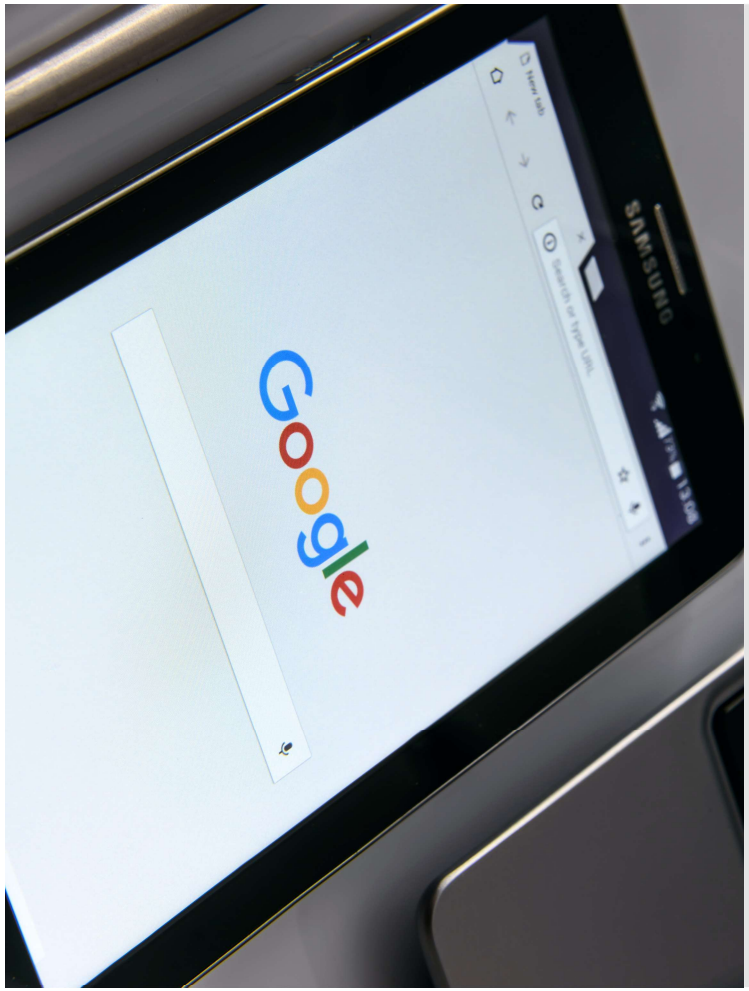
RGPD
Exemples d'application

RGPD

Exemples d'application

Google

- 50 millions d'euros d'amende ont été infligés par la CNIL à Google en 2019
- cette décision fait suite à 2 plaintes déposées par l'association *None Of Your Business* et la *Quadrature du Net*
- le Bureau Européen des Unions de Consommateurs a dénoncé des pratiques trompeuses de la part de Google au niveau de la fonction localisation



RGPD

Exemples d'application

Google

- Google est en effet capable de suivre la position d'un utilisateur même lorsque que ce paramètre est désactivé
- en fait, il existe un 2ème paramètre à désactiver pour réellement empêcher le suivi GPS
- durant son enquête la CNIL a tout simplement analysé " *le parcours d'un utilisateur et les documents auxquels il peut avoir accès en créant un compte Google lors de la configuration de son équipement mobile sous Android* "
- pour voir et modifier les 2 paramètres, l'utilisateur doit passer par plusieurs étapes et ainsi réaliser de nombreuses actions peu intuitives et mal documentées
- c'est ce manque d'information qui a été condamné

RGPD

Exemples d'application

Google

La CNIL explique que :

- " *les utilisateurs ne sont pas en mesure de comprendre l'ampleur des traitements mis en place par Google* "
- " *le consentement n'est pas valablement recueilli ni suffisamment éclairé* "

RGPD

Exemples d'application

Google

- *" les manquements constatés privent les utilisateurs de garanties fondamentales concernant des traitements pouvant révéler des pans entiers de leur vie privée "*
- *" cela repose sur un volume considérable de données, une grande variété de services et des possibilités de combinaisons de données quasi-illimitées "*

RGPD

Exemples d'application

Marriott

- la chaîne d'hôtels Marriott a été condamnée par l'ICO (Information Commissioner's Office) à payer une amende de 100 millions de livres sterling (110 millions d'euros), pour ne pas avoir su empêcher le vol des données de ses clients sur ses plateformes web et mobiles

RGPD

Exemples d'application

Marriott

- 383 millions de clients ont été touchés *(source : Marriott)*
- les données piratées concernaient notamment des cartes de crédit, des numéros de passeports et des identités
- le problème est apparu en 2014 lorsque les systèmes du groupe Starwood, racheté par Marriott en 2016, ont été compromis par une cyberattaque

RGPD

Exemples d'application

Marriott

- Marriott n'a pas pris les dispositions nécessaires au moment de ce rachat
- l'entreprise aurait du faire preuve de vigilance et s'assurer que les systèmes informatiques de Starwood étaient fiables
- le RGPD indique clairement que les organisations doivent être responsables des données personnelles qu'elles détiennent

RGPD

Exemples d'application

British Airways

- en 2018, British Airways a fait l'objet d'une cyberattaque par laquelle les pirates ont pu avoir accès aux données personnelles de 429 612 clients et employés, incluant noms, adresses et numéros de cartes de paiement
- du 22 juin au 5 septembre 2018, les fraudeurs ont mené plusieurs attaques leur permettant d'accéder à des fichiers non cryptés contenant les données des cartes de paiement des clients
- British Airways a été avertie de cette attaque par un tiers
- elle a notifié l'ICO le 6 septembre 2018 comme l'exige le RGPD
- elle a écopé d'une amende de 204 millions d'euros

RGPD

Exemples d'application

British Airways

- pour motiver sa sanction, l'autorité de contrôle retient que la compagnie n'a pas réussi à empêcher l'attaque, ni à la détecter
- ceci aurait pu être réalisé par des mesures de sécurité informatique basiques
- elle ajoute que ces mesures n'auraient entraîné aucun coût excessif ou barrières techniques
- au regard du nombre de personnes touchées et de l'importance du préjudice financier encouru, l'ICO estime qu'il s'agit d'un grave manquement aux principes de sécurité et de responsabilité du RGPD

RGPD

Exemples d'application

Médecine libérale

- 18 décembre 2020 : la CNIL inflige des amendes de 3 000 et 6 000 euros à deux médecins libéraux
- il leur est reproché d'avoir " *insuffisamment protégé les données personnelles de leurs patients* "
- ils ont de plus oublié de notifier une violation de données : " *des milliers d'images médicales hébergées sur des serveurs étaient librement accessibles sur Internet* "

RGPD

Exemples d'application

Médecine libérale

- les 2 médecins ont reconnu que " *les violations de données avaient pour origine un mauvais choix de configuration de leur box Internet ainsi qu'un mauvais paramétrage de leur logiciel d'imagerie médicale* "

RGPD

Exemples d'application

Médecine libérale

- ces images " *n'étaient pas systématiquement chiffrées* "
- " *les manquements constatés privent les utilisateurs de garanties fondamentales concernant des traitements pouvant révéler des pans entiers de leur vie privée* "

RGPD

Exemples d'application

Médecine libérale

Deux manquements sont notifiés :

- manquement à l'obligation de sécurité des données (article 32 du RGPD)
- manquement à l'obligation de notifier les violations de données (article 33 du RGPD)

RGPD

Exemples d'application

Médecine libérale

- *" en effet, les deux médecins n'ont pas effectué ces notifications obligatoires auxquelles ils auraient dû procéder après avoir appris que les images médicales de leurs patients étaient librement accessibles sur Internet "*
- les délibérations ont été rendues disponibles sur le site de l'autorité, mais les noms des deux professionnels de santé n'ont pas été révélés
- la CNIL a *" souhaité assurer la publicité de ces décisions pour alerter les professionnels de la santé sur leurs obligations et la nécessité de renforcer leur vigilance sur les mesures de sécurité apportées aux données personnelles qu'ils traitent "*

RGPD

Exemples d'application

Autres sanctions

- Prospection commerciale et droits des personnes : sanction de 600 000 euros à l'encontre d'EDF (*29 novembre 2022) : https://www.cnil.fr/fr/prospection-commerciale-et-droits-des-personnes-sanction-de-600-000-euros-lencontre-dedf*
- Sanction de 800 000 euros à l'encontre de la société DISCORD INC. (*17 novembre 2022) : https://www.cnil.fr/fr/sanction-de-800-000-euros-lencontre-de-la-societe-discord-inc*
- Fuite de données de santé : sanction de 1,5 million d'euros à l'encontre de la société DEDALUS BIOLOGIE (*21 avril 2022)* : *https://www.cnil.fr/fr/fuite-de-donnees-de-sante-sanction-de-15-million-deuros-lencontre-de-la-societe-dedalus-biologie*

RGPD

Exemples d'application

Autres sanctions

- Géolocalisation de véhicules de location : sanction de 175 000 euros à l'encontre d'UBEEQO INTERNATIONAL (*21 juillet 2022) : https://www.cnil.fr/fr/geolocalisation-de-vehicules-de-location-sanction-de-175-000-euros-lencontre-dubeeqo-international*
- Violation de données : sanction de 180 000 euros à l'encontre de la société SLIMPAY (*30 décembre 2021) : https://www.cnil.fr/fr/violation-de-donnees-sanction-de-180-000-euros-lencontre-de-la-societe-slimpay*
- Sanction de 500 000 euros à l'encontre de la société BRICO PRIVÉ (*17 juin 2021) : https://www.cnil.fr/fr/sanction-de-500-000-euros-lencontre-de-la-societe-brico-prive*