d'intégrité et de confidentialité (article 5 du RGPD) et (ii) les règles encadrant le traitement de catégories particulières de données à caractère personnel (article 9 du RGPD).

Plus encore, l'établissement de santé, en tant que responsable du traitement, n'a pas respecté les principes de protection des données dès la conception et la protection des données par défaut (article 25 du RGPD) ni mis en œuvre les mesures de sécurité adéquates (article 32 du RGPD).

En conséquence, l'autorité de contrôle a infligé une amende de 70 000 € à l'établissement de santé.

Source : ici

Transfert de données personnelles en dehors du cadre professionnel

Landesbeauftragte für Datenschutz und Akteneinsicht (Allemagne), Rapport 2021

Dans son rapport annuel 2021 sur la protection des données, l'autorité de contrôle Berlinoise a indiqué avoir infligé des amendes à 3 chiffres à l'encontre de deux employés qui s'étaient transférés des données personnelles pour des finalités extra-professionnelles.

La première affaire concernait l'employée d'une entreprise, gestionnaire de salaires, qui s'était envoyée, sur son adresse électronique privée, un tableau Excel contenant les données de 56 employés de l'entreprise. Dans ce tableau figuraient, notamment, l'identité, les jours de congés, les jours d'absence pour maladie, les données salariales, les heures supplémentaires effectuées et les cotisations auprès de la sécurité sociale des salariés de l'entreprise.

L'employée justifiait ce transfert par la nécessité de se protéger et de protéger ses collègues en raison de relations de travail compliquées.

L'employeur a déposé une plainte pénale, classée sans suite par le ministère public mais transmise à l'autorité de contrôle compétente.

Au cours de son enquête, l'autorité de contrôle a considéré (i) que l'action de l'employée n'était pas imputable à l'entreprise, (ii) que la transmission des données des employés sur son adresse électronique privée n'était pas nécessaire à l'accomplissement des tâches de l'entreprise et ainsi (iii) que la salariée avait « *outrepassé ses compétences et agi en tant que responsable du traitement* ».

En conséquence, l'autorité de contrôle a considéré que l'employée, responsable du traitement, avait traité des données personnelles sans base légale valable, et donc en infraction au RGPD.

Landesbeauftragte
für Datenschutz
und Akteneinsicht

La seconde affaire concernait un employé qui s'était transféré, sur son adresse électronique personnelle, des candidatures reçues par son employeur « *afin de s'inspirer de la présentation visuelle pour ses propres candidatures* ».

L'employeur, constatant que l'employé (i) avait agi sans autorisation, (ii) n'avait pas rendu les CV anonymes et (iii) avait outrepassé ses tâches professionnelles, a déposé plainte.

Au cours de son enquête, l'autorité de contrôle a également considéré que l'employé avait agi en tant que responsable du traitement. Constatant l'absence de consentement des personnes concernées, le traitement a été qualifié de contraire au RGPD pour défaut de base légale.

Face à ces manquements, l'autorité de contrôle a infligé à ces deux responsables du traitement une amende d'un montant à 3 chiffres.

Source : ici

ACTUALITÉS DU CABINET

Le CEPD a annoncé, en septembre dernier, que son action coordonnée 2023 portera sur les problématiques liées à la désignation du DPO et son positionnement.

Dans le cadre de cette action coordonnée, le CEPD invite les autorités nationales de protection des données à travailler sur le sujet.

Jusqu'à présent, l'action « répressive » de la CNIL sur la question du DPO, son positionnement dans l'organisme, ses moyens et ressources, a été relativement limitée.

Faut-il s'attendre à ce que la CNIL diligente des missions de contrôle sur ce sujet ?

A l'aide principalement de décisions d'autorités de contrôle d'autres membres de l'UE, nous essaierons ensemble d'identifier – à partir des manquements constatés - **les principales zones de risques**, telles que :

- L'absence de mentions d'information concernant le DPO dans les politiques de protection des données ;
- L'implication insuffisante du DPO ;
- L'absence de procédure permettant de prévenir les conflits d'intérêts ;
- L'insuffisance des moyens mis à la disposition du DPO ;
- Le manque d'autonomie du DPO ;
- L'absence de justification des missions exercées par le DPO;
- L'absence de plan de contrôle diligenté par le DPO ;
- Le caractère inadapté du niveau hiérarchique du DPO.

Cette matinale, **présentée par Alexandre FIEVEE**, avocat associé, et **Valentin VAUGE,** avocat, aura lieu le **16 novembre 2022** au **Cabinet DERRIENNIC, 5 avenue de l'Opéra 75001 Paris (4e étage)** ou, à votre convenance, via Webinar *(un lien de connexion vous sera adressé).*

Elle débutera à 9h30 précise après un café de bienvenue fixé à 9h00. **RSVP avant le 10 novembre 2022 à l'adresse suivante matinales@derriennic.com (inscription gratuite) en indiquant «Webinar » ou « Présentiel ».**

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

3000€ 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* » (2023).
Il a également fait en 2020 son entrée dans le classement Legal 500 dans la catégorie *« Next Generation Partners* ».

RENSEIGNEMENTS PRATIQUES

Prochaine session en 2022/2023 :
Sur demande.
Lieu de la formation :
Au cabinet Derriennic Associés (5 avenue de l'opéra - 75001 Paris) ou en visio-conférence.
Inscription et informations :