La Newsletter dédiée à la mise en conformité au RGPD

par @DerriennicParis

DERRIENNIC ASSOCIÉS

Conformité RGPD

#NewsDerriennicRGPD 15

Madame, Monsieur,

Nous vous proposons, en ce mois de juin, une lettre RGPD composée des actualités suivantes :

- Retour sur le rapport d'activité de la CNIL 2019 ;
- Détournement de finalité : le gendarme sanctionné ;
- Mise en demeure du département britannique en charge des taxes et des douanes pour défaut de base juridique ;
- Sanction de la CNIL sans mise en demeure préalable confirmée par le Conseil d'Etat ;
- Un nouveau décret sur la protection des données personnelles.

Retour sur le rapport d'activité 2018 de la CNIL

La CNIL a présenté, le 15 avril 2019, son rapport d'activité pour l'année 2018.

1. Outre les l'augmentation considérable du nombre des plaintes (11 077 en 2018, soit une croissance de 32.5% par rapport à 2017) et les 310 contrôles, que le cabinet avait évoqué au sein d'une précédente publication, le rapport d'activité de la CNIL pour l'année 2018 fait également état des chiffres suivants :

- 39 500 organismes ont désigné un délégué à la protection des données ; et 16 000 délégués à la protection des données ont été nommés.
- 4 264 demandes de droit d'accès indirect ont été adressées à la CNIL.
- 1 170 notifications de violations de données ont été reçues par la CNIL, dont 981 sont exclusivement liées à la perte de confidentialité. Ces violations concernent principalement le secteur de l'hébergement et de la restauration (188 notifications), le commerce, la réparation d'automobiles et de motocycles (180 notifications), les activités financières et d'assurance (139 notifications), ainsi que les activités spécialisées, scientifiques et techniques (137 notifications), l'information et la communication (100 notifications) et l'administration publique (92 notifications).

2. S'agissant des sujets de réflexion pour l'année 2019, la CNIL indique qu'elle s'intéressera :

- aux assistants vocaux ;
- au cloud computing, la CNIL s'inquiétant, à ce sujet, de la concentration du risque, ainsi que du pouvoir de négociation, jugé limité, des entités souhaitant recourir au cloud ;
- au partage de données, la CNIL estimant nécessaire « d'encourager le développement d'un modèle efficace et durable de portage des données, intégrant une forte composante éthique, basé sur le respect des droits fondamentaux, au titre desquels figure naturellement la protection des données personnelles et de la vie privée » ;
- à la communication politique, au sujet duquel la CNIL évoque notamment l'utilisation abusive de données à caractère personnel lors des campagnes politiques ;
- à la réutilisation de données accessibles « en ligne » par le monde de la recherche ;
- à la protection des données des enfants.

3. Si la CNIL a indiqué poursuivre en 2019 et renforcer sa politique d'accompagnement, elle précise que « cette amplification des actions d'accompagnement s'opèrera en parallèle d'un contrôle exigeant et, dans les cas qui le nécessitent, des sanctions seront prononcées car la crédibilité du RGPD repose aussi sur une politique de contrôles et de sanctions efficace (…) ».

Voir le rapport de la CNIL : *https://www.cnil.fr/fr/presentation-du-rapport-dactivite-2018-et-des-enjeux-2019-de-la-cnil*

.

Détournement de finalité : le gendarme sanctionné

Le 24 avril 2019, le Conseil d'Etat a rendu un arrêt par lequel il a confirmé la sanction d'un capitaine de gendarmerie qui a consulté, à des fins personnelles, des fichiers opérationnels de la gendarmerie.

Un capitaine de gendarmerie avait consulté, à des fins personnelles, des fichiers opérationnels de la gendarmerie relatifs à l'employeur de sa fille et avait consulté sans justification plus de 300 fiches individuelles de renseignements entre le 1er août 2014 et le 22 avril 2015.

Pour ce motif, par décision du 6 avril 2016, le ministre de la défense avait prononcé, à l'encontre de l'intéressé, une sanction de quinze jours d'arrêts.

Le Conseil d'Etat, saisi d'une demande d'annulation de la décision de sanction a, dans un premier temps, rappelé les dispositions de l'article 226-21 du Code pénal, sur le détournement de finalité :

« Le fait, par toute personne détentrice de données à caractère personnel à l'occasion de leur enregistrement, de leur classement, de leur transmission ou de toute autre forme de traitement, de détourner ces informations de leur finalité telle que définie par la disposition législative, l'acte réglementaire ou la décision de la Commission nationale de l'informatique et des libertés autorisant le traitement automatisé, ou par les déclarations préalables à la mise en œuvre de ce traitement, est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende. »

Selon le Conseil d'Etat, « la consultation par le capitaine C…, à des fins personnelles, des fichiers de gendarmerie ainsi que de nombreuses fiches individuelles de renseignements pour rechercher des informations concernant l'employeur de sa fille ainsi que plusieurs autres personnes constitue un détournement de la finalité d'un traitement de données à caractère personnel. Un tel manquement est constitutif d'une faute de nature à justifier une sanction disciplinaire, indépendamment des suites réservées aux procédures judiciaires éventuellement engagées. Par suite, le moyen tiré de ce que les faits reprochés à l'intéressé ne présentent pas de caractère fautif doit être écarté. »

S'agissant de la proportionnalité de la sanction infligée, le Conseil d'Etat a estimé : « Eu égard aux responsabilités de M.C…, à la nature des faits reprochés et au caractère répété et persistant des manquements constatés, le ministre de la défense n'a pas, dans les circonstances de l'espèce, pris une sanction disciplinaire disproportionnée en lui infligeant une sanction du premier groupe de quinze jours d'arrêts. »

Ainsi, le Conseil d'Etat a rejeté la demande d'annulation de la décision de sanction.

Voir la décision du Conseil d'Etat : *https://www.legifrance.gouv.fr/affichJuriAdmin.do?idTexte=CETATEXT000038420447*

Mise en demeure du département britannique en charge des taxes et des douanes pour défaut de base juridique

Her Majesty's Revenues and Customs (HMRC), le département britannique responsable de la collecte des taxes et du paiement de certains services fournis par l'Etat, a fait l'objet d'une mise en demeure de la part de l'autorité de contrôle britannique (l'ICO) pour défaut de base juridique, concernant le traitement de données biométriques qu'elle réalise aux fins d'authentification de ses utilisateurs.

Depuis janvier 2017, HMRC utilisait un système d'authentification vocal pour l'authentification de ses utilisateurs, lorsque ces derniers avaient recours à l'assistance téléphonique de HMRC.

HMRC n'avait pas offert d'autre moyen, pour les appelants, de s'identifier et l'information donnée aux personnes concernées, selon l'ICO, était incomplète.

En 2018, HMRC publia une information relative à la confidentialité de son système d'authentification vocale et sollicita les utilisateurs du service afin de recueillir leur consentement. Seuls 20% des 7 millions d'utilisateurs répondirent à cette sollicitation.

Pour autant, HMRC ne supprima pas les données relatives aux personnes concernées qui s'étaient abstenues de répondre positivement.

L'ICO relève que HMRC ne peut s'appuyer sur aucune des bases juridiques de l'article 6, paragraphe 1, du RGPD. Il ne peut, à ce titre, s'appuyer sur le consentement, puisqu'il n'a pas délivré une information suffisante s'agissant de la façon dont les données biométriques allaient être traitées et n'a pas donné aux utilisateurs la possibilité de refuser de donner leur consentement au traitement.

De plus, s'agissant d'un traitement de données biométriques, aucune des conditions de l'article 9 (« Traitement portant sur des catégories particulières de données à caractère personnel ») paragraphe 2 du RGPD n'était réunie. L'ICO ne peut, pour les mêmes raisons que s'agissant de la base juridique, se prévaloir du consentement des utilisateurs.

En conséquence, l'ICO a qualifié le traitement de donnée d'illicite et a mis en demeure HMRC, dans un délai de 28 jours, de :

- supprimer les données biométriques liées au système d'authentification vocal pour lesquelles HMRC n'a pas obtenu de consentement explicite ;

- solliciter ses fournisseurs afin qu'ils fassent de même.

Voir la mise en demeure de l'ICO : *https://ico.org.uk/media/action-weve-taken/enforcement-notices/2614924/hmrc-en-201905.pdf*

Sanction de la CNIL sans mise en demeure préalable confirmée par le Conseil d'Etat

Le 17 avril dernier, le Conseil d'Etat a rendu un arrêt par lequel il a confirmé une sanction pécuniaire infligée par la formation restreinte de la CNIL sans mise en demeure préalable à une association ayant manqué à son obligation de sécurité.

La formation restreinte de la CNIL avait prononcé, en juin 2018, une sanction sans mise en demeure préalable, de 75 000 euros, assortie d'une mesure de publicité de 2 ans, à l'encontre de l'Association pour le Développement des Foyers (ADEF) pour avoir insuffisamment protégé les données des utilisateurs de son site internet.

L'Association a formé un recours devant le Conseil d'Etat afin d'obtenir l'annulation de cette décision.

Le Conseil d'Etat, pour rejeter la requête de l'ADEF, a relevé les trois éléments suivants :

1. S'agissant de l'absence de mise en demeure préalable à la sanction :

L'article 45 de la Loi « Informatique et libertés » prévoit notamment que, « […] Lorsque le manquement constaté ne peut faire l'objet d'une mise en conformité dans le cadre d'une mise en demeure, la formation restreinte peut prononcer sans mise en demeure préalable et après une procédure contradictoire, les sanctions prévues au présent I ».

En l'espèce, le Conseil d'Etat a constaté qu'à la suite de la mise en place de mesures correctrices par l'ADEF, le manquement aux obligations de sécurité avait cessé et il n'était dès lors plus possible de faire l'objet d'une régularisation. Le Conseil d'Etat valide donc la sanction sans mise en demeure préalable.

2. S'agissant du montant de la sanction pécuniaire :

L'article 47 de la Loi « Informatique et libertés » précise les critères permettant de fixer le montant d'une sanction pécuniaire. Notamment, « Celui-ci doit être proportionné à la gravité du manquement commis et aux avantages tirés de ce manquement. »

Le Conseil d'Etat a ainsi relevé que :

- le manquement résultait d'un défaut de sécurité du formulaire en ligne de demande de logement qui permettait par simple modification de l'URL d'accéder aux documents téléchargés par les demandeurs de logement ;

- les documents en question (bulletin de paie, avis d'imposition, justificatifs d'identité…) contenaient des données à caractère personnel.

Le Conseil d'Etat a estimé que la sanction infligée (75 000 euros) n'était pas disproportionnée eu égard :

- à la gravité du manquement, qu'il aurait été possible de prévenir par des mesures simples de sécurité, comme l'occultation des chemins d'accès aux dossiers enregistrés ou l'authentification des utilisateurs du traitement ;

- aux moyens importants dont dispose l'association ;

- au délai avec lequel elle a apporté les mesures correctrices pour remédier au manquement.

3. S'agissant de la mesure de publicité :

Le Conseil d'Etat a rappelé que la sanction complémentaire de publication doit respecter le principe de proportionnalité et que la légalité de cette sanction s'apprécie au regard du support de diffusion retenu et, le cas échéant,

de la durée pendant laquelle cette publication est accessible de façon libre et continue.

Le Conseil d'Etat a relevé que la publication d'une sanction financière à pour intérêt de présenter un caractère dissuasif et un caractère informatif pour les utilisateurs du traitement concerné des risques auxquels ils ont été confrontés.

Compte tenu de cet intérêt, le Conseil d'Etat a estimé la sanction complémentaire de publication pendant 2 ans justifiée, tant au regard de la gravité du manquement sanctionné que de la quantité des données à caractère personnel concernées.

Voir la décision du Conseil d'Etat : *https://www.legifrance.gouv.fr/affichJuriAdmin.do?&idTexte=CETATEXT000038388017*

Références de la décision : CE 10eme-9eme chambre 17 avril 2019

Un nouveau décret sur la protection des données personnelles

Entré en vigueur le 1er juin 2019, le décret n° 2019-536 du 29 mai 2019 est pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (« Loi Informatique et Libertés »), telle que modifiée par l'ordonnance n° 2018-1125 du 12 décembre 2018 (« le Décret »).

Le Décret n°2019-536 du 29 mai 2019, qui abroge le décret n° 2005-1309 du 20 octobre 2005 pris pour l'application de la Loi Informatique et Libertés, tire les conséquences de forme et de fond de la loi Informatique et Liberté résultant de l'ordonnance susvisée (*https://www.legifrance.gouv.fr/eli/decret/2019/5/29/JUSC1911425D/jo/texte#JORFSCTA000038528457*).

Il prévoit des dispositions concernant notamment : la CNIL (composition, fonctionnement, contrôle de la mise en œuvre des traitements, mesures correctrices, sanctions et astreintes, formalités préalables) et les traitements relevant du régime de protection des données prévu par le RGPD (droit des personnes, obligations du responsable du traitement et du sous-traitant, etc.).