Amphi de droit

- Support moodle

La protection des données personnelles

La loi informatique et liberté et Le RGPD et la loi informatique et liberté (règlement européen) sont les 2 textes qui règlementent la gestion des **données personnelles** :

Des obligations pour les organisations, entreprises, associations ou collectivités publiques.

QU'EST-CE QU'UNE DONNÉE PERSONNELLE ?

Il s'agit de toute information relative à une personne physique identifiée ou identifiable, directement ou indirectement, par référence à un numéro d'identification (ex. : n° de sécurité sociale) ou à un ou plusieurs éléments qui lui sont propres (ex. : nom et prénom, date de naissance, éléments biométriques, empreinte digitale, ADN...).

LE RÈGLEMENT EUROPÉEN

Le règlement général sur la protection des données (RGPD) constitue le texte de référence en la matière au sein de l'Union européenne. Entré en application le 25 mai 2018, il donne plus de contrôle aux personnes sur leurs données, tout en offrant un cadre unifié et simplifié aux entreprises.

Depuis 2018, le RGPD a permis de :

1. Renforcer les droits des personnes, notamment grâce au droit à la portabilité des données personnelles et des dispositions propres aux personnes mineures.
2. Responsabiliser les acteurs traitant des données (responsables de traitement et sous-traitants).
3. Crédibiliser la régulation grâce à une coopération étroite entre les autorités de protection des données européennes et des pouvoirs de sanction renforcés.

Pour les professionnels, un renforcement des obligations:

Une responsabilisation des acteurs

Les administrations, sociétés et associations traitant des données personnelles, mais aussi leurs prestataires et sous-traitants, sont aujourd'hui pleinement responsables de la protection des données qu'ils traitent. Il leur appartient d'assurer la conformité au RGPD tout au long du cycle de vie de leurs traitements de données personnelles et d'être en mesure de la démontrer.

Les outils de la conformité

D'un point de vue opérationnel, la conformité au règlement européen repose sur différents outils parmi lesquels :

- le registre des traitements RT et la documentation interne ;
- la cybersécurité et la notification de certains incidents ;
- les analyses d'impact sur la protection des données (AIPD) pour les traitements pouvant être sensibles.

Le DPO (délégué à la protection des données)

La mise en œuvre de ces outils implique, au préalable, la désignation d'un pilote interne : le délégué à la protection des données, dit DPO, véritable chef d'orchestre de la protection des données personnelles au sein de l'organisme.

Pour les particuliers, un renforcement des droits :

Le RGPD a renforcé la maîtrise par l'individu de ses données. Il s'applique **dès lors qu'une personne en Europe est substantiellement affectée** par un traitement de données. Les acteurs mondiaux sont donc soumis au droit européen lorsqu'ils offrent un produit ou un service à des personnes en Europe, même à distance. Ce critère, dit du « ciblage », constitue une évolution profonde : désormais, la territorialité du droit européen de la protection des données se construit autour de la personne, et non plus seulement autour du territoire d'implantation des entreprises.

Le **RGPD** et la nouvelle loi du 20 juin 2018 reconnaissent aux personnes :

- un droit à une information plus claire et accessible ;
- une protection renforcée des enfants avec un recueil du consentement auprès des parents d'enfants de moins de 15 ans ;
- un droit à la portabilité qui permet de récupérer ses données sous une forme aisément réutilisable et de les transférer ensuite à un tiers ;
- le droit à réparation d'un dommage matériel ou moral, notamment dans le cadre d'actions collectives.

Le droit élémentaire d'information est accompagné dispositions complémentaires

QUELS SONT VOS DROITS ?

Le droit d'accès

Vous pouvez demander directement au responsable d'un fichier s'il détient des informations sur vous, et demander à ce que l'on vous communique l'intégralité de ces données.

Le droit de rectification

Vous pouvez demander la rectification des informations inexactes vous concernant. Le droit de rectification complète le droit d'accès.

Le droit à la portabilité

Vous pouvez récupérer une partie de vos données dans un format lisible par une machine. Libre à vous de stocker ailleurs ces données portables ou de les transmettre d'un service à un autre.

Le droit d'opposition

Vous pouvez vous opposer, pour des motifs légitimes, à figurer dans un fichier. Vous pouvez également vous opposer à ce que les données vous concernant soient diffusées, transmises ou conservées.

Le droit au déréférencement

Vous pouvez saisir les moteurs de recherche de demandes de déréférencement d'une page web associée à vos nom et prénom.

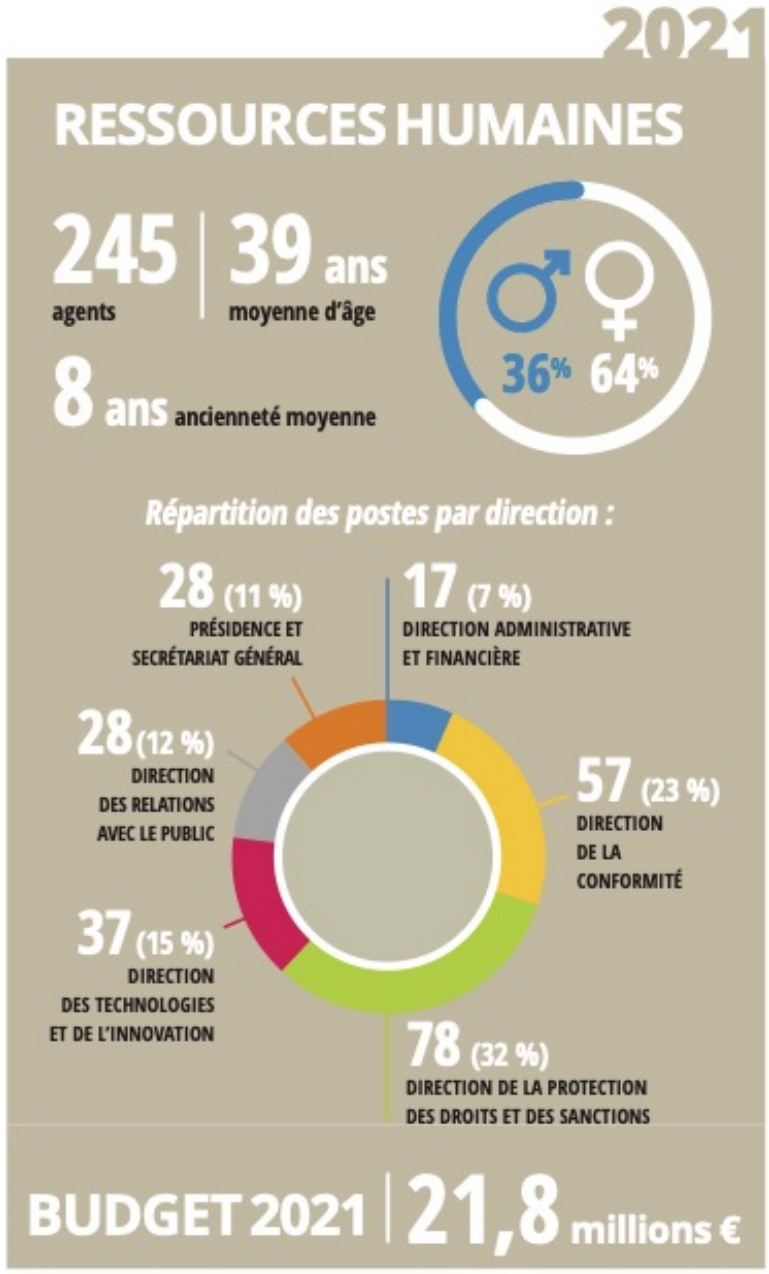
Le droit d'accès aux fichiers de police, de gendarmerie, de renseignement, FICOBA

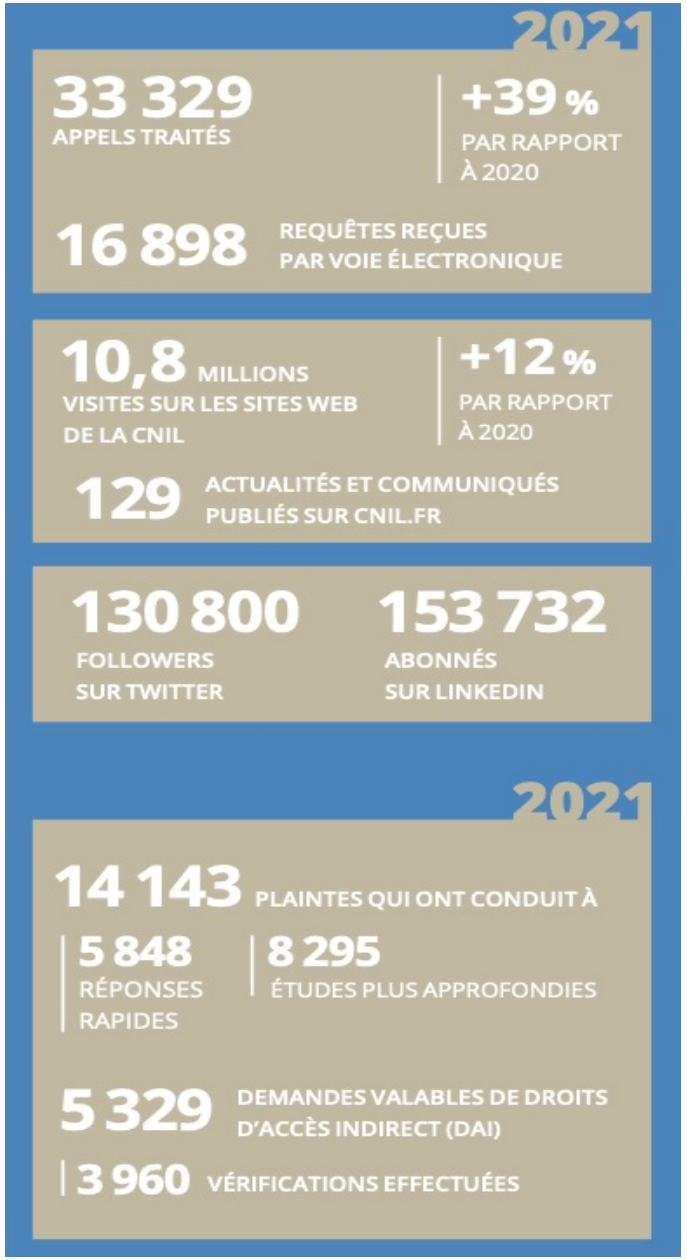
Il s'effectue directement auprès des administrations gestionnaires pour la plupart de ces fichiers. Si elles vous opposent un refus ou ne vous répondent pas dans un délai de 2 mois, vous pouvez vous adresser à la CNIL.

- Le RGPD et la loi informatique et libertés prévoient des sanctions :

- Le volet « pénal » de la loi prévoit les infractions et les sanctions
- 5 ans et 300 000 Euros
- Le RGPD ne prévoit pas encore d'échelle de sanctions (cela devrait venir) même si des sanctions en % du chiffre d'affaires mondial peuvent s'appliquer !

La CNIL : le gendarme des données personnelles





Conseiller et règlementer

L'activité de conseil et de réglementation de la CNIL est variée : avis sur des projets de texte concernant la protection des données personnelles ou créant de nouveaux fichiers, conseils, participation à des auditions parlementaires.

Dans le cadre de cette activité, la CNIL veille à la recherche de solutions permettant aux organismes publics et privés de poursuivre leurs objectifs légitimes dans le strict respect des droits et libertés des citoyens.

Le bac à sable d'accompagnement renforcé de la CNIL

La CNIL a décidé, en 2021, de compléter ses outils d'appui à l'innovation par la mise en place d'un « bac à sable », dans une logique de régulation souple et ouverte sur des problématiques émergentes. Ce dispositif fournit aux projets sélectionnés un accompagnement renforcé de la CNIL en apportant des réponses pragmatiques et de la sécurité juridique. Après un premier « bac à sable » consacré aux données de santé, l'édition 2022 est dédiée aux outils numériques dans le domaine de l'éducation.

Accompagner la conformité

À l'heure du RGPD, la conformité représente un indicateur de bonne gouvernance, répondant à l'enjeu de réputation, de confiance et un avantage concurrentiel pour les entreprises.

Afin d'aider les organismes privés et publics, la CNIL propose une boîte à outils complète et adaptée en fonction de leur taille et de leurs besoins parmi lesquels :

- des guides pratiques ;
- des pages dédiées pour de nombreux acteurs et secteurs d'activité, comme la santé ou les collectivités territoriales ;
- un modèle de registre simplifié ;
- des exemples de mentions d'information ;
- un téléservice de désignation du délégué à la protection des données ;
- un téléservice de notification des violations de données personnelles ;
- un logiciel pour mener une analyse d'impact sur la protection des données (AIPD) ;
- mais également des permanences juridiques et réponses aux demandes de conseils qui lui sont adressées.

Contrôler

Le contrôle constitue un moyen privilégié d'intervention auprès des responsables de traitement et de leurs sous-traitants. Il permet à la CNIL de vérifier notamment sur place la mise en œuvre concrète du RGPD et de la loi. Le programme des contrôles est élaboré en fonction des plaintes reçues, des thèmes d'actualité et des grandes problématiques (actualité, nouvelles technologies) dont la CNIL est saisie.

L'origine des procédures formelles de contrôle en 2021 :

- 31 % s'inscrivent dans le cadre de l'instruction de plaintes ou de signalements
- 22 % sont effectués à l'initiative de la CNIL, notamment au vu de l'actualité
- 37 % résultent des thématiques prioritaires annuelles décidées par la CNIL
- 8 % sont liés aux contrôles mis en œuvre dans le cadre de la lutte contre la COVID-19
- 2 % sont réalisés dans le cadre des suites de mises en demeure ou de procédures de sanction

Sanctionner et mettre en demeure

À l'issue de contrôles ou de plaintes, en cas de méconnaissance de la réglementation par les organismes, la CNIL peut notamment :

- prononcer un avertissement ;
- mettre en demeure l'organisme ;
- limiter temporairement ou définitivement un traitement ;
- suspendre les flux de données ;
- ordonner de satisfaire aux demandes d'exercice des droits des personnes ;
- ordonner la rectification, la limitation ou l'effacement des données ;
- prononcer une amende administrative.

2021

135 MISES EN DEMEURE DONT 2 PUBLIQUES ET 3 ADOPTÉES EN COOPÉRATION AVEC D'AUTRES CNIL EUROPÉENNES

45 RAPPELS À L'ORDRE PRONONCÉS PAR LA PRÉSIDENTE DE LA CNIL

18 SANCTIONS
DONT **15** AMENDES
POUR UN MONTANT CUMULÉ
DE **214 106 000 €**

17 PROJETS DE SANCTIONS EUROPÉENS EXAMINÉS PAR LA CNIL

RENTRÉE SCOLAIRE : CE QUE LES ÉTABLISSEMENTS SCOLAIRES ET PÉRISCOLAIRES PEUVENT VOUS DEMANDER

Publié le 28/09/2020

DÉPLOIEMENT DE CAMÉRAS « AUGMENTÉES » DANS LES ESPACES PUBLICS : LA CNIL PUBLIE SA POSITION

Publié le 19/07/2022

PRIVACY RESEARCH DAY : RETROUVEZ L'ÉVÈNEMENT EN VIDÉO

Publié le 30/06/2022

#Etablissements d'enseignement

RENTRÉE SCOLAIRE : CE QUE LES ÉTABLISSEMENTS SCOLAIRES ET PÉRISCOLAIRES PEUVENT VOUS DEMANDER

À l'occasion de la rentrée, les parents doivent fournir de nombreuses informations pour l'école, la crèche, la cantine, le transport scolaire ou les activités ...

Actualités

PRENEZ DATE : AIR2022, LE LUNDI 7 NOVEMBRE DE 14 H À 18 H À LA CNIL ET SUR LES RÉSEAUX SOCIAUX

Publié le 10/08/2022

LES CNIL EUROPÉENNES ADOPTENT UN AVIS SUR L'ESPACE EUROPÉEN DES DONNÉES DE SANTÉ ET RENFORCENT LEUR COOPÉRATION SUR LES CAS STRATÉGIQUES

Publié le 01/08/2022

« LA VIE DE LA LOI » : LE NOUVEL OUTIL DE LA CNIL POUR SUIVRE L'ÉVOLUTION DES TEXTES FRANÇAIS

Publié le 18/07/2022

STRATÉGIE EUROPÉENNE POUR LA DONNÉE : LA CNIL ET SES HOMOLOGUES SE PRONONCENT SUR LE DATA GOVERNANCE ACT ET LE DATA ACT

Publié le 13/07/2022

Communiqués

Prospection commerciale et droits des personnes : sanction de 600 000 euros à l'encontre d'ACCOR

Publié le 17/08/2022

Cookies : clôture de l'injonction prononcée à l'encontre de FACEBOOK

Publié le 28/07/2022

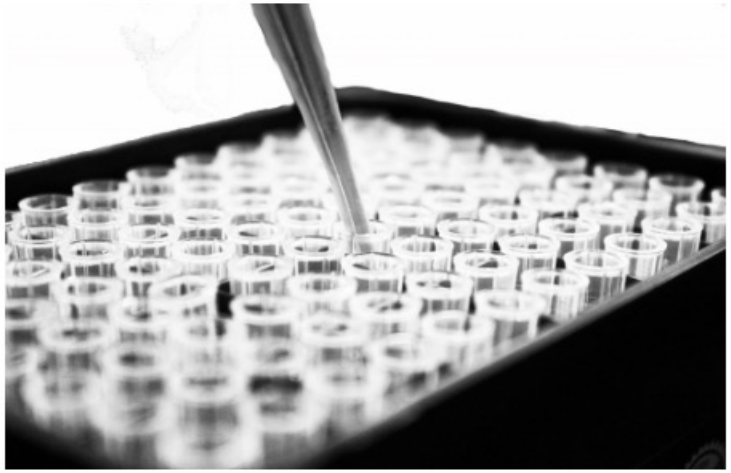
Contrôle de l'âge sur les sites web : la CNIL invite à développer des solutions plus efficaces et respectueuses de la vie privée

Publié le 26/07/2022

Géolocalisation de véhicules de location : sanction de 175 000 euros à l'encontre d'UBEEQO INTERNATIONAL

Publié le 21/07/2022

Fuite de données de santé : sanction de 1,5 million d'euros à l'encontre de la société DEDALUS BIOLOGIE



Dans sa décision du 15 avril 2022, la CNIL sanctionne la société DEDALUS BIOLOGIE à hauteur de 1,5 million d'euros en raison de défauts de sécurité ayant conduit à la fuite de données médicales de 500 000 personnes.

En février 2021, une fuite de donnée concernant près de 500 000 personnes a été révélée. Les nom, prénom, numéro de sécurité sociale, nom du médecin, date d'examen et surtout des informations médicales (VIH, cancers, maladies génétiques, grossesses, traitements médicamenteux suivis par le patient, ou encore des données génétiques) de ces personnes ont ainsi été diffusés sur internet.

La CNIL a donc effectué des contrôles auprès de la société DEDALUS BIOLOGIE qui commercialise des solutions logicielles pour des laboratoires d'analyse médicale. Elle a constaté que cette dernière avait manqué à plusieurs obligations prévues par le RGPD, en particulier à l'obligation d'assurer la sécurité des données personnelles.

La CNIL relève ainsi un manquement à l'obligation pour le sous-traitant de respecter les instructions du responsable de traitement (art. 29 RGPD) puisque les données migrées entre le laboratoire et le logiciel étaient plus importantes que prévues.

La CNIL constate également un manquement à l'obligation d'assurer la sécurité des données personnelles (art. 32 RGPD) du fait des nombreux manquements techniques et organisationnels en matière de sécurité de la société DEDALUS BIOLOGIE (absence de chiffrement, d'effacement automatique, de procédure spécifique de migration…).

Enfin, la CNIL relève un manquement à l'obligation d'encadrer par un acte juridique formalisé les traitements effectués pour le compte du responsable de traitement (art. 28 RGPD) puisque les conditions générales de vente de la société DEDALUS BIOLOGIE et les contrats de maintenance transmis ne contiennent pas les mentions prévues par l'article 28-3 du RGPD.

Ainsi, la formation restreinte de la CNIL a prononcé une amende de 1,5 million d'euros. Ce montant a été décidé au regard de la gravité des manquements retenus et en prenant en compte le chiffre d'affaires de la société DEDALUS BIOLOGIE.

Pourquoi TotalEnergies est sanctionné d'une amende d'un million d'euros par la Cnil

La Cnil a infligé une sanction d'un million d'euros à TotalEnergies. En cause : ses pratiques de prospection commerciale, qui ont manqué à deux règlements, dont le RGPD. Un sujet sur lequel le gendarme de la protection des données personnelles a décidé de concentrer ses efforts.

Un million d'euros pour TotalEnergies et une mauvaise publicité sur le site de la CNIL : c'est la sanction retenue par la Commission Nationale Informatique et Libertés à l'égard de Totalenergies, producteurs et fournisseur d'énergie anciennement connu sous le nom de Total.

Dans son avis, la CNIL explique avoir épinglé Totalenergies pour plusieurs manquements à la réglementation en vigueur en matière de prospection commerciale : sur son site web, la société proposait un formulaire en ligne permettant de souscrire à une nouvelle offre. Simplement celui ci autorisait l'entreprise à appeler le client pour des opérations de prospection commerciale sans lui proposer la possibilité de refuser ce démarchage. Un nouveau client était donc automatiquement enrôlé dans les programmes de prospection commerciale de Totalenergies, ce qui va à l'encontre des dispositions prévues par l'article L. 34-5 du code des postes et des communications électroniques selon la CNIL.

Outre cet écart, la CNIL indique avoir constaté plusieurs manquements aux principes énoncés par le RGPD concernant cette fois plus spécifiquement le démarchage téléphonique des personnes. La CNIL souligne ainsi à manquement à l'obligation d'informer les personnes démarchées par téléphone de leurs droits : « les informations essentielles concernant le traitement de leurs données n'étaient pas communiquées aux personnes contactées » et celles ci ne pouvaient pas y accéder l'appui d'une touche au début de l'appel par exemple.

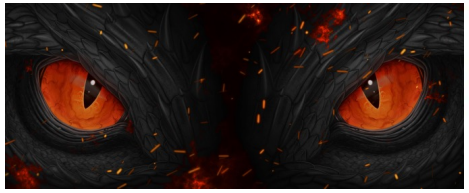
Dans la même veine, la CNIL constate que les méthodes de démarchages téléphoniques de Totalenergies ne permettaient pas de respecter le droit d'accès aux données et le droit d'opposition. Et précise également que la société n'a pas répondu aux demandes d'exercice de ces droits par les clients concernés dans un délai d'un mois, la durée maximum prévue par les textes.

Le Futur proche

Data Governance Act, Data Act : de quoi s'agit-il ?

Le *Data Governance Act* et le *Data Act* s'inscrivent dans le cadre de la stratégie européenne pour les données, présentée par la Commission européenne en février 2020. Cette stratégie vise à développer un marché unique de la donnée en soutenant l'accès, le partage et la réutilisation responsables, dans le respect des valeurs de l'Union européenne et notamment la protection des données personnelles.

Elle s'inscrit dans le contexte plus large du plan d'action de la Commission européenne visant à assurer la souveraineté numérique de l'Europe à l'horizon 2030, et est complémentaire de la stratégie européenne en matière d'intelligence artificielle.



Le règlement sur la gouvernance des données (*Data Governance Act*)

Première brique de la série de mesures annoncées dans le cadre de la stratégie européenne des données, le *Data Governance Act* a été adopté en mai 2022, et sera applicable en septembre 2023. Il vise à favoriser le partage des données personnelles et non personnelles en mettant en place des structures d'intermédiation. Ce règlement comporte :

- un encadrement ainsi qu'une assistance technique et juridique facilitant **la réutilisation de certaines catégories de données protégées du secteur public** (informations commerciales confidentielles, propriété intellectuelle, données personnelles) ;
- **une certification obligatoire pour les fournisseurs de services d'**intermédiation de données ;
- **une certification facultative pour les organismes pratiquant l'**altruisme en matière de données.

Le règlement sur les données (*Data Act*)

La proposition législative de la Commission européenne, présentée le 23 février 2022, a pour objectif **d'assurer une meilleure répartition de la valeur issue de l'utilisation des données personnelles et non personnelles entre les acteurs de l'économie de la donnée,** notamment liées à l'utilisation des objets connectés et au développement de l'Internet des objets.