Cybersécurité

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 ferait 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 la vocation des autorités de protection des données à accompagner l'ensemble des entreprises et les 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

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 outils comme la notification des violations, l'analyse d'impact sur la protection des données, les codes de conduite ou la certification.

LES CHIFFRES

2 825
notifications
de violation de données en 2020. **+ 24 %** par rapport à 2019.

+ de 500
notifications
de violations résultant d'une attaque par rançongiciel reçues en 2020, soit **20 %** du volume total.

2/3
des sanctions
prononcées par la CNIL visent des manquements à l'obligation de sécurité des données et plus de **40 %** des sanctions sont prises sur ce seul fondement.

3 X plus
de violations
liées à des attaques par cryptoverrouillage sur des établissements de santé (centre hospitalier, clinique, EPHAD, maison de santé, établissements de soin, laboratoires etc.).

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

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 reçoit, chaque année, de nombreuses notifications de violations de données qui peuvent avoir de lourdes conséquences. La CNIL joue pleinement son rôle au service de la cybersécurité en déployant son action autour de quatre axes :

1. **La sensibilisation du grand public**
2. **L'accompagnement des professionnels**
3. **Un contrôle systématique et des sanctions régulières et élevées**
4. **La participation à l'écosystème cyber,** notamment par sa collaboration avec l'Agence nationale de la sécurité des systèmes d'information (ANSSI) et sa présence à différents évènements thématiques.

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, notamment via le collectif Educnum qu'elle a initié en mai 2013. Celui-ci rassemble divers acteurs issus du monde de l'éducation, de la recherche, de l'économie numérique, de la société civile, de Fondations d'entreprises et d'autres institutions, pour porter et soutenir des actions visant à promouvoir une véritable culture citoyenne du numérique.

L'accompagnement des professionnels

La mise en conformité avec les règles de protection des données constitue souvent la première étape dans la mise en place d'une politique de cybersécurité. C'est pourquoi la CNIL publie régulièrement des guides pour accompagner les responsables de traitement et leurs sous-traitants, comme par exemple :

- **une recommandation sur les mots de passe ;**
- **un guide sur la sécurité des données personnelles ;**
- **les guides sur les analyses d'impact sur la protection des données et le logiciel PIA ;**
- **une check-list sécurité ;**
- **un guide pour les développeurs, publié sur la plateforme GitHub.**
- **des publications régulières des « violations du trimestre » qui donnent les bonnes pratiques pour les éviter ou en limiter les conséquences (injections SQL, credential stuffing, fraude au président) ;**
- **le guide de sensibilisation aux cyberattaques édité par l'ANSSI avec la contribution de la CNIL « Attaques par rançongiciels, tous concernés » ;**
- **des bonnes pratiques sur des logiciels (Elasticsearch).**

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, 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 outils d'évaluation sur la base des activités spécifiques de leurs adhérents.

FOCUS

Les attaques par rançongiciel

Le rançongiciel (ransomware ou cryptolocker en anglais) est un programme malveillant qui empêche l'accès de la victime à ses données, en les chiffrant avec une clé connue uniquement de l'attaquant, 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 sur son « hôte », le terminal cible, ce programme va progressivement chiffrer tous les fichiers accessibles et les rendre 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 tailles importantes 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.

Un contrôle systématique et des sanctions régulières

2/3 des sanctions depuis 2017 incluent un manquement à la sécurité.

+ de 40 % des sanctions de la CNIL sont prises sur ce seul fondement.

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.

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.

Une prise de conscience des organismes encore insuffisante

Tous les organismes sont aujourd'hui touchés par les attaques, quels que soient leur taille et leur secteur.

La CNIL constate **une réelle prise de conscience liée à ces enjeux de cybersécurité** au sein des organismes. Celle-ci passe par le développement des échanges entre les responsables des métiers, les responsables de la protection des données, les responsables des risques et de la sécurité et la direction des systèmes d'information. Cette pluridisciplinarité est une nécessité : il ne peut, en effet, y avoir de protection des données sans sécurité.

Néanmoins, si cette évolution se traduit par une meilleure anticipation dans les projets liés aux systèmes d'information, **les règles de bases en sécurité ne sont pas toujours respectées.** En particulier, les organismes de taille moyenne, souvent insuffisamment équipés en matière de sécurité informatique, sont particulièrement touchés par **la vague de rançongiciels qui frappe l'ensemble des entreprises et administrations** depuis quelques années et notoirement en 2020 et début 2021.

La CNIL constate également des manquements liés au défaut de déploiement de solutions de chiffrements adéquates, tant lors de ses contrôles que dans le cadre des notifications de violations de données qui lui ont été adressées. La mise en place de ces solutions doit devenir un réflexe.

LES NOTIFICATIONS DE VIOLATION DE DONNÉES PERSONNELLES

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

Le RGPD définit une violation de données à caractère personnel 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. »

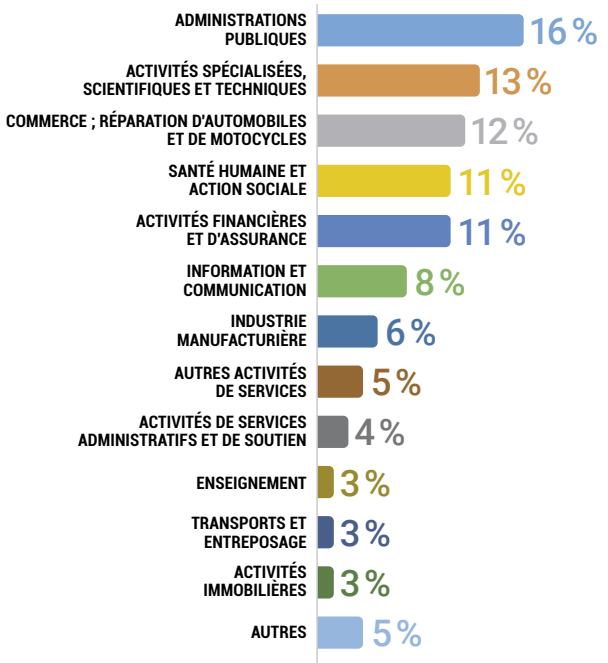
Il s'agit de tout incident de sécurité, d'origine malveillante ou non et se produisant de manière intentionnelle ou non, ayant comme conséquence de compromettre l'intégrité, la confidentialité ou la disponibilité de données personnelles.

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 2020 a vu le nombre de violations de données notifiées à la CNIL en progression de 24 % par rapport à l'année précédente. En moyenne, plus de 11 notifications ont été reçues par jour ouvré.

Les secteurs d'activité les plus concernés :



Nature et causes des violations notifiées

69 % 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 démontrent 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 2020 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).

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.

LE PIRATAGE INFORMATIQUE EN 2020

→ **47 %** du total des notifications adressées à la CNIL, soit **1 315** notifications. (**+ 70 %** par rapport à 2019)

→ **94 %** des actes externes malveillants notifiés à la CNIL.

L'attaque la plus répandue reste l'attaque par rançongiciel.

LES RESSOURCES UTILES

- **Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques :** 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

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

www.cnil.fr

www.cnil.fr/fr/cybersecurite

AGENCE LINÉAL - 03 20 41 40 76

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

www.cnil.fr