Cybersécurité

Le RGPD : la meilleure prévention contre les risques cyber

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

www.cnil.fr

LE RGPD, UN INSTRUMENT AU SERVICE DE LA CYBERSÉCURITÉ

La sécurité informatique, une obligation présente dès 1978 et un cadre renforcé avec le RGPD

La sécurité fait partie des principes fondamentaux de la loi Informatique et Libertés. En effet, l'absence de sécurité d'un traitement de données personnelles fait notamment courir le risque que des données soient récupérées par un tiers malveillant et utilisées contre les personnes concernées.

Le RGPD a rehaussé les exigences en matière de sécurisation des données personnelles. Il a ainsi renforcé le rôle des autorités de protection des données auprès de l'ensemble des entreprises et des administrations en matière de cybersécurité.

LES OBLIGATIONS DE SÉCURITÉ PRÉVUES PAR LE RGPD
Mettre en place des mesures techniques et organisationnelles pour sécuriser les données
Tenir un registre des violations de données
Effectuer une analyse d'impact (AIPD) > Pour certains traitements sensibles
Notifier la CNIL d'une violation de données > En cas de risque pour les personnes
Informer les personnes d'une violation de données > En cas de risque élevé pour les personnes

Le RGPD est le seul texte à imposer des obligations de cybersécurité précises, de façon transversale, et soumises au pouvoir de contrôle et de sanction d'une autorité administrative telle que la CNIL.

En cas de non-respect des règles

Amende administrative de 20 millions d'euros ou 4 % du chiffre d'affaires

La CNIL accompagne les administrations et les entreprises dans la prise en compte de la sécurité informatique.

L'obligation de sécurité, inscrite dans la loi depuis plus de 40 ans, a été renforcée par le RGPD et complétée de nouvelles obligations et d'outils comme la notification des violations, l'analyse d'impact sur la protection des données, les codes de conduite ou la certification.

LES CHIFFRES

5 037 notifications de violation de données en 2021. **+ 79 %** par rapport à 2020.

+ de 2 150 notifications de violations résultant d'une **attaque par rançongiciel** reçues en 2021, soit **43 %** du volume total.

1/2 des sanctions prononcées par la CNIL en 2021 vise des manquements à l'obligation de sécurité.

FOCUS

Qu'est-ce qu'une Analyse d'Impact sur la Protection des Données (AIPD) ?

L'AIPD est un outil qui permet de construire un traitement conforme au RGPD et respectueux de la vie privée. Elle concerne les traitements de données personnelles qui sont susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes concernées. Le RGPD prévoit qu'un organisme doit, lorsqu'il n'arrive pas à réduire son niveau de risque résiduel de façon satisfaisante, consulter son autorité de contrôle (la CNIL en France) préalablement à la mise en place du traitement. S'il s'avère impossible de réduire suffisamment les risques à l'issue de cette phase d'échanges, alors l'autorité de contrôle peut rendre un avis indiquant que le traitement envisagé constitue une violation du RGPD.

En savoir + www.cnil.fr/AIPD

LES NOTIFICATIONS DE VIOLATION DE DONNÉES PERSONNELLES

Qu'est-ce qu'une violation de données ?

Le RGPD définit une violation de données personnelles comme « une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données. »

Il s'agit de 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.

Quelques exemples :

- **suppression accidentelle de données médicales conservées par un établissement de santé et non sauvegardées par ailleurs ;**
- **perte d'une clef USB non sécurisée contenant une copie de la base clients d'une société ;**
- **introduction malveillante dans une base de données scolaires et modification des résultats obtenus par les élèves.**

L'année 2021 a vu le nombre de violations de données notifiées à la CNIL progresser de de 79 % par rapport à l'année précédente. En moyenne, près de 14 notifications ont été reçues par jour.

LE RGPD IMPOSE AUX RESPONSABLES DE TRAITEMENT :

> de documenter, en interne, les violations de données personnelles ;

> de notifier les violations présentant un risque pour les droits et libertés des personnes à la CNIL dans un délai de 72 h ;

> d'informer, lorsque le risque est élevé, les personnes concernées.

Nature et causes des violations notifiées

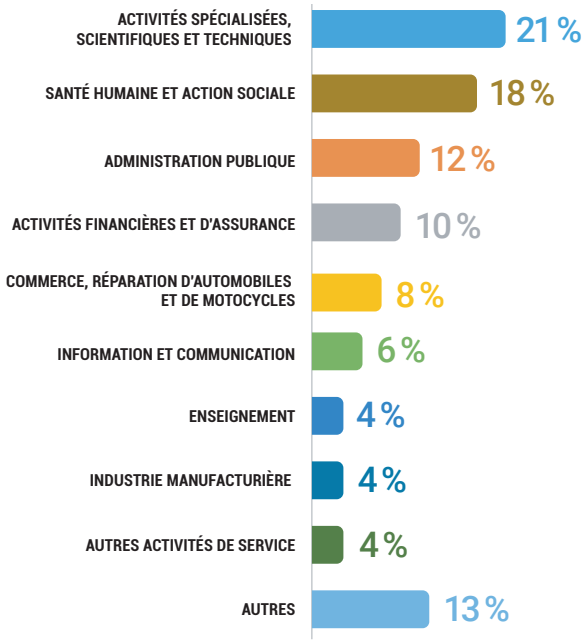
80 % des notifications de violations reçues par la CNIL concernent une **perte de confidentialité**, c'est-à-dire une intrusion par un tiers qui peut prendre connaissance des données, voire les copier.

Bien que le RGPD considère qu'une violation de données personnelles peut aussi résulter d'un incident de sécurité engendrant une perte d'intégrité et de disponibilité, les statistiques montrent que ce type de violation de données reste encore méconnu des responsables de traitement.

Toutefois, même si elles demeurent marginales par rapport aux notifications de perte de confidentialité, la CNIL constate **une nette progression des notifications liées à une perte d'intégrité (données modifiées illégitimement) et de disponibilité (données inaccessibles pendant un certain temps).** Cette évolution est notamment due à la progression des violations résultant d'une attaque par **rançongiciel**.

Par ailleurs, l'obligation de notification à l'autorité de contrôle d'une violation de données concerne les violations ayant une origine accidentelle ou illicite. La majorité des notifications reçues par la CNIL en 2021 concerne une violation de données ayant pour origine un acte externe malveillant (piratage, vol d'un support physique ou les arnaques au faux support techniques).

Les secteurs d'activité les plus concernés (chiffres 2021) :



LE PIRATAGE INFORMATIQUE EN 2021

→ **59 %** du total des notifications adressées à la CNIL, soit **3 000** notifications. (**+ 128 %** par rapport à 2020).

→ **43 %** des notifications reçues concernent une attaque par rançongiciel.

LES RESSOURCES UTILES

- **Les technologies pour protéger son patrimoine informationnel, protéger les personnes concernées des atteintes à leurs données : www.cnil.fr/fr/cybersecurite**
- **Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques à consulter quotidiennement : www.cert.ssi.gouv.fr**
- **ANSSI (Agence nationale de la sécurité des systèmes d'information) : www.ssi.gouv.fr**
- **Assistance et prévention en sécurité numérique : www.cybermalveillance.gouv.fr**

LE RÔLE DE LA CNIL EN MATIÈRE DE CYBERSÉCURITÉ

La sécurité des données personnelles est, au-delà d'une obligation légale, un enjeu majeur pour tous les organismes publics et privés, ainsi que pour tous les individus. La CNIL joue pleinement son rôle au service de la cybersécurité en déployant son action autour de quatre axes :

La sensibilisation du grand public

Pour sensibiliser le grand public aux enjeux de sécurisation des données personnelles dans les usages du quotidien, la CNIL propose différentes ressources. Elle a ainsi publié un guide, *Comment protéger mes données* ?, et de nombreuses fiches pratiques sur son site web, parmi lesquelles :

- Phishing : détecter un message malveillant
- Prévenir, repérer et réagir face au piratage de ses comptes sociaux
- Réagir en cas de chantage à la webcam
- 4 réflexes pour mieux protéger votre identité en ligne
- Comment réagir face à une usurpation d'identité ?
- 10 conseils pour rester net sur le web
- Les conseils de la CNIL pour un bon mot de passe
- La navigation privée pour limiter les risques de piratage de vos comptes en ligne

La CNIL met également en place des partenariats avec des relais au sein de la société civile et des entreprises.

L'accompagnement des professionnels

Dans la mise en place d'une politique de cybersécurité efficace, toutes les étapes sont essentielles. Afin d'accompagner au mieux les professionnels, la CNIL met à disposition son expertise au travers de nombreuses ressources, notamment :

- une recommandation sur les mots de passe, qui sera prochainement mise à jour ;
- une recommandation sur la journalisation ;
- un guide général sur la sécurité des données ainsi qu'une check-list ;
- des fiches pratiques pour sécuriser les sites web et les systèmes d'information ;
- des publications régulières sur des exemples de violations de données fréquentes (rançongiciels, fraude au président, attaques sur les messageries, attaques sur les défauts de configuration de cloud, credential stuffing, etc.)

Au-delà de ces conseils généraux, applicables dans la plupart des cas, la CNIL publie également des rappels et des bonnes pratiques pour de nombreux secteurs d'activité dans ses différents guides (TPE/PME, associations, collectivités, etc.). La question de la sécurité des données tient également une place importante dans les projets bénéficiant d'un accompagnement renforcé de la CNIL dans le cadre de son dispositif « bac à sable » lancé en 2021 sur le thème de la santé numérique et sur les EdTech cette année.

Un accompagnement spécifique des TPE/PME

La CNIL met à disposition des TPE/PME différents outils, tels que le guide de vulgarisation du RGPD co-édité avec Bpifrance, une check-list RGPD, des référentiels, le guide des durées de conservation des données, un modèle simplifié de registre ou encore des fiches pratiques sur son site web. Pour en assurer la diffusion, la CNIL a mis en place une stratégie dite « des têtes de réseaux », indispensable pour toucher indirectement l'ensemble des acteurs via les associations, fédérations ou réseaux professionnels. Ces derniers produisent également, avec le concours de la CNIL, des guides pratiques et des outils d'évaluation adoptés aux activités spécifiques de leurs adhérents.

Une prise de conscience des organismes e

Tous les organismes sont aujourd'hui touchés par les attaques, quels q

La CNIL constate une réelle prise de conscience liée à ces enjeux de cybersé échanges entre les responsables des métiers, les responsables de la prote direction des systèmes d'information. Cette pluridisciplinarité est une néces

Néanmoins, si cette évolution se traduit par une meilleure anticipation da sécurité ne sont pas toujours respectées. En particulier, les organismes de t informatique, sont particulièrement touchés par la vague de rançongiciels qu années, et particulièrement en 2020 et début 2021.

La CNIL constate également des manquements liés au défaut de déploiem que dans le cadre des notifications de violations de données qui lui ont été

Un contrôle systématique et des sanctions régulières

Par ailleurs, la sécurité est vérifiée de manière systématique dans les 300 procédures formelles de contrôle que la CNIL mène chaque année, d'abord par la vérification du respect des principes de base (mots de passe, sécurisation des bases de données et du réseau, etc.), mais aussi par la vérification de l'existence d'un registre des violations, nouvelle obligation issue du RGPD.

Les manquements les plus fréquents :

- **des données librement accessibles par modification d'URL (défaut d'authentification, URL prédictible),** par exemple quand il suffit de modifier un nombre dans la barre d'adresse pour accéder à des documents d'autres personnes ;
- **une politique de mot de passe non conforme, ne respectant pas au minimum la recommandation mot de passe de la CNIL ;**
- **la transmission de mot de passe en clair,** par exemple lors de la création d'un compte sur un site web ;
- **la transmission de données par une connexion non chiffrée (HTTP),** par exemple dans le cas d'un formulaire sur un site web par lequel l'utilisateur envoie des données personnelles ;
- **l'absence de verrouillage automatique des sessions des postes de travail, permettant ainsi à un tiers d'accéder à un système d'information contenant des données personnelles ;**
- **un défaut de protocole de test afin de garantir l'absence de vulnérabilité avant la mise en production d'un nouveau développement :** c'est le cas quand un organisme développe un nouvel outil (application, site web, formulaire) traitant des données personnelles, sans prévoir de phase de test destinée à identifier les éventuelles vulnérabilités de l'outil.

La participation à l'écosystème cyber

La CNIL a développé de nombreux partenariats avec les acteurs de la cybersécurité, notamment avec l'Agence nationale de la sécurité des systèmes d'information (ANSSI).

Guide de sensibilisation aux cyberattaques édité par l'ANSSI avec la contribution de la CNIL « Attaques par rançongiciels, tous concernés ».

En 2022, pour renforcer son action, la CNIL a rejoint le Campus Cyber, qui rassemble les principaux acteurs du domaine en France. Ses relations se sont également intensifiées avec le GIP Actions contre la cybermalveillance (ACYMA) dont le but est de lutter contre les actes de cybermalveillance en s'appuyant sur le dispositif cybermalveillance.gouv.fr. Cette collaboration s'est traduite par l'adhésion de la CNIL au GIP en mars 2022.

La CNIL est également membre d'associations telles que le Club EBIOS ou le CESIN et participe aux principaux évènements liés à la cybersécurité comme le Forum International de la Cybersécurité (FIC).

Les attaques par rançongiciel

FOCUS

Le rançongiciel (*ransomware* ou *cryptolocker* en anglais) est un programme malveillant qui empêche l'accès de la victime à ses données, en les chiffrant, qui va ensuite demander une rançon à la victime en échange de la clé de déchiffrement. Il se transmet souvent par une pièce jointe de courriel ou des liens permettant le téléchargement de logiciels ou de contenus. Une fois présent dans le système informatique, ce programme va progressivement chiffrer tous les fichiers accessibles et les rendre ainsi illisibles. Dans le cas d'un réseau d'entreprise, le logiciel va chercher à se propager sur toutes les ressources accessibles.

Le rançongiciel est répandu car très rentable pour les attaquants. Si ce type d'attaque est parfois opportuniste, pour des rançons correspondant généralement à quelques centaines d'euros, de plus en plus d'entités de taille importante sont ciblées pour des montants pouvant atteindre plusieurs millions d'euros.

Certains rançongiciels utilisent des failles de sécurité connues afin de se propager via le réseau des organismes touchés et de multiplier les dommages. En particulier, en rendant inaccessibles les serveurs, logiciels et données de leurs victimes, les rançongiciels entraînent une indisponibilité de services critiques (site web, services destinés aux utilisateurs ou internes) et très souvent une altération et/ou une perte de disponibilité des données personnelles, ce qui constitue alors une violation de données personnelles.

encore insuffisante

que soient leur taille et leur secteur.

curité au sein des organismes. Celle-ci passe par le développement des ction des données, les responsables des risques et de la sécurité et la sité : il ne peut, en effet, y avoir de protection des données sans sécurité.

ns les projets liés aux systèmes d'information, les règles de bases en aille moyenne, souvent insuffisamment équipés en matière de sécurité ui frappe l'ensemble des entreprises et administrations depuis quelques

ent de solutions de chiffrements adéquates, tant lors de ses contrôles adressées. La mise en place de ces solutions doit devenir un réflexe.

Commission nationale
de l'informatique
et des libertés
3 place de Fontenoy
TSA 80715
75334 PARIS CEDEX 07
01 53 73 22 22

www.cnil.fr

www.cnil.fr/fr/cybersecurite

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

www.cnil.fr