NEWSLETTER RGPD

NUMÉRO 30 ● MARS 2021

Madame, Monsieur,

Les violations de données et la sécurité des données sont sous les projecteurs. La CNIL a sanctionné un responsable du traitement et son sous-traitant pour manquement à l'obligation de sécurisation des données. Le CEPD a, pour sa part, publié un document recensant un certain nombre d'exemples de violations de données et visant à aider les responsables de traitement à gérer ces violations.

Nous vous proposons donc, ce mois-ci, de découvrir les articles suivants :

Nous vous avons également préparé un « flash info » sur la fin de la période d'adaptation laissée par la CNIL pour se mettre en conformité au nouveau cadre règlementaire en matière de cookies. **P.2**

Nous vous souhaitons une bonne lecture de la présente lettre.

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. **P8**

FLASH INFO

COOKIES : LA « PERIODE D'ADAPTATION » S'ACHEVE LE 31 MARS 2021

Par une publication en date du 4 février dernier (accessible ici), la CNIL a rappelé que la période accordée aux opérateurs pour mettre en conformité leurs sites web et applications mobiles prend fin le 31 mars 2021.

Pour mémoire, par deux délibérations du 17 septembre 2020, la CNIL avait adopté, d'une part, de nouvelles lignes directrices relatives à l'utilisation des cookies (accessibles ici) et, d'autre part, la version définitive de ses recommandations visant à proposer des modalités pratiques de recueil d'un consentement conforme aux règles applicables (accessible ici).

A cette occasion, la CNIL avait précisé qu'elle ne sanctionnerait les manquements au nouveau cadre juridique qu'à l'issue d'une « période d'adaptation » de 6 mois, soit à compter du 1er avril 2021.

Cette période d'adaptation arrivant prochainement à son terme, la CNIL incite les opérateurs à auditer leurs sites web et applications mobiles pour se mettre en conformité avec le nouveau cadre règlementaire.

Nous nous tenons à votre disposition pour en discuter et vous accompagner dans cette démarche de mise en conformité.

*****

CONSENTEMENT :

COMPTEURS COMMUNICANTS LINKY : LA CNIL CLOTURE SA MISE EN DEMEURE A L'ENCONTRE D'EDF

PAR UNE DECISION DU 15 FEVRIER DERNIER (ACCESSIBLE ICI), LA CNIL A CLOTURE SA MISE EN DEMEURE A L'ENCONTRE DE LA SOCIETE EDF CONCERNANT LE TRAITEMENT DES DONNEES DE CONSOMMATION D'ELECTRICITE COLLECTEES DANS LE CADRE DES COMPTEURS COMMUNICANTS LINKY.

Pour mémoire, par une décision du 31 décembre 2019 (accessible ici), rendue publique le 11 février 2020, la CNIL avait mis en demeure la société EDF de se mettre en conformité avec les dispositions du RGPD en raison du non-respect de certaines exigences relatives au recueil du consentement et d'une durée de conservation excessive des données de consommation issues des compteurs communicants LINKY.

La CNIL avait accordé à EDF un délai de trois mois pour se mettre en conformité, délai qui avait été prolongé en raison de la crise sanitaire liée à la COVID-19.

Après plusieurs échanges entre la CNIL et EDF, l'autorité de contrôle a estimé que les éléments de réponse apportés permettent de démontrer que les manquements constatés lors du contrôle ont depuis cessé.

Dans ce contexte, la CNIL a procédé à la clôture de la mise en demeure en indiquant toutefois que « si la persistance ou la réitération des manquements visés dans la mise en demeure était constatée à l'occasion de vérifications ultérieures, une procédure de sanction pourrait être engagée à l'encontre [d'EDF] conformément aux articles 20 et suivants de la loi du 6 janvier 1978 modifiée ».

SECURITE :

LES EXEMPLES DE VIOLATIONS DE DONNEES DU CEPD

LE CEPD A ADOPTE, LE 14 JANVIER 2021, DES LIGNES DIRECTRICES VISANT A AIDER LES RESPONSABLES DE TRAITEMENT A GERER LES VIOLATIONS DE DONNEES, ET NOTAMMENT A EVALUER DES RISQUES.

Le RGPD définit la violation de données comme : « une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données ».

Le RGPD impose aux responsables du traitement :

- de documenter les violations de données, par exemple au moyen d'un registre des violations ;
- de notifier à l'autorité de contrôle les violations de données susceptibles d'engendrer un « risque pour les droits et libertés des personnes physiques » ;
- de communiquer les violations de données susceptibles d'engendrer un « risque élevé pour les droits et libertés des personnes physiques » aux personnes concernées.

Afin d'aider les responsables du traitement à satisfaire à ces obligations, le CEPD a publié des lignes directrices présentant des exemples de violations de données et détaillant, pour chaque exemple :

- les mesures de prévention qui auraient pu permettre d'éviter la violation ;
- l'évaluation des risques ;
- les mesures permettant d'atténuer les effets de la violation ;
- les obligations à la charge du responsable du traitement (inscription au registre des violations, notification à l'autorité de contrôle, communication aux personnes concernées).

Ainsi, le CEPD prend l'exemple d'un ancien salarié ayant récupéré, durant son préavis, des données à caractère personnel relatives aux clients de son employeur afin de les utiliser, à des fins de prospection, pour son propre compte. Le CEPD fait les observations suivantes :

- aucune mesure de prévention ne peut être mise en œuvre efficacement, compte tenu du fait que le salarié avait accès aux données de façon légitime, dans le cadre de l'exécution de son contrat de travail ;
- l'employeur ne peut pas considérer le risque comme faible, puisqu'il ignore les intentions de son ancien salarié s'agissant de l'usage qu'il fera des données ;
- afin d'atténuer les effets de la violation, l'employeur peut utiliser des moyens légaux visant à empêcher l'ancien salarié d'utiliser abusivement les données ;
- le CEPD indique que cette violation doit être notifiée à l'autorité de contrôle, sans qu'il soit nécessaire de la communiquer aux personnes concernées.

Dans le cadre d'une attaque par bourrage d'identifiant (« credential stuffing » cf. notre article sur un responsable du traitement et son sous-traitant sanctionnés par la CNIL) affectant le site internet d'une banque et se traduisant par une fuite de données identifiantes et financières de 100 000 clients, le CEPD indique les éléments suivants :

- le fait que la violation affecte des données financières, et que le nombre de personnes concernées est élevé, rend la violation particulièrement sévère, le risque est ainsi évalué comme étant « élevé », ce qui signifie que la violation doit être notifiée à l'autorité de contrôle et communiquée aux personnes concernées ;
- au titre des mesures de prévention susceptibles de neutraliser ce type d'incident, le CPED recommande au responsable du traitement la mise en œuvre d'une authentification à deux facteurs sur le site internet concerné.

Lien vers les lignes directrices du CEPD :
https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202101_databreachnotificationexamples_v1_en.pdf

SECURITE :

UN RESPONSABLE DU TRAITEMENT ET SON SOUS-TRAITANT CONDAMNES PAR LA CNIL POUR DEFAUT DE SECURITE DES DONNEES

LA CNIL A PRONONCE UNE AMENDE DE 150 000 EUROS, AINSI QU'UNE AMENDE DE 75 000 EUROS, RESPECTIVEMENT A L'ENCONTRE D'UN RESPONSABLE DU TRAITEMENT ET DE SON SOUS-TRAITANT, POUR DEFAUT DE SECURITE DES DONNEES.

La CNIL a, le 27 janvier 2021, publié un communiqué dans lequel elle indique avoir sanctionné un responsable du traitement et son sous-traitant, qui n'auraient pas pris les mesures suffisantes pour faire face à une attaque par bourrage d'identifiants (« credential stuffing ») sur le site internet du responsable du traitement. La CNIL souligne n'avoir pas souhaité rendre publique cette décision.

Les faits sont les suivants : entre juin 2018 et janvier 2020, la CNIL a reçu plusieurs dizaines de notifications de violations de données personnelles en lien avec un site internet de commerce électronique. Après investigations, la CNIL a établi que le site internet avait subi de nombreuses attaques de type « credential stuffing », qui consistent à réaliser, à l'aide d'un robot, un grand nombre de tentatives de connexion au moyen d'identifiants et de mots de passe accessibles sur internet, dont la publication résulte de violations de données antérieures.

La CNIL a estimé que les sociétés mises en cause avaient tardé à mettre en place des mesures permettant de lutter efficacement contre ces attaques répétées, préférant concentrer leur stratégie de réponse sur le développement d'un outil de détection et de blocage des attaques lancées à partir de robots.

Or, le développement de cet outil a pris un an à compter des premières attaques, alors que, selon la CNIL, d'autres mesures auraient pu être mises en œuvre dans l'intervalle :

- limiter le nombre de requêtes autorisées par adresse IP sur le site internet ;
- faire apparaitre un CAPTCHA dès la première tentative d'authentification d'un utilisateur à son compte.

Du fait de ce manque de diligence, qui constitue, pour la CNIL, un manquement à l'obligation de sécurité des données, les données d'environ 40 000 clients ont été rendues accessibles aux attaquants.

La CNIL affirme qu'il appartient au responsable du traitement de décider « de la mise en place de mesures et donner des instructions documentées à son sous-traitant ». Pour sa part, le sous-traitant doit rechercher «les solutions techniques et organisationnelles les plus appropriées» pour assurer la sécurité des données, et «les proposer au responsable du traitement».

Face à ces manquements, la CNIL a prononcé deux amendes distinctes : 150 000 euros à l'encontre du responsable du traitement et 75 000 euros à l'encontre du sous-traitant.

Lien vers la publication de la CNIL : https://www.cnil.fr/fr/credential-stuffing-la-cnil-sanctionne-un-responsable-de-traitement-et-son-sous-traitant

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