NON RESPECT DU RGPD : LES SANCTIONS (1/5)

Des sanctions administratives ou pénales peuvent être prononcées par la formation restrainte de la CNIL à l'égard des responsables de traitement et des sous-traitants qui ne respecteraient pas les dispositions du RGPD et qui ne se seraient pas mis en conformité après rappel à l'ordre, mise en demeure de mise en conformité d'un traitement ou demande express de satisfaction des demandes d'exercice des droits des personnes.

Les contrôles avant sanction

Sanctions prononcées à l'issue de contrôles en ligne, sur pièces ou sur place, d'auditions sur convocation et de l'instruction de plaintes reçues par la CNIL.

Un arsenal de sanctions...

La CNIL peut limiter temporairement ou définitivement un traitement, suspendre les flux de données et rendre publiques les sanctions appliquées :

Amende Art. 83	Pénal Art. 84	Autre Art. 84

Selon la nature du dysfonctionnement constaté, sa durée et sa gravité, la sanction peut aller...

jusqu'à 10 millions d'euros ou 2% du chiffre d'affaire mondial (violations de niveau 1*)

jusqu'à 20 millions d'euros ou 4% du chiffre d'affaire mondial (violations de niveau 2*)

de 15 000€ à 300 000€ d'amende

de 1 à 5 ans d'emprisonnement

Dommages et intérêts
Déficit d'image lié à la non conformité
Peines spécifiques pour les personnes morales

Legifrance. Le service public de l'accès au droit | Code pénal - Articles 226-16. à 226-24.
CNIL. (s. d.-a). Les sanctions pénales. Consulté à l'adresse https://www.cnil.fr/fr/les-sanctions-penales
CNIL. (s. d.-a). Comment se passe un contrôle de la CNIL ? Consulté à l'adresse https://www.cnil.fr/fr/comment-se-passe-un-controle-de-la-cnil

Carole Blancot (Désignation CNIL : N° DPO- 37620)
carole.blancot@spotpink.com

RGPD : AMENDES ADMINISTRATIVES (2/5)

Selon la nature du dysfonctionnement constaté, sa durée et sa gravité, le montant de l'amende peut aller jusqu'à 10 millions d'euros ou 2% du chiffre d'affaire mondial, pour ce qui concerne les sujets suivants :

Les violations de niveau 1

1. Consentement des enfants
2. Obligations générales du responsable de traitement et du sous-traitant
3. Certification
4. Codes de conduite
5. Traitement ne nécessitant pas d'identification

Selon la nature du dysfonctionnement constaté, sa durée et sa gravité, le montant de l'amende peut aller jusqu'à 20 millions d'euros ou 4% du chiffre d'affaire mondial, pour ce qui concerne les sujets suivants :

Les violations de niveau 2

6. Consentement
7. Licéité
8. Principes de base d'un traitement
9. Catégories particulières de données
10. Droits des personnes concernées
11. Transferts hors UE
12. Obligations découlant du droit des états membres (Art. 85 à 91)
13. Non-respect d'une injonction ou entrave à l'action de la CNIL (enquête)

Carole Blancot (Désignation CNIL : N° DPO- 37620)
carole.blancot@spotpink.com

RGPD : SANCTIONS PÉNALES (3/5)

L'article 84 du RGPD dispose que les états membres peuvent mettre en place d'autres sanctions pour réprimander les violations qui ne font pas l'objet d'amendes administratives au sens de l'article 83 du RGPD.
Ces sanctions sont effectives, proportionnées et dissuasives.

5 ans d'emprisonnement et 300 000€ d'amende :

Défaut de formalité préalable (Art. 226-16 du Code pénal)

Traitements réalisés sur des données incluant le numéro de sécurité sociale (Art. 226-16-1-A du Code pénal)

Non respect d'obligations générales incombant au responsable de traitement et au sous-traitant (Art. 226-17 du Code pénal)

Défaut de notification d'une violation (Art. 226-17-1 du Code pénal)

Collecte interdite (Art. 226-18 du Code pénal)

Non effectivité du droit d'opposition (Art. 226-18-1 du Code pénal)

Défaut de consentement pour le traitement de certaines données sensibles (Art. 226-19 du Code pénal)

Traitements illicites de données de santé (Art. 226-19-1 du Code pénal)

Durées de conservation excessives (Art. 226-20 du Code pénal)

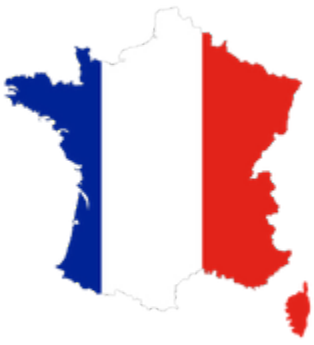
Détournement de la finalité des données personnelles lors d'un traitement de données (Art. 226-21 du Code pénal)

Transfert de données à des tiers non autorisés (Art. 226-22 du Code pénal)

Transfert de données hors UE sans garanties de protection suffisantes (Art. 226-22-1 du Code pénal)

Entrave à l'action de la CNIL (Art. 226-22-2 du Code pénal) → **Un an d'emprisonnement et 15 000€ d'amende**

Carole Blancot (Désignation CNIL : N° DPO- 37620)
carole.blancot@spotpink.com



RGPD : SANCTIONS PRONONCÉES (4/5)

21/01/2019 - GOOGLE LLC

50 millions d'euros d'amende pour non-respect de principes essentiels du RGPD

C'est la première fois que la CNIL fait application des nouveaux plafonds de sanction prévus par le RGPD. Le montant retenu ainsi que la publicité de l'amende, se justifient par la gravité des manquements constatés qui concernent des principes essentiels du RGPD : la transparence, l'information et le consentement (manquement à l'obligation de disposer d'une base légale pour les traitements de personnalisation de la publicité).

La société GOOGLE LLC a fait appel de la décision de la CNIL devant le Conseil d'Etat.

25/07/2019 - ACTIVE ASSURANCES

Amende de 180 000€ pour défaut de sécurité et violation de données

Après un signalement et un contrôle en ligne, la formation restreinte de la CNIL a prononcé une amende administrative de 180 000€ à l'encontre de la société, Active Assurances pour un défaut de sécurité des données personnelles. L'affaire remonte à juin 2018 lorsqu'un client d'Active Assurances a signalé à la commission avoir été capable, à partir de son compte, d'accéder aux données personnelles d'autres clients.

18/06/2019 - UNIONTRAD COMPANY

Amende de 20 000€ pour vidéosurveillance excessive des salariés

Le dispositif de vidéosurveillance déployé par la société UNIONTRAD COMPANY plaçait ses salariés sous surveillance constante. A l'issue d'un contrôle sur place, la CNIL a prononcé une sanction de 20 000€ et a également prononcé une injonction afin que la société prenne des mesures pour assurer la traçabilité des accès à la messagerie professionnelle partagée.

06/06/2019 - SERGIC

Amende de 400 000€ pour atteinte à la sécurité des données et non-respect des durées de conservation

Un contrôle en ligne a eu lieu après réception d'une plainte formulée auprès de la CNIL par un utilisateur du site édité par la société. A l'issue d'un contrôle sur place la formation restreinte a prononcé une amende de 400 000 euros, et décidé de rendre publique sa sanction au regard de la gravité du manquement, du manque de diligence de la société dans la correction de la vulnérabilité et du fait que les documents accessibles révélaient des aspects très intimes de la vie des personnes.

- 27/12/2018 : BOUYGUES TELECOM - 250 000€ d'amende pour manquement à la sécurité des données clients.
- 20/12/2018 : UBER - 400 000€ d'amende pour atteinte à la sécurité des données des utilisateurs.
- 20/09/2018 : ASSISTANCE CENTRE d'APPELS - 10 000€ d'amende pour un système biométrique au travail illégal (à des fins de contrôle des horaires des salariés).

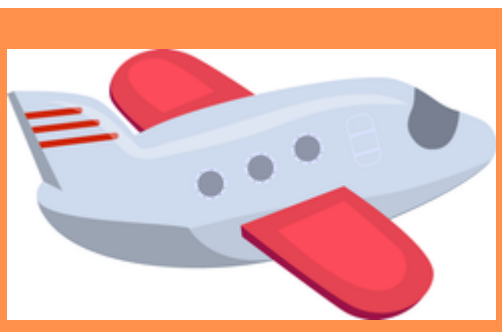
SOURCES

CNIL. (s. d.-a). Les sanctions prononcées par la CNIL. Consulté à l'adresse https://www.cnil.fr/fr/les-sanctions-prononcees-par-la-cnil

Lettre AFCDP n°152 - L'Actualité des données personnelles - Septembre 2019

Carole Blancot (Désignation CNIL : N° DPO- 37620)
carole.blancot@spotpink.com

RGPD : SANCTIONS (5/5)



BRITISH AIRWAYS 204 MILLIONS D'EUROS

Violation de données

429 000 clients avaient été concernés par deux vols successifs des données bancaires communiquées sur le site de la compagnie aérienne en 2018.

BERLIN : PLUSIEURS MILLIONS D'EUROS

Non respect du règlement général européen sur la protection des données (DSGVO).

L'autorité de contrôle du Land de Berlin annonce qu'elle est sur le point d'infliger une amende de plusieurs millions d'euros pour violation du RGPD, mais sans dévoiler l'identité du responsable de traitement concerné.

HÔPITAL HAGA DE LA HAYE

460 000€ d'amende

L'hôpital Haga de La Haye (Pays-Bas) a été sanctionné par l'autorité de contrôle néerlandaise pour défaut de sécurité des dossiers patients. Le dossier médical d'une « star » d'une série télévisée avait été consulté par nombre de personnels n'ayant aucune légitimité à y accéder. Si des mesures suffisantes n'ont pas mises en place début octobre 2019, une sanction de 100 000€ supplémentaires sera infligée toutes les deux semaines (dans la limite de 300 000€).

RECONNAISSANCE FACIALE DANS UNE ÉCOLE SUÉDOISE

200 000 couronnes

Le DPA suédois (Datainspektionen) a infligé sa première sanction au titre du RGPD (environ 25 000€) au lycée de la ville de Skellefteå qui, à titre expérimental, vérifiait la présence des élèves dans l'établissement grâce à une caméra et à un logiciel de reconnaissance faciale. L'autorité a rejeté le consentement comme fondement et affirmé que le contrôle de la présence pouvait être effectué par d'autres moyens moins intrusifs.

QUEBEC : 2 PERSONNES ARRÊTÉES

Violation de données

Deux personnes ont été arrêtées après une violation de données au Québec qui a impacté 23 000 salariés et anciens salariés du Revenu Québec.

L'une des deux personnes est un salarié de l'administration fiscale qui a transféré les données (numéro de sécurité sociale, date de naissance et salaire) à l'extérieur de l'organisation.

SOURCE

Lettre AFCDP n°152 - L'Actualité des données personnelles - Septembre 2019

Carole Blancot (Désignation CNIL : N° DPO- 37620)
carole.blancot@spotpink.com