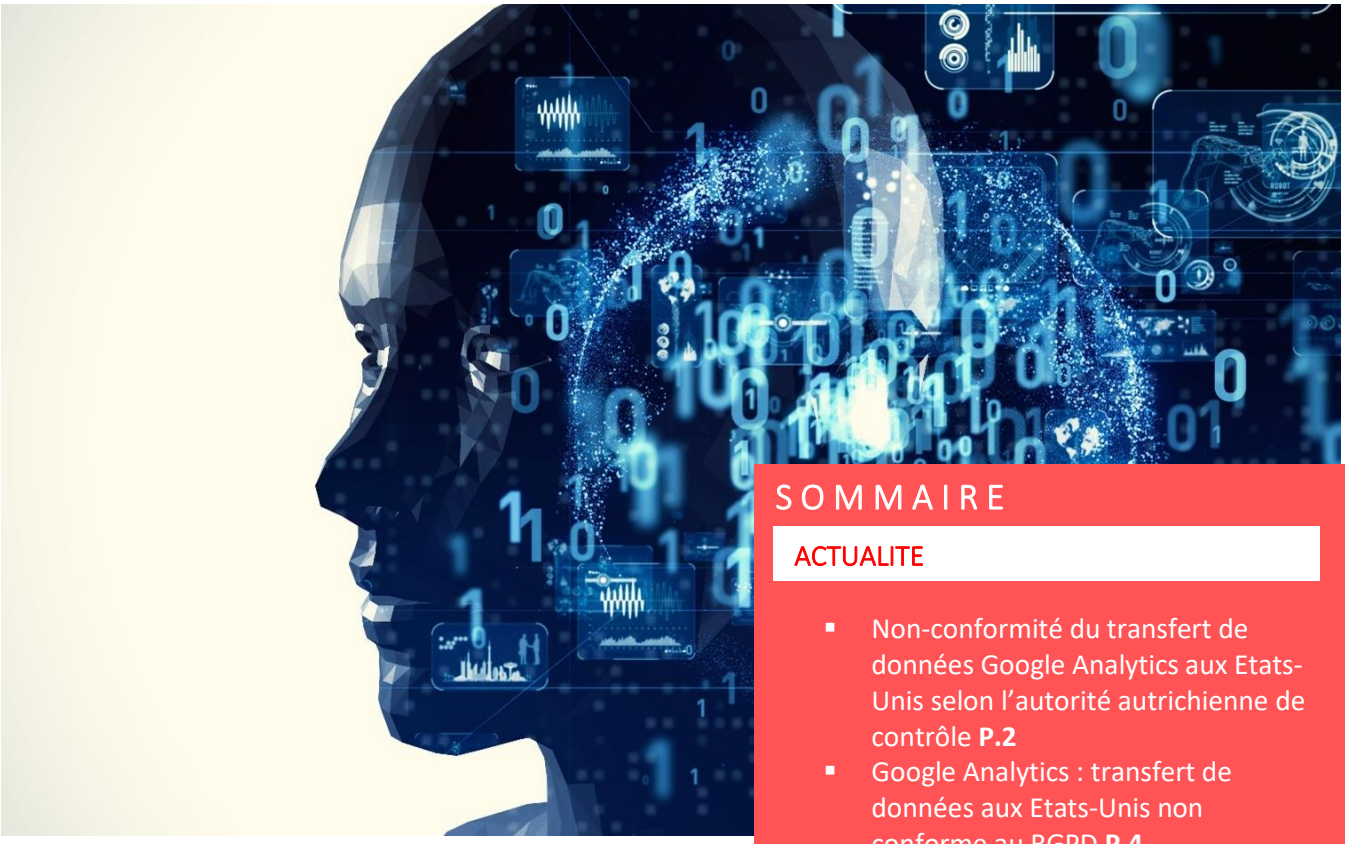
NEWSLETTER RGPD

NUMÉRO 40 • FÉVRIER 2022



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 **P.14**

SOMMAIRE

ACTUALITE

- Non-conformité du transfert de données Google Analytics aux Etats-Unis selon l'autorité autrichienne de contrôle **P.2**
- Google Analytics : transfert de données aux Etats-Unis non conforme au RGPD **P.4**
- Les thèmes prioritaires de contrôle de la CNIL pour l'année 2022 **P.5**
- Facebook condamnée par la CNIL a une amende record **P.8**
- La CNIL prononce une sanction d'un montant de 300 000 euros à l'encontre de Free Mobile **P.9**
- Affaire Benalla : une ONG sanctionnée par la CNIL belge **P.10**

VU DANS LA PRESSE

- DPO : Quelle gouvernance pour être conforme au RGPD ? **P.6**

ACTUALITE EUROPEENNE

- Panorama de quelques décisions rendues par des autorités nationales de contrôle **P.11**

NON-CONFORMITE DU TRANSFERT DE DONNEES GOOGLE ANALYTICS AUX ETATS-UNIS SELON L'AUTORITE AUTRICHIENNE DE CONTROLE

Par une décision du 22 décembre 2021, l'autorité de contrôle autrichienne a estimé que le transfert hors UE de données à caractère personnel opéré par la solution Google Analytics est contraire au RGPD.

A la suite d'une plainte pour violation des principes généraux de transfert de données (articles 44 et suivants du RGPD), adressée le 18 aout 2020 à l'encontre de l'éditeur d'un site web et de Google, l'autorité de contrôle autrichienne s'est penchée sur l'utilisation de Google Analytics, et plus particulièrement sur les transferts de données hors Union Européenne que l'utilisation de cet outil engendre.

Google Analytics, outil de mesure du trafic de sites web, établit des rapports sur la fréquentation des sites et permet de mesurer et d'optimiser l'efficacité des campagnes publicitaires. Dans le cadre de l'utilisation de cet outil, des données sont transférées à Google aux Etats-Unis.

Après s'être déclarée compétente, l'autorité autrichienne de contrôle a d'abord vérifié que les données transitant par l'outil Google Analytics, et *in fine* transférées à Google en dehors de l'Union Européenne, répondent à la définition de données personnelles conformément à l'article 4 du RGPD.

L'autorité de contrôle a relevé qu'un identifiant unique (identifiant à la fois le navigateur et l'appareil de l'internaute) était créé lors de la connexion sur un site doté de Google Analytics. Selon l'autorité, dès lors que ce numéro d'identification permet d'individualiser les visiteurs, les données répondent à la définition de donnée personnelle posée par le RGPD.

L'autorité de contrôle a, ensuite, qualifié l'éditeur du site de responsable du traitement, ce dernier ayant décidé des finalités (analyses statistiques), des moyens de l'outil et ayant pris la décision d'implémenter l'outil sur son site en insérant un code JavaScript.
Google a, quant à lui, été qualifié de sous-traitant, dès lors qu'il se contente de fournir le service Google Analytics et n'exerce aucune influence sur les finalités et moyens.

L'autorité de contrôle a enfin, et surtout, contrôlé le respect, par l'exportateur de données, des dispositions du chapitre V du RGPD qui encadre « *les transferts de données à caractère personnel vers des pays tiers* ».

Après avoir rappelé que les transferts de données à caractère personnel vers les Etats-Unis ne font pas l'objet d'une décision d'adéquation au sens de l'article 45 du RGPD, et que la décision « Schrems II » de la CJUE a estimé que la signature de Clauses Contractuelles Types (« CCT ») ne permet pas de passer outre les programmes de surveillance étatique (notamment le FISA Act) et donc ne garantit donc pas un niveau de protection adéquat au sens de l'article 44 du RGPD, l'autorité de contrôle a vérifié si les <u>mesures complémentaires</u> mises en œuvre par l'éditeur du site web étaient suffisantes pour considérer le transfert de données comme assurant un niveau de protection adéquat.

Au terme d'une analyse *in concreto* des mesures complémentaires mises en œuvre par le responsable du traitement et son sous-traitant, l'autorité de contrôle a qualifié ces mesures d'inutiles et d'inefficaces, puisque ne permettant pas d'empêcher ou de limiter l'accès des agences américaines de renseignement aux données.

Selon l'autorité de contrôle autrichienne, les mesures contractuelles et organisationnelles - (i) « *la notification des demandes de données à la personne concernée* », (ii) « *la publication d'une politique de gestion des demandes gouvernementales* », et (iii) « *l'examen minutieux de toute demande d'accès aux données* » - sont inefficaces, dès lors qu'elles n'empêchent pas l'accès des autorités américaines aux données.

Les mesures techniques - la pseudonymisation, l'anonymisation et le chiffrement - ont également été remises en causes, chacune sur un fondement différent.

L'autorité de contrôle a estimé :

- d'une part, que le fait que les données Google Analytics soient agrégées pour l'éditeur du site web (sous la forme de graphiques et de tableaux) ne constitue pas une pseudonymisation au sens du RGPD, d'autant plus que cet outil peut être cumulé avec d'autres outils (le compte Google de la personne par exemple) pour lever la pseudonymisation ;
- d'autre part, que la fonction d'anonymisation de l'adresse IP, en plus de ne pas être correctement mise en œuvre, n'était pas suffisante pour considérer les données comme anonymes, car n'étant qu'une des nombreuses *« pièces du puzzle » de « l'empreinte numérique du plaignant »* ;
- enfin, le fait que les données présentes dans les data center soient cryptées est insuffisant dès lors que Google est en possession de la clé de déchiffrement. Google a donc la possibilité d'accéder aux donnés en clair.

En conclusion, l'autorité de contrôle a estimé que « *les "mesures complémentaires" en question ne sont pas efficaces, car elles ne comblent pas les lacunes de la protection juridique mises en évidence dans le cadre de l'arrêt de la CJUE du 20 juin 2020, c'est-à-dire les possibilités d'accès et de surveillance des services de renseignement américains ».*

Source : Datenschutzbehörde – DSB (Autriche), 22 décembre 2021
Lien vers la décision en allemand :
https://noyb.eu/sites/default/files/2022-01/E-DSB - Google Analytics_DE_bk_0.pdf

GOOGLE ANALYTICS : TRANSFERT DE DONNEES AUX ETATS-UNIS NON CONFORME AU RGPD

A la suite de plusieurs plaintes émises par l'association NOYB, la CNIL a analysé la conformité au RGPD de Google Analytics, et plus particulièrement la conformité au chapitre V du RGPD, relatif à l'encadrement des transferts de données hors Union Européenne.

Google Analytics est un outil pouvant être intégré sur des sites web, par les gestionnaires de ces derniers, afin de mesurer le trafic. Dans le cadre de l'utilisation de cet outil, des données personnelles sont collectées (notamment l'identifiant du visiteur) puis transférées par Google aux Etats-Unis.

En coopération avec les autres autorités de contrôle européennes, la CNIL a analysé les conditions dans lesquelles les données collectées sont transférées vers les Etats-Unis, pays n'assurant pas un niveau de protection adéquat depuis l'invalidation du Privacy Shield par la Cour de Justice de l'Union Européenne (arrêt « Schrems II »).

La CNIL a d'abord rappelé qu'en l'absence de décision d'adéquation, le transfert de données personnelles vers les États-Unis n'est conforme au RGPD que s'il est encadré par (i) des garanties appropriées (comme des Clauses Contractuelles Types) comportant (ii) des mesures supplémentaires visant à garantir le plein effet des garanties appropriées.

Bien que constatant la présence de mesures supplémentaires, la CNIL a considéré ces dernières insuffisantes car ne permettant pas d'exclure « *la possibilité d'accès des services de renseignements américains à ces données* ».

Google Analytics est un outil pouvant être intégré sur des sites web, par les gestionnaires de ces derniers, afin de mesurer le trafic. Dans le cadre de l'utilisation de cet outil, des données personnelles sont collectées (notamment l'identifiant du visiteur) puis transférées par Google aux Etats-Unis.

En coopération avec les autres autorités de contrôle européennes, la CNIL a analysé les conditions dans lesquelles les données collectées sont transférées vers les Etats-Unis, pays n'assurant pas un niveau de protection adéquat depuis l'invalidation du Privacy Shield par la Cour de Justice de l'Union Européenne (arrêt « Schrems II »).

La CNIL a d'abord rappelé qu'en l'absence de décision d'adéquation, le transfert de données personnelles vers les États-Unis n'est conforme au RGPD que s'il est encadré par (i) des garanties appropriées (comme des Clauses Contractuelles Types) comportant (ii) des mesures supplémentaires visant à garantir le plein effet des garanties appropriées.

Bien que constatant la présence de mesures supplémentaires, la CNIL a considéré ces dernières insuffisantes car ne permettant pas d'exclure « *la possibilité d'accès des services de renseignements américains à ces données* ».

Lien vers l'article de la CNIL :
https://www.cnil.fr/fr/utilisation-de-google-analytics-et-transferts-de-donnees-vers-les-etats-unis-la-cnil-met-en-demeure

LES THÈMES PRIORITAIRES DE CONTRÔLE DE LA CNIL POUR L'ANNÉE 2022

Le 15 février 2022, la CNIL a publié, la liste de ses thèmes propriétaires de contrôle pour 2022, au rang desquels figurent la prospection commerciale, les outils de surveillance dans le cadre du télétravail et l'usage du cloud computing.

La CNIL est investie d'un pouvoir de contrôle afin de vérifier, notamment, le respect des obligations figurant dans la loi du 6 janvier 1978 dite « *Informatique et Libertés* » et le RGPD.

Ces contrôles peuvent résulter de réclamations et de signalements, mais également être menés spontanément, sur la base du programme annuel des contrôles de la CNIL.

Les thèmes composant ce programme sont, pour l'année 2022, les suivants :

1. La prospection commerciale. La CNIL entend contrôler le respect du référentiel dédié à la gestion commerciale, qu'elle a publié le 3 février 2022, lequel inclut des dispositions quant à la réalisation d'opérations de prospection commerciale.

Dans ce contexte, la CNIL rappelle que la prospection commerciale non sollicitée fait partie des « *irritants du quotidien des français* » et constitue un sujet récurent de plaintes et d'appels adressés à la CNIL.

2. Les outils de surveillance dans le cadre du télétravail. La CNIL note que le recours au télétravail a été rendu obligatoire dans le cadre des vagues épidémiques liées à la COVID-19 et pressent que cette pratique pourrait se généraliser et perdurer.

Le recours au télétravail a entrainé le développement d'outils spécifiques, dont certains outils permettant aux employeurs d'assurer un suivi plus étroit des tâches et activités quotidiennes des salariés.

La CNIL indique avoir largement communiqué sur les règles et bonnes pratiques à respecter afin d'assurer un équilibre entre vie privée au travail et contrôle légitime de l'activité des travailleurs et souhaite aujourd'hui vérifier la conformité des pratiques des employeurs.

3. L'utilisation de l'informatique en nuage (*cloud computing*). Selon la CNIL, le recours aux technologies de *cloud computing* est susceptible d'impliquer des transferts de données hors UE. Elle compte donc approfondir les questions relatives aux transferts de données et à l'encadrement des relations contractuelles entre responsables de traitement et sous-traitants.

Lien vers la publication de la CNIL :
https://www.cnil.fr/fr/thematiques-prioritaires-de-controle-2022-prospection-commerciale-cloud-et-surveillance-du

DPO : QUELLE GOUVERNANCE POUR ÊTRE CONFORME AU RGPD ?

A la suite de l'ouverture de vingt-cinq procédures d'audit par l'Autorité de contrôle luxembourgeoise (la « CNPD »), deux enquêtes ont conduit la CNPD ä condamner deux organismes qui n'avaient pas pris toutes les mesures permettant au DPO d'exercer ses missions conformément aux exigences du RGPD. Comme chaque mois, Alexandre Fiévée tente d'apporter des réponses aux questions que tout le monde se pose en matière de protection des données personnelles, en nous appuyant sur les décisions rendues par les autorités nationales de contrôle au niveau européen.

Le délégué *est* chargé *de* piloter la conformité au règlement européen *sur la* protection *des* données au sein *de* l'organisme qui l'a désigné, s'agissant *de* l'ensemble *des* traitements *mis* en œuvre par cet *organisme »* [1], explique la Cnil. « Pour *garantir l'effectivité de ses missions,* ajoute-t-elle, le délégué doit : disposer de *qualités* profes*sionnelles et de* connaissances *spécifiques ;* bénéficier de *moyens* matériels *et* organisationnels, *des ressources* et *du* positionnement lui permettant *d'exercer* efficacement *ses* missions ». La désignation du DPO est obligatoire dans certains cas énumérés dans le RGPD. Dans les autres cas, sa désignation reste fortement recommandée, le DPO étant considéré comme le « chef *d'orchestre* » de la mise en conformité au RGPD de l'organisme dont il dépend. Le DPO est principalement en charge : (i) d'informer et de conseiller le responsable du traitement ou le sous-traitant, ainsi que leurs employés ; (ii) de contrôler le respect de la réglementation en matière de protection des données ; (iii) de conseiller l'organisme sur la réalisation d'uneanalyse d'impact relative à la protection des données et d'en vérifier l'exécution ; (iv) de coopérer avec l'autorité de contrôle ; (v) et d'être le point de contact des personnes concernées.

Le DPO doit bénéficier du soutien de l'organisme qui l'a désigné. Ce dernier doit donc : (i) s'assurer de l'implication du DPO dans toutes les questions relatives à la protection des données ; (ii) lui fournir les ressources nécessaires à la réalisation de ses missions ; (iii) lui permettre d'agir de manière indé- pendante ; (iv) lui faciliter l'accès aux données et aux opérations de traitement ; (v) et veiller à l'absence de conflit d'intérêts.

Les affaires[2]

La CNPD, l'autorité de contrôle luxembourgeoise, a lancé en 2018 une campagne d'enquête thématique sur la fonction du DPD, qui s'est traduite par l'ouverture de 25 procédures d'audit concernant tant le secteur privé que le secteur public. Deux enquêtes ont été ouvertes, l'une concernant un établissement de crédit, l'autre une entreprise de transport. Plusieurs griefs ont été relevés.

Premier grief : le défaut de publication des coordonnées du DPD. « *Le DPD doit* pouvoir *être* contacté aisément et directement via un *canal* de *communication* adapté aux personnes concernés »[3], indique la CNPD. Or les coordonnées du DPD ne figuraient sur aucun support et n'étaient notamment pas mentionnées sur le site internet de l'organisme contrôlé.

Autre grief : le manquement à l'obligation d'associer le DPD à toutes les questions relatives à la protection des données.

Il est normal de s'attendre, selon le chef d'enquête, à ce que le DPD participe « de manière formalisée et sur la base d'une fréquence définie, au Comité de Direction, aux comités de nouveaux produits, aux comités de sécurité ou tout autre comité jugé utile dans le cadre de la protection des données »[4]. Le fait que la présence du DPD à ces comités ne reposait sur aucune règle ni sur une fréquence définie constitue, selon la CNPD, un manquement.

L'autorité de contrôle a constaté un autre manquement concernant l'obligation de garantir l'autonomie du DPD, celui-ci n'étant pas rattaché, dans les faits, au niveau le plus élevé de la direction comme l'impose pourtant le RGPD. « *En effet, le DPD est rattaché à une personne du département (...) qui est elle-même rattachée à une personne du département (...) qui est elle-même rattachée au Chief Compliance Offices souligne le chef d'enquête. Bien que le DPD puisse intervenir de manière ad hoc ou Comité exécutif et au Comité de contrôle interne à se demande et à tout moment, le rattachement hiérarchique à la Direction et donc l'accès à cette dernière ne sont pas directs et permanents.* »[5]

Il était également reproché aux deux sociétés un manquement relatif à la mission de contrôle du DPD, aucun plan de contrôle n'ayant été formalisé. Selon la CNPD, « la mission de contrôle effectuée par le DPD auprès du contrôlé devrait être suffisamment formalisée, par exemple par un plan de contrôle en matière de protection des données, afin de pouvoir démontrer que le DPD puisse effectuer sa mission de contrôle au respect du RGPD de manière adéquate »[6].

Compte tenu de ces différents manquements, la CNPD a infligé aux deux sociétés une amende administrative d'un montant de 15 . 400 euros pour la première[7] et d'un montant de 18. 700 euros pour la seconde[8].

Quelles recommandations ?

Depuis l'entrée en vigueur du RGPD, tout organisme doit mettre en œuvre les mécanismes et les procédures internes permettant de démontrer le respect des règles relatives à la protection des données. La fonction de DPO n'échappe pas à la règle. Le RGPD définit les compétences attendues d'un DPO et les moyens qu'il doit disposer pour exercer ses missions. Le règlement insiste par ailleurs sur la capacité du DPO d'agir en toute indépendance. A l'aune de ces deux décisions, tout organisme devrait organiser un audit de la fonction du DPO, et ce afin de vérifier que la gouvernance « *RGPD* » est conforme aux exigences règlementaires.

Alexandre FIÉVÉE

Notes :

[1] https://www.cnil.fr/fr/devenir-delegue-la-protection-des-donnees
[2] CNPD, délibération n° 40FR/2021 du 27 octobre 2021 ; CNPD, délibération n° 41FR/2021 du 27 octobre 2021.
[3] CNPD, délibération n° 41FR/2021 du 27 octobre 2021.
[4] CNPD,déliberation n° 40FR/2021 du 27 octobre 2021 ; CNPD,déliberation n° 41FR/2021 du 27 octobre 2021.
[5] CNPD,déliberation n° 41FR/2021 du 27 octobre 2021.
[6] CNPD,déliberation n° 40FR/2021 du 27 octobre 2021 ; CNPD,déliberation n° 41FR/2021 du 27 octobre 2021.
[7] CNPD,déliberation n° 40FR/2021 du 27 octobre 2021.
[8] CNPD,déliberation n° 41FR/2021 du 27 octobre 2021.

FACEBOOK CONDAMNÉE PAR LA CNIL A UNE AMENDE RECORD

Par une délibération en date du 31 décembre 2021, la CNIL a condamné la société Facebook Ireland Limited à une amende de 60 millions d'euros pour non-respect de la législation en matière de cookies.

Postérieurement à quatre saisines enregistrées entre octobre 2020 et mars 2021, une délégation de la CNIL a effectué le 8 avril 2021 un contrôle en ligne du site web « facebook.com ».

A la suite de ce contrôle, la CNIL a retenu un manquement à l'article 82 de la loi Informatique et Libertés.

L'autorité de contrôle a considéré que, sur le site web « facebook.com », la procédure de refus des cookies proposée aux internautes français est contre-intuitive et bien moins simple que la procédure d'acceptation des cookies.

A cet égard, la CNIL a notamment relevé qu'il fallait trois actions pour refuser les cookies, contre une pour les accepter. L'autorité de contrôle a également estimé que l'information fournie à l'internaute français pour refuser les cookies n'était pas claire l'incitant à penser qu'il n'est finalement pas possible de poursuivre sa navigation en refusant le dépôt de cookies publicitaires.

Ce faisant, la CNIL a estimé qu'il n'y avait pas de garantie d'un consentement libre de l'internaute français.

Outre l'amende salée prononcée, l'autorité de contrôle a enjoint la société Facebook Ireland Limited de se mettre en conformité dans délai de trois mois sous peine d'une astreinte de 100.000 euros par jour de retard, et a ordonné la publication de la décision.

Lien vers la décision de la CNIL :
https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000044840532

LA CNIL PRONONCE UNE SANCTION D'UN MONTANT DE 300.000 EUROS À L'ENCONTRE DE FREE MOBILE

Par une délibération en date du 28 décembre 2021, la CNIL a prononcé une amende administrative à l'encontre de la société Free mobile pour non-respect des droits des utilisateurs et de l'obligation de sécurité des données.

Entre les mois de décembre 2018 et de novembre 2019, plusieurs plaintes (19 – dont seulement 7 donneront lieu à la caractérisation de manquements) ont été adressées à la CNIL visant les conditions dans lesquelles la société Free Mobile traitait les demandes d'exercice des droits de ses utilisateurs, notamment en matière de prospection commerciale.

Après un contrôle sur pièces et un autre sur place, ce sont quatre manquements que la CNIL a retenu à l'encontre de la société Free Mobile.

Concernant d'abord les droits d'accès, la CNIL a estimé que la société Free mobile avait violé notamment les articles 12 et 15 du RGPD en ne donnant pas suite aux demandes des plaignants.

Le droit d'opposition des personnes concernées au traitement de leurs données personnelles (articles 12 et 21 du RGPD) n'a pas non plus été respecté, selon la CNIL, en ce que des demandes de désabonnement n'ont pas été traitées.

Un autre manquement a été relevé par la CNIL concernant l'obligation de traitement sécurisé des données (article 32 du RGPD).

L'autorité de contrôle a reproché à la société Free Mobile de transmettre à ses utilisateurs des mots de passes qui n'étaient « *ni à usage unique et dont le renouvellement* [n'était] *pas imposé, le rend[ant] aisément et immédiatement utilisable par un tiers qui aurait un accès indu au message qui le contient.* ». Pour la formation restreinte, ces modalités de transmission « *ne sont pas adaptées au regard du risque que ferait peser sur la personne concernée la captation de leur identifiant et de leur mot de passe par un tiers* » qui « *pourrait ainsi accéder à toutes les données à caractère personnel présentes dans le compte utilisateur* » parmi lesquelles les nom, prénom, numéro de ligne mobile, adresse postale, adresse électronique, relevé d'identité bancaire, numéro de ligne mobile…

Outre une injonction de mise en conformité, la formation restreinte de la CNIL a prononcé une amende administrative de 300.000 euros à l'encontre de la société Free Mobile.

La délibération de la CNIL est disponible ici : https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000044810599?isSuggest=true

AFFAIRE BENALLA : UNE ONG SANCTIONNÉE PAR LA CNIL BELGE

Le 27 janvier 2022, l'autorité de protection des données belge (APD) a prononcé une amende de 2.700 € à l'encontre de l'ONG EU DisinfoLab, ainsi qu'une amende de 1.200 € à l'encontre de l'un de ses chercheurs, pour collecte massive et publications de données dans le cadre d'une étude visant à identifier l'orientation politique des personnes à l'origine des tweets portant sur l'affaire Benalla.

L'ONG EU DisinfoLab, dont l'objectif est la lutte contre la désinformation, a réalisé une étude en rapport avec le débat mené sur Twitter concernant l'affaire Benalla. Dans le cadre de cette étude, l'ONG a vu sa méthodologie être remise en cause et a, afin de répondre aux critiques, pris la décision de publier les données personnelles de nombreux utilisateurs.

Saisie par de nombreuses plaintes desdits utilisateurs, lesquels dénonçaient l'utilisation de leurs données (qui étaient d'ailleurs sensibles) dans le cadre de la réalisation de l'étude et la publication de ces données en ligne, la CNIL a saisi l'autorité de protection des données belge (APD) afin qu'elle instruise les plaintes des résidents français.

Cette saisine de l'APD reposait sur la procédure de coopération instaurée par le RGPD, les responsables du traitement étant, en l'espèce, des résidents belges.

L'APD a relevé les manquements suivants :

- L'ONG EU DesinfoLab n'a pas documenté le traitement dans son registre et n'a pas réalisé d'analyse d'impact ;
- L'ONG EU DesinfoLab n'a pas pris les mesures nécessaires pour assurer la sécurité des données traitées ;
- la collecte des données et leur publication sur Twitter ne reposaient sur aucune base légale.

En conséquence de ces manquements, l'APD a prononcé une amende de 2.700 € à l'encontre de l'ONG EU DesinfoLab et une amende 1.200 € à l'encontre du chercheur ayant participé à la publication des données sur Twitter.

Lien vers la publication de la CNIL :
https://www.cnil.fr/fr/profilage-politique-lautorite-belge-de-protection-des-donnees-prononce-deux-sanctions-apres-saisine

ACTUALITE EUROPEENNE :

PANORAMA DE QUELQUES DECISIONS RENDUES PAR DES AUTORITÉS NATIONALES DE CONTRÔLE

Sécurité : sanction d'une université pour défaut de test

UODO (Pologne), 9 décembre 2021

En mai 2020, l'université de technologie de Varsovie a notifié à l'autorité de contrôle polonaise une violation de données. La notification indiquait qu'une personne inconnue et non autorisée avait téléchargé, à partir du réseau informatique de l'université, une base de données contenant les données personnelles d'environ 5000 personnes (étudiants et professeurs).

L'enquête, diligentée par l'autorité de contrôle, a révélé que la faille provenait d'une application créée 10 ans auparavant, développée par les employés de l'université, permettant aux étudiants de s'inscrire aux cours et d'obtenir des documents administratifs (dossier administratif, certificats, justificatif de paiement des frais de scolarité…). Cette application permettait également aux professeurs de télécharger des fichiers liés à leurs enseignements.

L'analyse technique de la violation a révélé qu'en janvier 2020 et avril 2020, un tiers non autorisé muni d'informations d'identification probablement volées, avait profité de la fonctionnalité de téléchargement de fichiers de l'application pour y installer des portes dérobées. Ces dernières ont permis le téléchargement, en avril 2020, des données personnelles faisant l'objet de la violation.

Rappelant qu'il est « *indispensable que le responsable du traitement, dans le cadre de la mise en œuvre des obligations découlant du [RGPD], vérifie périodiquement si les solutions techniques et organisationnelles utilisées ne comportent pas de faiblesses pouvant affecter le risque de violation des droits ou libertés des personnes concernées* », l'autorité de contrôle a constaté que l'université n'avait pas mis en œuvre les mesures techniques et organisationnelles appropriées pour assurer en permanence la confidentialité des activités de traitement.

A cet égard, elle relève que l'université n'a pas régulièrement testé, mesuré et évalué l'efficacité de ces mesures et n'a pas pris en compte les risques liés au traitement de données à caractère personnel dans l'application susmentionnée. Compte tenu de ce qui précède, l'autorité de contrôle a infligé à l'université une amende de 9.000 €.

Lien vers la décision :
https://www.uodo.gov.pl/decyzje/DKN.5130.2559.2020%2520

Sanction d'un employeur pour avoir transmis à un tiers non autorisé les données d'un salarié

AEPD (Espagne), 14 décembre 2021

Un salarié a déposé une plainte, devant l'autorité de contrôle espagnole, après avoir constaté que son employeur (une société de construction immobilière) avait adressé à son client (une entreprise publique de logements sociaux) des données personnelles le concernant, dont des données de santé (arrêt maladie pour cause de COVID).

Dans cette espèce, l'entreprise publique, reprochant au constructeur d'avoir mal respecté les affectations relatives aux ressources humaines prévues au contrat, avait engagé une procédure administrative de sanction à l'encontre de ce dernier. Pour expliquer cette situation, le constructeur invoqua l'indisponibilité de son salarié pour cause de COVID et transmit à l'entreprise publique, en guise de pièce justificative, l'arrêt maladie de son salarié.

L'autorité de contrôle a rappelé que les traitements de données de santé, en tant que catégorie spéciale de données personnelles, font l'objet d'un principe d'interdiction (art. 9 du RGPD). Si l'employeur pouvait effectivement se prévaloir de l'exception posée à l'article 9§2 du RGPD (détaillant les situations dans lesquelles le traitement de données de santé est autorisé), les principes posés à l'article 5 du RGPD auraient dû être respectés, ce qui n'a pas été le cas en l'espèce.

Selon l'autorité de contrôle, non seulement l'employeur n'a pas respecté le principe de minimisation, mais en plus il aurait dû recueillir le consentement exprès de son salarié.

Par conséquent, l'autorité de contrôle a infligé à l'employeur une amende de 50.000 €.

Lien vers la décision
https://www.aepd.es/es/documento/ps-00324-2021.pdf

Interdiction d'exiger la signature de la personne concernée qui exerce ses droits

HBDI (Hesse, Allemagne), 19 décembre 2020

La société ABIS, filiale de la Deutsche Post, exigeait que les demandes d'exercice des droits effectuées par les personnes concernées soient signées de manière manuscrite et transmises par courrier, fax, ou en pièce jointe à un courriel. Cette exigence était justifiée par la nécessité, selon ABIS, d'identifier la personne exerçant ses droits.

A la suite d'une plainte, l'autorité de contrôle de Hesse a rappelé que le RGPD n'impose aucune exigence formelle pour l'exercice des droits des personnes, et notamment « pas de signature de la personne concernée ».

Ainsi, un responsable du traitement ne peut pas obliger les personnes concernées à utiliser un moyen spécifique, tel que le fax ou la lettre recommandée, pas plus qu'il ne peut exiger de demande signée, d'autant qu'une signature n'est pas un gage pour une « identification claire de la personne concernée ».

Lien vers l'article
https://www.datenanfragen.de/blog/abis-unterschrift-dsgvo-anfragen/

Sanction d'une entreprise pour ne pas avoir supprimé les métadonnées de photographies

HBDI (Hambourg, Allemagne), 2020

Un citoyen allemand a découvert que de nombreuses coordonnées GPS d'utilisatrices d'une marketplace (proposant à la vente des sous-vêtements portés) étaient accessibles en ligne.

Alertée, l'autorité de contrôle de Hambourg a ouvert une enquête à l'encontre de l'entreprise exploitant la marketplace.

Au cours de son enquête, l'autorité de contrôle a constaté que les métadonnées des photographies de sous-vêtements n'avaient pas été « nettoyées », et qu'ainsi il était possible de déterminer l'emplacement exact où la photo avait été prise. Selon l'autorité de contrôle, 760 femmes, âgées de 18 à 50 ans, étaient concernées par cette violation de données.

L'autorité de contrôle a, dans un premier temps, rappelé qu'un responsable du traitement doit mettre en œuvre les mesures techniques et organisationnelles appropriées, en fonction des risques, et doit en outre respecter les principes de *privacy by design* et *privacy by default*.

Dans un second temps, l'autorité de contrôle a rappelé que les photos prises par des appareils photos numériques sont généralement doublées d'informations, appelées *Exhangeable Image File Format* (EXIF), qui contiennent des données telles que la localisation GPS. Ces métadonnées sont considérées comme des données personnelles, puisqu'il est « *possible d'identifier plusieurs personnes concernées avec relativement peu d'efforts* »

Selon l'autorité de contrôle, le nettoyage des données EXIF est une exigence standard pour les exploitants d'une marketplace en ligne, ce qui signifie que les images doivent être débarrassées de leurs métadonnées avant d'être publiées.
et organisationnelles.

En tirant les conclusions de l'absence de nettoyage de ces photographies par le responsable du traitement, l'autorité de contrôle a estimé que l'entreprise n'avait pas pris les mesures techniques et organisationnelles.

Lien vers le rapport d'activité
https://datenschutz-hamburg.de/assets/pdf/29._taetigkeitsbericht_datenschutz_2020.PDF

ACTUALITÉ DU CABINET

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* » (2020).
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 :
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