La Newsletter dédiée à la mise en conformité au RGPD

par @DerriennicParis

DERRIENNIC ASSOCIÉS

Conformité RGPD

#NewsDerriennicRGPD 19

Madame, Monsieur,

Nous vous proposons, en cette fin d'année 2019, de découvrir les actualités suivantes :

- 500.000 € d'amende pour démarchage téléphonique illégal
- Le ministre de l'intérieur : un responsable du traitement pas comme les autres
- Une possible fuite de données chez un groupe hôtelier
- Brexit : une décision d'adéquation avant 2021 ?
- Vidéosurveillance à l'insu des salariés : pas d'atteinte à la vie privée

Nous vous en souhaitons une bonne lecture.

500.000 € d'amende pour démarchage téléphonique illégal

FUTURA INTERNATIONALE a été condamnée, par une décision de la CNIL du 21 novembre dernier, au paiement d'une amende administrative de 500.000 €, notamment pour n'avoir pas respecté le droit d'opposition des personnes sollicitées dans le cadre d'opérations de prospection commerciale.

Une particulière a saisi la CNIL d'une plainte au motif que, malgré une opposition à la prospection exprimée oralement auprès des opérateurs téléphoniques et par courrier adressé au siège de FUTURA INTERNATIONALE, les appels n'avaient pas cessé.

Suite à cette plainte, la CNIL a procédé à un contrôle sur place dans les locaux de FUTURA INTERNATIONALE, afin de « vérifier la conformité de tous les traitements en lien avec la prospection commerciale mis en œuvre par ou pour le compte de la société aux dispositions de la loi du 6 janvier 1978 modifiée ».

Ce contrôle a révélé que :

- FUTURA INTERNATIONALE procédait à une collecte directe des données, mais également à une collecte indirecte, auprès de tiers, « dans le cadre d'un programme de parrainage » ;

- FUTURA INTERNATIONALE faisait appel, s'agissant des opérations de prospection commercial téléphonique, à des centres d'appels situés en dehors de l'Union européenne, agissant en qualité de sous-traitants ;

- FUTURA INTERNATIONALE n'avait pas mis en place de « mécanisme centralisé permettant que soient prises en compte les demandes d'opposition exprimées par les personnes démarchées » ;

- parmi les commentaires sur les clients, enregistrés par les téléopérateurs dans leur logiciel de gestion de la clientèle, certains étaient « relatifs à l'état de santé des personnes démarchées » et contenaient « des propos injurieux à leur encontre » ;

- lorsqu'un opérateur appelait un prospect, celui-ci n'était pas systématiquement informé de l'enregistrement de l'appel, ni des caractéristiques du traitement.

Dans ce cadre, la CNIL a mis en demeure FUTURA INTERNATIONALE de prendre un certain nombre de mesures visant à remédier aux manquements identifiés.

Cette mise en demeure étant restée sans effet, la CNIL est entrée en voie de condamnation, s'agissant des manquements suivants :

- un manquement à l'article 5-1-c) du RGPD, dans la mesure où les commentaires injurieux étaient « inadéquats au regard de la finalité pour laquelle les données sont traitées » et que rien ne justifiait « la présence de données relatives à la santé des personnes dans le logiciel de gestion des clients et prospects ».

- un manquement à l'obligation d'information des personnes concernées (articles 12, 13 et 14 du RGPD), la CNIL relevant que « les personnes qui font l'objet de prospection téléphonique ne sont soit destinataires d'aucune information relative à l'enregistrement de l'appel soit sont simplement informées de l'enregistrement de la conversation sans qu'aucune autre information ne leur soit communiquée quant au traitement de leurs données » ;

- un manquement à l'obligation de respecter le droit d'opposition des personnes concernées (article 21 du

RGPD) puisque « quelle que soit la modalité d'expression de l'opposition, celle-ci restait ineffective » ;

- un manquement à l'obligation de coopérer avec l'autorité de contrôle (article 31 du RGPD), la CNIL n'ayant pas obtenu, à la suite du contrôle, communication de l'ensemble des pièces nécessaires à l'exercice de sa mission, malgré les prorogations de délais accordées ;

- un manquement à l'obligation d'encadrer les transferts de données à caractère personnel hors de l'Union européenne, FUTURA INTERNATIONALE réalisant un tel transfert via son logiciel de gestion des clients et prospects, sans avoir prévu de garantie appropriée. La CNIL relève, à ce titre, que les clauses contractuelles auxquelles FUTURA INTERNATIONALE a eu recours suite à la mise en demeure, afin d'encadrer le transfert à ses sous-traitants situés hors du territoire de l'Union européenne, n'ont été adoptées ni par la Commission européenne, ni par une autorité de contrôle.

Compte tenu de ce qui précède, la CNIL a prononcé à l'encontre de FUTURA INTERNATIONALE une amende de 500.000 €, ainsi qu'une injonction de produire les justificatifs de sa mise en conformité, sous astreinte de 500 € par jour de retard à l'issue d'un délai d'un mois suivant la notification de la décision.

Lien vers la décision :
https://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000039419459&fastReqId=461698027&fastPos=1

Le ministre de l'intérieur : un responsable du traitement pas comme les autres

Par un arrêt du 24 octobre 2019, le Conseil d'Etat a considéré que le ministre de l'intérieur, répondant à une demande de droit d'accès, n'est pas tenu de délivrer copie des documents servant de support aux données à caractère personnel.

Pour rappel, l'article 15 du Règlement général sur la protection des données (RGPD) prévoit qu'en cas d'exercice du droit d'accès par une personne concernée, le responsable du traitement doit lui fournir une copie des données à caractère personnel faisant l'objet du traitement.

L'article 41 de la loi dite « Informatique et libertés » n° 78-17 du 6 janvier 1978, dans sa version applicable aux faits, prévoyait un régime dérogatoire s'agissant de l'exercice du droit d'accès dans le cadre des traitements intéressant la sureté de l'état, la défense ou la sécurité publique :

« La demande est adressée à la commission qui désigne l'un de ses membres appartenant ou ayant appartenu au Conseil d'Etat, à la Cour de cassation ou à la Cour des comptes pour mener les investigations utiles et faire procéder aux modifications nécessaires. Celui-ci peut se faire assister d'un agent de la commission. Il est notifié au requérant qu'il a été procédé aux vérifications.

Lorsque la commission constate, en accord avec le responsable du traitement, que la communication des données qui y sont contenues ne met pas en cause ses finalités, la sûreté de l'Etat, la défense ou la sécurité publique, ces données peuvent être communiquées au requérant. »

Ces dispositions figurent, aujourd'hui, en substance, à l'article 118 de la loi du 6 janvier 1978.

En l'espèce, un particulier a saisi la CNIL d'une demande de communication des informations la concernant contenues dans les fichiers de services de l'information générale du ministre de l'intérieur, dans le cadre du droit d'accès prévu à l'article 41 susvisé.

Suite au refus qui a été opposé à cette demande, le Tribunal administratif de Paris, dans un jugement du 13 mai 2016, a, sur demande du particulier, annulé la décision de refus et a enjoint le ministre de l'intérieur de communiquer les informations à la personne concernée sous 3 mois à compter de la notification du jugement, sous astreinte de 100 euros par jour de retard.

Si la personne concernée a pu consulter ces informations dans les locaux d'une préfecture, le 17 novembre 2017, elle n'a pas, en revanche, pu obtenir une copie des documents en cause, malgré les demandes en ce sens.

Estimant que le ministre de l'intérieur n'avait pas correctement exécuté l'injonction qui lui avait été faite, la personne concernée a demandé au Tribunal administratif de Paris de procéder à la liquidation de l'astreinte pour un montant de 34.500 euros. Par jugement du 12 décembre 2017, le Tribunal administratif a liquidé l'astreinte à un montant de 3.650 €.

La Cour administrative d'appel de Paris, saisie par le particulier, a, le 15 novembre 2018, porté l'astreinte à 8.200 € au motif que la complète exécution de cette injonction impliquait la remise d'une copie des documents sollicités et a enjoint le ministre de l'intérieur de délivrer ladite copie au requérant.

Le ministre de l'intérieur s'est pourvu en cassation. Le Conseil d'Etat a donné raison au ministre de l'intérieur, dès lors que le responsable du traitement communique, dans

le cadre de l'article 41, les données à caractère personnel selon les modalités qu'il définit :

« Le ministre de l'intérieur, qui n'était donc pas tenu de remettre à M.B. une copie des documents consultés, a pu valablement exécuter l'injonction qui lui était faite en s'assurant que le requérant puisse consulter les données sollicitées sur place »

Le Conseil d'Etat a, en conséquence, annulé l'arrêt de la Cour administrative d'appel de Paris pour erreur de droit.

Lien vers la décision :
https://www.legalis.net/jurisprudences/conseil-detat-10eme-9eme-ch-reunies-decision-du-24-octobre-2019-2/

Une possible fuite de données chez un groupe hôtelier

D'après un article publié par le journal « Le Parisien », une fuite de donnée serait survenue au sein d'un grand groupe hôtelier français.

Une filiale d'AccorHotels aurait connu une fuite des données à caractère personnel concernant plus de 130.000 voyageurs européens.

Les données concernées par la fuite seraient les suivantes : des historiques de réservation d'hôtels et de transports, des factures, ainsi que des références incomplètes de cartes de crédit.

Le problème ayant conduit à cette fuite aurait eu pour origine un port de firewall laissé ouvert après le déploiement d'une mise à jour sur le serveur de la société, ce qui aurait conduit au libre accès des données pendant plusieurs semaines.

Pour rappel, le Règlement général sur la protection des données (RGPD) prévoit que le responsable du traitement, ainsi que le sous-traitant, mettent en œuvre « toutes les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque ».

En cas de violation de données susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées, le RPGD impose également au responsable du traitement de notifier ladite violation à la CNIL et de la communiquer aux personnes concernées. En l'espèce, ces actions auraient bien été entreprises par la société concernée.

Lien vers l'article de presse :
http://www.leparisien.fr/high-tech/une-filiale-d-accorhotels-au-coeur-d-une-fuite-massive-de-donnees-sensibles-20-11-2019-8197647.php

Brexit : une décision d'adéquation avant 2021 ?

Le texte de Déclaration politique révisée sur le Brexit, adopté par la Commission européenne le 17 octobre dernier, évoque la protection des données à caractère personnel et laisse entrevoir une décision d'adéquation d'ici la fin de l'année 2020.

Le Royaume-Uni ayant décidé de quitter l'Union Européenne, il deviendra un pays tiers au sens du RGPD, ce qui imposera aux entités soumises au RGPD d'encadrer les transferts vers ce pays, à moins que le Royaume-Uni ne soit reconnu par la Commission européenne comme offrant un niveau de protection des données adéquat.

La Commission européenne a adopté, le 17 octobre 2019, une déclaration de politique révisée encadrant les relations futures entre l'Union européenne et le Royaume-Uni. Cette déclaration évoque le sujet de la protection des données dans les termes suivants :

« The Union's data protection rules provide for a framework allowing the European Commission to recognise a third country's data protection standards as providing an adequate level of protection, thereby facilitating transfers of personal data to that third country. On the basis of this framework, the European Commission will start the assessments with respect to the United Kingdom as soon as possible after the United Kingdom's withdrawal, endeavouring to adopt decisions by the end of 2020, if the applicable conditions are met. Noting that the United Kingdom will be establishing its own international transfer regime, the United Kingdom will in the same timeframe take steps to ensure the comparable facilitation of transfers of personal data to the Union, if the applicable conditions are met. The future relationship will not affect the Parties' autonomy over their respective personal data protection rules. »

Ainsi, la Commission affirme entamer les démarches tendant à l'évaluation du niveau de protection des données à caractère personnel offert par le Royaume-Uni et évoque la possibilité d'une décision d'adéquation avant la fin de l'année 2020 si les conditions d'une telle adéquation sont remplies.

Le Royaume-Uni étant actuellement soumis au RGPD et ayant déjà formulé la volonté de se doter de normes internes équivalentes à ce règlement, il est fort probable qu'il soit reconnu par la Commission européenne comme présentant un niveau de protection adéquat.

Lien vers la déclaration :
https://ec.europa.eu/commission/sites/beta-political/files/revised_political_declaration.pdf

Vidéosurveillance à l'insu des salariés: pas d'atteinte à la vie privée

La Cour européenne des droits de l'homme, dans un arrêt du 17 octobre 2019, a considéré que l'utilisation d'un système de vidéosurveillance ayant pour objet d'identifier des personnes responsables de vols supposés ne porte pas atteinte à la vie privée des salariés concernés, quand bien même ces derniers n'ont pas été informés conformément aux règles de droit interne applicables en matière de protection des données.

Un employeur, soupçonnant ses salariés de commettre des vols au sein du supermarché dans lequel ils travaillaient, a procédé à l'installation, d'une part, de « caméras visibles dirigées vers les entrées et sorties du magasin, dont l'employeur avait informé le personnel » et, d'autre part, de « caméras cachées orientées vers les caisses, dont ni les requérantes ni les autres membres du personnel n'avaient été informés ».

Saisies par des employées licenciées à la suite de vols enregistrés par le système de vidéosurveillance, les juridictions espagnoles ont estimé que cette vidéosurveillance constituait « une mesure justifiée (il existait des soupçons raisonnables que la demanderesse avait commis de graves irrégularités sur son lieu de travail), adéquate au regard du but poursuivi par l'entreprise (vérifier si l'employée était responsable des irrégularités et adopter le cas échéant les mesures disciplinaires pertinentes), nécessaire (dans la mesure où l'enregistrement servirait à prouver ces irrégularités) et équilibrée (l'enregistrement s'est limité à la zone des caisses et a eu une durée limitée, suffisante pour vérifier qu'il s'agissait non pas d'un fait isolé ou d'une confusion, mais bien d'un comportement illicite répété). ».

Saisie par les requérantes, la CEDH relève que :

- « la mise en place de la vidéosurveillance se justifiait par des raisons légitimes, à savoir les soupçons, nourris par le directeur du magasin en raison des pertes importantes constatées sur plusieurs mois, que des vols avaient été commis » ;

- « l'ampleur des pertes constatées par l'employeur pouvait donner à penser que des vols avaient été commis par plusieurs personnes et qu'informer l'un quelconque des membres du personnel risquait effectivement de compromettre le but de la vidéosurveillance » ;

- les requérantes « n'étaient pas individuellement ciblées par la vidéosurveillance », les caméras ayant été dirigées vers les caisses ;

- le lieu de travail était ouvert au public et que les activités filmées, à savoir l'encaissement des achats, « n'étaient pas de nature intime ou privée », « l'attente qu'elles [les requérantes] pouvaient avoir s'agissant de la protection de leur vie privée était donc nécessairement réduite » ;

- la vidéosurveillance a durée dix jours et « a cessé dès que les employés responsables ont été identifiés » ;

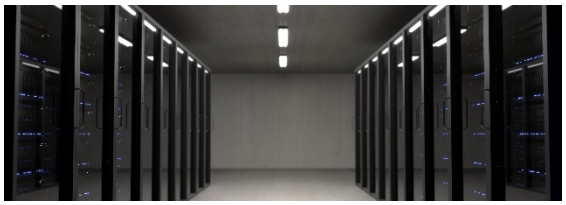
- si la vidéosurveillance et les enregistrements ont bien servi à licencier les requérantes, ceux-ci « n'ont pas été utilisés par l'employeur à d'autres fins que celle de trouver les responsables des pertes de produits constatées et de les sanctionner » ;

- si le droit interne applicable exigeait une information des personnes s'agissant du traitement de leurs données à caractère personnel, qui n'est pas nécessairement complète en l'espèce, « l'information donnée à la personne faisant l'objet d'une surveillance et son ampleur ne sont que l'un

des critères à prendre en compte pour apprécier la proportionnalité d'une telle mesure dans un cas donné ».

La Cour a, en conséquence, conclut à l'absence de manquement à l'article 8 de ce la Convention européenne des droits et de l'homme, et a donné raison aux juridictions espagnoles.

Lien vers la décision :
https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-197095%22]}



SAVE THE DATE !

#MatinaleDerriennic :

11/12/2019 : OUTILS DE CONFIRMITÉ RGPD - Privacy by design et PIA

19/12/2019 : RGPD - Bilan 2019