La CNIL donne ses consignes pour renforcer la sécurité des grandes bases de données

30 avril 2025

L'année 2024 a été marquée par une recrudescence de fuites de données massives, concernant plusieurs millions de personnes. Leur fréquence croissante justifie de renforcer la sécurité des traitements concernant de grands volumes de données personnelles. La CNIL met en avant les mesures nécessaires à cette fin.

L'année 2024 a été marquée par un accroissement important du nombre de violations de données touchant plusieurs millions de personnes. Ces incidents ont concerné quelques acteurs publics et, de manière notable, des bases de données clients/prospects et usagers de nombreux acteurs privés.

Les informations fournies par les organismes dans les notifications ou obtenues à l'occasion des contrôles menés par la CNIL montrent que ces violations sont dues à des attaques opportunistes. Elles ont souvent des modes opératoires similaires rendus possible par des défauts récurrents de sécurité :

- les couples « identifiant + mot de passe » de connexion d'utilisateurs légitimes avaient été usurpés, et ont permis d'accéder aisément aux données ;
- les intrusions et les exfiltrations n'ont pas été détectées par l'organisme avant la mise en vente ou l'exploitation des jeux de données ;
- une part significative des incidents impliquait un **sous-traitant**, au sens de l'article 4.8 du RGPD, dont les mesures de sécurité étaient insuffisantes.

Traiter un très grand nombre de données personnelles, implique de mettre en œuvre des mesures de sécurité renforcées

L'article 5.1.f) du RGPD impose aux responsables de traitement et aux sous-traitants de traiter les données personnelles de façon à leur garantir un niveau de sécurité approprié. Son article 32 prévoit ainsi qu'ils doivent mettre en place des mesures de sécurité adaptées, compte tenu des risques et de l'état de l'art, afin de protéger les données qu'ils traitent.

Le guide de la sécurité des données personnelles publié par la CNIL rappelle les précautions de sécurité élémentaires. Ces principes constituent un socle : ils doivent être mis en œuvre de façon systématique. Elles protègent la plupart des systèmes non sensibles contre des risques les plus courants.

Toutefois, les récentes violations montrent que certaines de ces mesures élémentaires doivent être renforcées pour prévenir les risques de sécurité qui concernent les **grandes bases de données**. Cette notion inclut les bases de données « clients » et les logiciels CRM (*customer relationship* management), souvent mis en œuvre par des entreprises s'adressant au grand public.

Dans la présente communication, le terme de « bases de données » est à entendre de manière large comme l'ensemble des systèmes d'information permettant le traitement d'un même ensemble de données personnelles, **avec tous les composants, réseaux et applications impliqués dans ces traitements** et l'accès aux données (que celles-ci soient ou non contenues dans une ou plusieurs « bases de données » au sens technique).

Les bases qui contiennent les données de plusieurs millions de personnes sont à considérer comme étant de « grandes bases de données », au sens de la présente communication.

De tels traitements présentent des **risques particulièrement importants**, en particulier parce qu'une **violation de données** personnelles les affectant entraîne **des conséquences sur une part significative de la population** et expose les personnes à de nombreux risques (hameçonnage, usurpation d'identité, etc.). Elle peut également, par rebond, fragiliser d'autres systèmes d'information via l'utilisation des données compromises.

Les mesures de sécurité dites « périmétriques », qui visent à protéger un système d'information contre des menaces qui lui sont extérieures, **doivent ainsi être complétées pour des systèmes de grande taille exposés sur Internet.** Pour ces raisons, s'agissant des grandes bases de données, des mesures de « défense en profondeur », permettant également de se protéger de menaces ayant déjà atteint le SI lui-même, doivent être mises en œuvre.

La CNIL met en avant plusieurs mesures essentielles pour sécuriser les grandes bases de données

La CNIL appelle l'attention des responsables de traitement sur **des mesures de sécurité qu'elle considère comme en principe requises au titre des articles 5.1.f et 32 du RGPD dès lors que des grandes bases de données sont concernées**, notamment au regard des risques d'exfiltrations massives de données. Ces mesures prolongent et renforcent les précautions de sécurité élémentaires. Elles doivent, en outre, être déclinées en fonction de l'architecture du traitement.

Cette liste, à l'instar des mesures cyber prioritaires de l'ANSSI ou celles pour prévenir les fuites de données, ne vise pas à énumérer toutes les mesures suffisantes pour assurer la sécurité des traitements, ce que seule une analyse approfondie des risques permet de déterminer.

La CNIL rappelle par ailleurs que s'assurer du respect des autres principes du RGPD, tels que la minimisation des données et la limitation de la durée de conservation, y compris par des mesures techniques, selon les principes de protection des données dès la conception et par défaut, vient limiter l'impact des fuites de données pour les personnes concernées. Elle rappelle également que le délégué à la protection des données a vocation à être impliqué dans la démarche de sécurisation des traitements de données personnelles.

En l'absence de mesures de sécurité adéquates, la CNIL peut être amenée à relever un manquement à l'article 32, passible d'une amende administrative pouvant s'élever jusqu'à 10 millions d'€ ou jusqu'à 2 % du chiffre d'affaires annuel, le montant le plus élevé étant retenu.

1 Sécuriser les accès externes au système d'information, via une authentification multifacteur

Cette mesure apparaît comme essentielle lorsque la connexion au SI est possible depuis l'extérieur de l'organisme et notamment lorsque des utilisateurs (employés, prestataires, partenaires, etc.) peuvent accéder à des données de plusieurs millions de personnes. Près de 80% des violations de grande ampleur constatées par la CNIL en 2024 ont été permises par l'usurpation du compte d'un employé ou d'un sous-traitant qui était protégé uniquement par un mot de passe.

L'ajout d'un deuxième facteur d'authentification contribue à **réduire significativement le risque d'un accès non autorisé à la suite d'une usurpation d'identité**, dans un contexte où la circulation des « identifiants & mots de passe » résultant de précédentes fuites de données et la fréquence des attaques réutilisant ces données de manière massive (*credential stuffing* ou « bourrage d'identifiant ») doivent être prises en compte.

Les responsables de traitement peuvent à cet égard s'appuyer sur la recommandation de la CNIL relative à l'authentification multifacteur, ainsi que sur les recommandations de l'ANSSI relatives à l'authentification multi-facteur et aux mots de passe.

Pour les grandes bases de données, la CNIL recommande :

- de mener une analyse de risques prenant en compte les événements redoutés pouvant survenir en lien avec les différents moyens d'accéder aux données ;
- de privilégier l'utilisation de l'authentification reposant sur un **facteur de possession** (satisfaisant au moins le niveau « R39 - - » identifié dans les recommandations de l'ANSSI).

Ce type de mesure doit s'inscrire dans une **politique plus large de gestion des identités et des accès** que l'organisme doit mettre en œuvre et maintenir dans le temps, en fonction des profils d'utilisateurs (collaborateurs, prestataires, développeurs, administrateurs, etc.). Ce processus doit tendre à ce que seuls les utilisateurs autorisés puissent accéder aux informations pertinentes, en fonction de leur rôle dans l'organisation et des informations dont ils ont besoin pour accomplir leurs tâches professionnelles.

Pour les organismes qui n'y auraient pas encore recours, la mise en place d'une sécurisation des accès distants par l'authentification multifacteur est susceptible d'engendrer un effort humain et financier non négligeable, ainsi qu'un délai de déploiement dont il convient de tenir compte. Tout en reconnaissant ces contraintes, la CNIL considère, vis-à-vis des grandes bases de données, cet effort comme proportionné au regard des risques pour les personnes concernées et du bénéfice apporté en termes de sécurité.

Enfin, la CNIL rappelle que l'obligation d'assurer la sécurité des données personnelles s'impose pour tous les traitements. À cet égard, au-delà du cas des grandes bases, la mise en place d'une authentification multifacteur est requise dans d'autres contextes, en particulier quand la violation des données exposerait les personnes concernées à des risques élevés (en raison par exemple de la présence de données bancaires ou de numéros de sécurité sociale) ou lorsque les données traitées sont sensibles au sens du RGPD.

2 Journaliser, analyser et fixer des limites sur les flux de données qui transitent sur le système d'information

Le responsable du traitement comme le sous-traitant doivent **mettre en place une journalisation adaptée** afin de les aider à détecter les incidents concernant des données personnelles de façon précoce et disposer d'éléments exploitables pour les analyser a posteriori.

Pour y parvenir, l'organisme doit **se doter de moyens humains et d'une organisation adéquate** pour analyser les alertes et **y réagir le plus tôt possible.**

Dès lors que des fonctionnalités d'extraction « de masse » sont offertes, il est nécessaire de **limiter le volume des extractions** qu'un attaquant serait en mesure de réaliser en les exploitant. Les mesures préventives peuvent notamment consister à limiter les volumes de requêtes autorisés par utilisateur et à l'échelle globale, pour une application donnée. Ces limitations peuvent aussi porter sur la quantité de données transitant sur les flux sortants.

De manière complémentaire, la CNIL rappelle que sa recommandation relative à la journalisation, ainsi que celle de l'ANSSI pour l'architecture d'un système de journalisation, précisent les mesures à mettre en œuvre et recommandent en particulier :

- de mettre en œuvre une architecture de journalisation permettant d'assurer une traçabilité des accès et des actions des différents utilisateurs habilités à accéder aux systèmes d'information, pour une durée comprise entre six mois et un an. Une bonne pratique consiste à journaliser les accès (aux applicatifs, aux API, au système, au réseau) de manière dissociée du système principal (« puits de logs ») ;

- de mettre en œuvre ce système de journalisation de façon ciblée et permettre de détecter une activité potentiellement suspecte aussitôt que possible. La CNIL recommande de prioriser la supervision des traces sur les périmètres ou composants les plus sensibles au regard des risques plutôt que de constituer un grand volume de journaux non exploitées ou non exploitables ;

- de déterminer les événements à journaliser en fonction du contexte et des supports (postes de travail, pare-feu, équipements réseau, serveurs, etc.) pour :
  - détecter ou retarder un flux « anormal » ou excédant une limite de volume de données ;
  - ne laisser passer que les flux explicitement autorisés ;
  - conserver les connexions autorisées réussies et toutes les tentatives de connexions rejetées ;
  - contrôler le flux de données qui transitent, y compris en fonction des heures ;
  - identifier les défauts de configuration, les injections de requêtes SQL, etc.

3 Considérer l'humain comme un acteur de la sécurité : organiser des sensibilisations régulières adaptées aux profils d'utilisateurs (collaborateurs, développeurs, dirigeants, sous-traitants, etc.)

Le RGPD exige du responsable du traitement et du sous-traitant de mettre en œuvre les mesures techniques **et organisationnelles** appropriées afin de garantir un niveau de sécurité adapté au risque. Les solutions techniques seules sont insuffisantes pour assurer la protection des données personnelles dont un organisme a la charge.

La réalisation de **programmes périodiques de formation et de sensibilisation** en matière de respect de la vie privée et de sécurité apparaît nécessaire. Ces programmes doivent rappeler aux utilisateurs les erreurs les plus courantes entraînant des violations de données, la manière de les éviter et celle d'y réagir.

En effet, au regard des incidents notifiés à la CNIL, **de nombreuses situations semblent pouvoir être évitées par la sensibilisation accrue des utilisateurs :**

- des comptes de connexion qui sont partagés entre utilisateurs ;
- un utilisateur qui clique sur un lien reçu dans un message (hameçonnage) l'invitant à saisir son identifiant et son mot de passe sur un faux site ;
- un logiciel malveillant qui a été installé sur le poste d'un utilisateur et a permis de dérober les données de connexion (*malware*, *infostealer*).

Les responsables de traitement peuvent en particulier s'appuyer sur les contenus de sensibilisation mis à disposition par cybermalveillance.gouv.fr tels que le kit de sensibilisation et la sensibilisation SensCyber ainsi que le MOOC SecNumAcadémie.

Au même titre que les mesures techniques, les mesures organisationnelles sont susceptibles de faire l'objet de vérifications par la CNIL dans le cadre d'un contrôle. À cette occasion, elle en appréciera l'existence et la qualité. Comme pour les mesures techniques, l'absence de mesures organisationnelles ou des mesures insuffisantes ou inadaptées (absence de messages de sensibilisation du personnel ou de point de contact pour faire remonter un incident, par exemple) est susceptible de constituer un manquement aux obligations de sécurité issues du RGPD.

4 Encadrer la sécurité des données avec les sous-traitants

Un contrat de sous-traitance doit être conclu avec chacun des sous-traitants, précisant l'ensemble des éléments prévus à l'article 28 du RGPD : la durée et le périmètre de la sous-traitance, la finalité de la sous-traitance, les instructions de traitement documentées, l'encadrement en cas de recours à un sous-traitant ultérieur, la notification immédiate de toute violation de données.

Les traitements de très grands volumes de données par un sous-traitant doivent bénéficier du **même niveau de sécurisation renforcée et adapté aux risques.** Toute la chaine de sous-traitance doit être prise en considération, ce qui inclut les sous-traitants directs et les sous-traitants ultérieurs, en particulier ceux offrant des prestations à partir d'un cloud.

Le **responsable de traitement** doit exiger du sous-traitant la transmission de la Politique de Sécurité des Systèmes d'Information (PSSI), ainsi que de toutes les preuves de ses certifications en matière de sécurité de l'information et annexer ces documents au contrat.

Le responsable de traitement doit veiller, au préalable et pendant toute la durée du traitement avec le sous-traitant, à ce que les mesures respectent l'état de l'art et prennent en compte les recommandations de la CNIL.

S'agissant de bases de données de grande échelle, le responsable de traitement doit réaliser, faire réaliser ou disposer d'audits ou d'inspections périodiques auprès du sous-traitant, pendant toute la durée de la relation contractuelle.

La CNIL renforcera dès 2025 ses actions pour améliorer la sécurité des données personnelles

La CNIL a fait de la cybersécurité l'un des trois axes principaux de son plan d'action stratégique 2025-2028. Dès cette année, elle renforce ses actions dans le domaine afin d'améliorer le niveau de sécurité des données des Français :

- par l'accompagnement, en poursuivant l'élaboration de recommandations pour sécuriser les données personnelles au regard de l'évolution de la menace et de l'état de l'art ;
- par le contrôle des organismes, en particulier sur la mise en place de mesures renforcées s'agissant de grandes bases de données ;
- à travers la poursuite de son action d'information et de sensibilisation de tous les publics à la cybersécurité et l'hygiène numérique.

En raison du grand nombre de violations intervenues l'an dernier sur des **bases de clients/prospects et usagers**, la CNIL estime qu'un effort spécifique de sécurisation est nécessaire. Elle demande à toutes les entreprises possédant des bases de ce type, comptant plusieurs millions de personnes, de s'assurer que des **mesures adaptées aux risques soient déployées, en particulier une authentification multifacteur** pour les employés, partenaires, sous-traitants et autres intervenants accédant à distance à la base.

Consciente des difficultés opérationnelles que peut engendrer la mise en place de l'authentification multifacteur, la CNIL accompagnera les acteurs concernés dans cette démarche et les invite dans ce cadre à prendre connaissance des recommandations et guides existants (notamment : sa recommandation relative à l'authentification multifacteur, sa recommandation relative à la journalisation, son guide de la sécurité des données personnelles, ainsi que les guides et recommandations de l'ANSSI).

La CNIL renforcera dès 2026 sa politique de contrôle pour s'assurer de la mise en place de l'authentification multifacteur pour ces grandes bases de données. L'absence de cette mesure pourra justifier que soit initiée une procédure de sanction. En tout état de cause, la CNIL continuera à traiter les plaintes dont elle est saisie, à mener les contrôles qui lui paraîtront nécessaires et à adopter, si besoin, les mesures correctrices qui s'imposent. À cette occasion, elle tiendra notamment compte de l'existence de violations précédentes qui aurait dû conduire l'organisme concerné à mettre en place cette mesure d'authentification renforcée.

Elle rappelle que la mise en place d'une authentification multifacteur était déjà jugée en principe nécessaire au titre du RGPD pour des bases de données comprenant des données sensibles ou des données dont la violation exposerait les personnes à des risques importants (données bancaires et numéro de sécurité sociale notamment).

Pour approfondir

- Les contenus de la CNIL sur la cybersécurité