EPD
ÉQUIPE PROTECTION DES DONNÉES

CENTRE DE GESTION
de la fonction publique territoriale

RGPD

Les Actus

Un tour d'horizon des actualités sur la protection des données des derniers mois

Janvier-Mars 2025

Sanctions et mesures correctrices : bilan 2024 de l'action de la CNIL

L'année 2024 est marquée par un doublement des sanctions prononcées par la CNIL par rapport à 2023.

Au total, 331 décisions ont été rendues dont :

- **180 mises en demeure**. Parmi les thématiques majeures, figurent notamment l'absence de réponse aux demandes d'exercice de droits ou encore l'insuffisance des mesures de sécurité pour protéger les données.
- **64 rappels aux obligations légales**, un chiffre inédit pour ce type de mesures.
- **87 sanctions, totalisant un montant de 55 212 400 euros en 2024**. Parmi ces sanctions 18 ont été prononcées selon la procédure ordinaire et 69 selon la procédure simplifiée.

Quelques exemples de sanctions prononcées dans le cadre de la procédure de sanction simplifiée :

- Défaut de coopération avec la CNIL (absence de réponse à ses sollicitations)
- Non-respect de l'exercice des droits des personnes concernées
- Manquement à la sécurité des données personnelles (mots de passe insuffisamment robustes, stockage de mots de passe en clair, par exemple)
- Manquement à la minimisation des données (commentaires excessifs, par exemple)

Enfin, des organismes ont également été sanctionnés pour ne pas avoir permis aux utilisateurs de refuser les cookies aussi facilement que de les accepter, en compliquant notamment le mécanisme de refus des cookies (cf. ci-dessous).

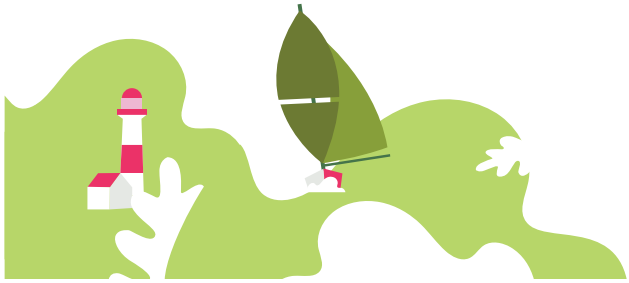
La CNIL met en demeure des éditeurs de sites web de modifier leurs bannières cookies considérées comme trompeuses

La CNIL a mis en demeure plusieurs éditeurs de sites web après avoir constaté des pratiques non conformes concernant les bandeaux de consentement pour le dépôt des cookies. Ces bannières ont été jugées trompeuses, incitant de manière excessive les internautes à accepter les cookies et rendant le refus plus difficile.

Les pratiques jugées non conformes observées par la CNIL sont les suivantes :

- L'option de refus des cookies est peu visible et moins mise en avant que l'option d'acceptation (couleur, taille de police, emplacement).
- L'option de refus noyée parmi d'autres informations sans distinction visuelle claire.
- Une option d'acceptation répétée plusieurs fois, tandis que l'option de refus n'apparaît qu'une seule fois et avec des termes peu clairs, comme «je décline les finalités non essentielles».

A cette occasion, la CNIL rappelle que le dépôt de cookies nécessite le consentement explicite des utilisateurs, et que refuser les cookies doit être aussi simple que de les accepter. Bien que la législation ne spécifie pas de format précis pour les bannières, elle exige qu'elles soient claires, transparentes et qu'elles ne trompent pas l'internaute. Les informations figurant sur cette bannière doivent préciser les finalités des cookies et la manière de refuser leur dépôt.



Droit d'accès : bilan des contrôles de la CNIL

En 2024, dans le cadre d'une action coordonnée au niveau européen, la CNIL a mené des contrôles sur 11 organismes publics et privés pour vérifier la mise en œuvre du droit d'accès des personnes à leurs données personnelles. En effet, en vertu de l'article 15 du RGPD, les personnes disposent du droit d'obtenir du responsable de traitement l'accès aux données personnelles les concernant.

Les contrôles ont révélé que la majorité des organismes avaient mis en place des procédures pour traiter les demandes d'accès (par exemple la désignation d'un DPO), mais ces mesures sont parfois insuffisantes et certains organismes ne fournissent qu'une réponse partielle ou incomplète. Par exemple, certains organismes ne fournissent qu'une copie des données sans préciser les informations sur leur traitement, tandis que d'autres excluent systématiquement certains traitements ou catégories de données.

À la suite de ces contrôles, la CNIL a déjà adressé plusieurs rappels aux obligations légales et pourrait prendre d'autres mesures correctives (mise en demeure, amende) ou clore les procédures si aucune violation n'est constatée.

Violations massives de données en 2024 : bilans et conseils de la CNIL

En 2024, la CNIL a reçu notification de 5 629 violations de données personnelles. Au-delà de cette hausse significative par rapport aux années précédentes, la CNIL relève la recrudescence de violations de très grande ampleur, comme celles ayant touché des structures telles que France Travail ou encore le société Free.

Dans son bilan, la CNIL constate que les violations de données massives sont souvent dues à des défauts de sécurité récurrents, par exemple : hameçonnage, failles de sécurité dans les pares-feux, habilitations trop larges, conservation des données pendant une durée excessive…

La CNIL rappelle donc l'importance de renforcer les mesures de sécurité au regard des risques pour les données personnelles, par exemple : systématiser les comptes nominatifs individuels, limiter l'accès au réseau (y compris via VPN) aux seuls équipements authentifiés par exemple ou encore appliquer de façon stricte les principes de durée de conservation limitée des données personnelles par un mécanisme d'archivage ou de purge automatique.

Focus : la violation de données personnelles

Une violation de données personnelles se définit comme tout incident de sécurité, d'origine malveillante ou non et se produisant de manière intentionnelle ou non, ayant comme conséquence de compromettre l'intégrité, la confidentialité ou la disponibilité de données personnelles.
Exemples : suppression accidentelle de données personnelles, perte de documents ou de matériels contenant des données personnelles, introduction malveillante dans une base de données…

En cas de violation de données, le RGPD prévoit une procédure à suivre (articles 33 et 34 du RGPD) :

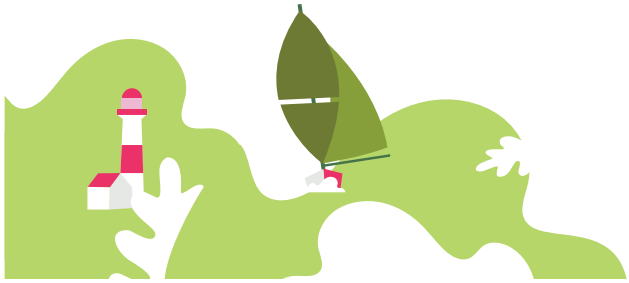
- La violation de données doit être documentée par le responsable de traitement dans un registre dédié ;
- En cas de risque pour les droits et libertés des personnes, la violation de données doit être notifiée à la CNIL dans les 72 heures suivant la constatation de la violation. Cette violation peut être notifiée via le téléservice dédié de la CNIL ;
- En cas de risque élevé pour les droits et libertés des personnes, il revient au responsable de traitement de notifier la violation aux personnes concernées, sauf exceptions limitativement énumérée par le texte.

Dès la constatation d'une violation de données, nous vous préconisons de prendre l'attache de votre délégué à la protection des données afin qu'il vous accompagne pour le traitement de celle-ci.

En Europe : des municipalités sanctionnées suite à la perte d'une clé USB contenant des données personnelles

L'autorité polonaise de protection des données a annoncé avoir infligé des amendes allant de 3 500 à 4 600 euros à deux institutions municipales polonaises, suite à la perte d'une clé USB contenant des données personnelles non chiffrées. Cette clé, utilisée pour transférer des informations d'un système de gestion des ressources humaines à un autre, renfermait des données sensibles relatives à plus de 1 500 personnes. Parmi ces informations figuraient des éléments tels que noms, prénoms, dates de naissance, adresses, numéros de compte bancaire, coordonnées, détails sur les revenus, numéros de cartes d'identité, ainsi que l'historique de l'emploi et les données concernant les enfants des agents.

Les données n'ayant pas été correctement protégées, l'autorité polonaise de protection des données a décidé d'imposer des amendes aux institutions concernées. Ainsi, cette décision, fondée sur le RGPD, souligne l'application du Règlement européen à l'ensemble de ses membres.



Pour en savoir plus :

Sanctions et mesures correctrices : bilan 2024 de l'action de la CNIL
https://www.cnil.fr/fr/sanctions-et-mesures-correctrices-bilan-2024-de-laction-de-la-cnil

Des bannières cookies considérées comme trompeuses
https://www.cnil.fr/fr/bannieres-cookies-trompeuses-la-cnil-met-en-demeure-des-editeurs-de-sites-web

Droit d'accès : bilan des contrôles de la CNIL dans le cadre d'une action coordonnée européenne
https://www.cnil.fr/fr/droit-dacces-bilan-des-controles-de-la-cnil-dans-le-cadre-dune-action-coordonnee-europeenne

Violations massives de données en 2024 : bilan et conseils de la CNIL
https://www.cnil.fr/fr/violations-massives-de-donnees-en-2024-quels-sont-les-principaux-enseignements-mesures-a-prendre

L'absence de mesures techniques et organisationnelles appropriées peut poser des problèmes
Data Legal Drive – 13/11/24

EPD
ÉQUIPE PROTECTION DES DONNÉES

Service protection des Données
Direction Développement Numérique
et Assistance Métiers
02 96 58 63 66
cil@cdg22.fr