CNPD
COMMISSION NATIONALE POUR LA PROTECTION DES DONNÉES

# Six ans de RGPD au Luxembourg

# COMPRENDRE LES VIOLATIONS DE DONNÉES POUR MIEUX PROTÉGER LES DROITS ET LIBERTÉS DES PERSONNES ET ACCOMPAGNER LES RESPONSABLES DE TRAITEMENT

Alors que nous marquons le sixième anniversaire de l'entrée en application du Règlement général sur la protection des données (RGPD) en Europe, il est temps de faire un bilan des enseignements tirés des notifications de violations de données à caractère personnel au Luxembourg. Dans ce contexte, la CNPD souhaite donner un aperçu sur les informations récoltées au cours de ces années.

**Rappel :**

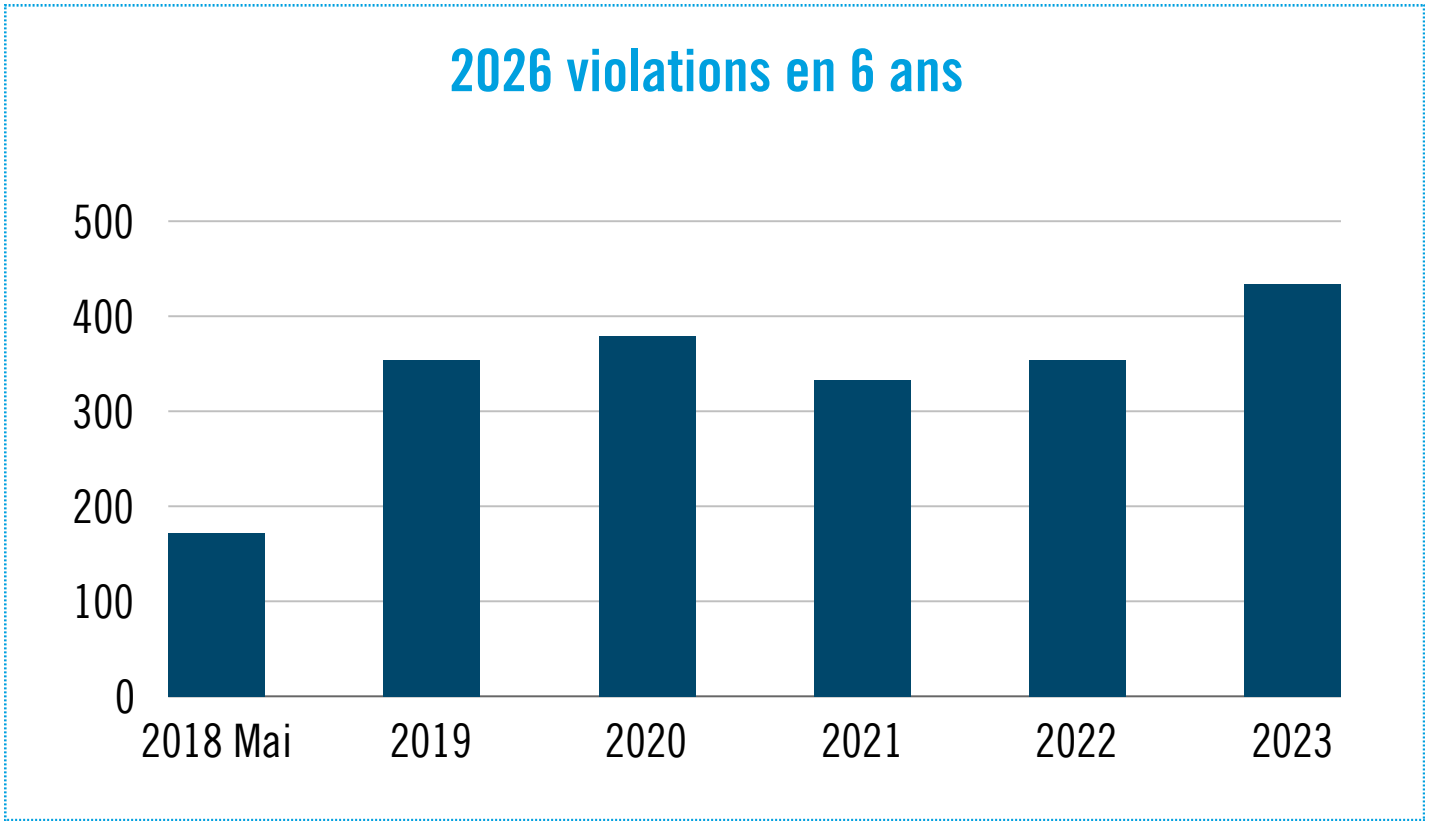
Une violation de données se produit lorsque des données personnelles sont compromises altérant ainsi leur intégrité, leur confidentialité ou leur disponibilité.

Si les responsables de traitement constatent une telle violation de données personnelles, elles ont l'obligation de la notifier à la CNPD dans un délai de 72 heures après en avoir pris connaissance si la violation en question est susceptible d'engendrer un risque pour les droits et libertés des personnes concernées, ainsi qu'aux personnes concernées elles-mêmes dans les meilleurs délais si ce risque est élevé.

# Analyse volumétrique des notifications

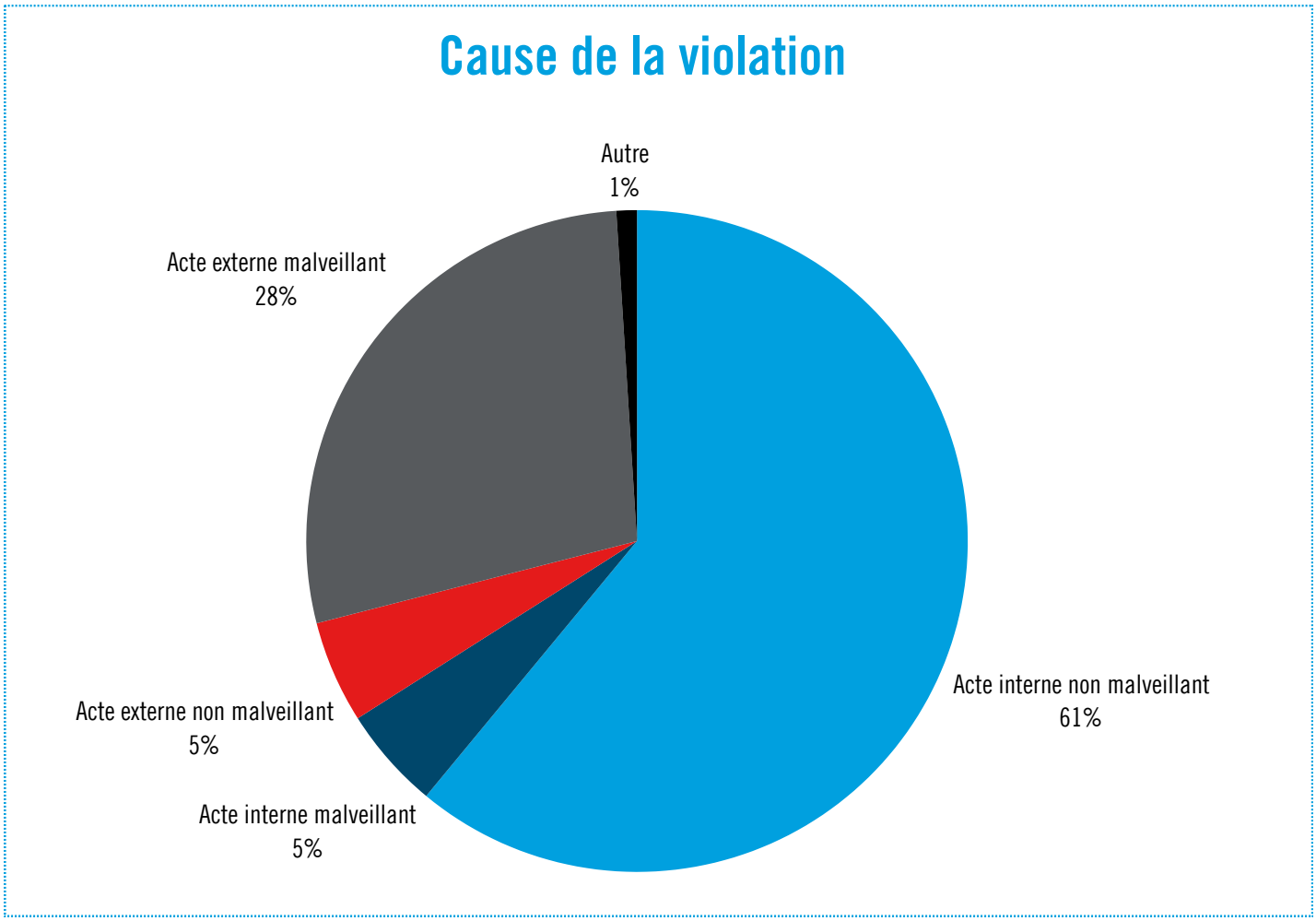
Au fil des ans, la CNPD a recueilli un nombre significatif de notifications de violations de données, provenant d'une variété d'entreprises et d'organisations. Cette riche source d'informations offre un aperçu précieux des types de violations de données rencontrées au Luxembourg, du moins celles qui ont été notifié à la CNPD.

En effet, il est important de noter que le nombre de notifications de violations de données reçues par la CNPD n'est pas représentatif du nombre réel d'incidents. En effet, tous les incidents ne sont pas systématiquement notifiés et il y a un biais lié au secteur d'activité et à la taille de l'entreprise : les grandes entreprises, mieux structurées et mieux dotées sont sur-représentées surtout si elles évoluent dans un secteur fortement régulé comme par exemple les services financiers, bancaires, assurances, télécommunication ou santé.




Après une montée en puissance rapide, symbole de la bonne compréhension et intégration du processus de notification par les entreprises luxembourgeoises, grâce notamment aux importants travaux de communication et de sensibilisation de la CNPD pendant la phase d'entrée en application du RGPD, on note une relative stabilité à travers le temps.

# L’humain au cœur de la problématique :




L'erreur humaine (acte interne non malveillant) est un facteur majeur de violations de données dans le contexte du RGPD, représentant plus de 50 % des cas. Elle peut survenir de diverses manières, comme des fautes de frappe, l'envoi d'e-mails au mauvais destinataire, la perte de matériel informatique, ou l'utilisation de mots de passe faibles. Les erreurs humaines se produisent souvent à cause de procédures inappropriées, d'un manque de formation ou de supervision, ou de la fatigue des employés.

Pour minimiser ces risques, les entreprises peuvent mettre en place des mesures telles que des programmes de formation réguliers sur la sécurité des données, des processus de vérification stricts, des contrôles d'accès, et des systèmes de sécurité renforcés. En instaurant une culture de la sécurité et en sensibilisant les employés aux risques, les entreprises peuvent réduire considérablement les violations de données dues à des erreurs humaines.

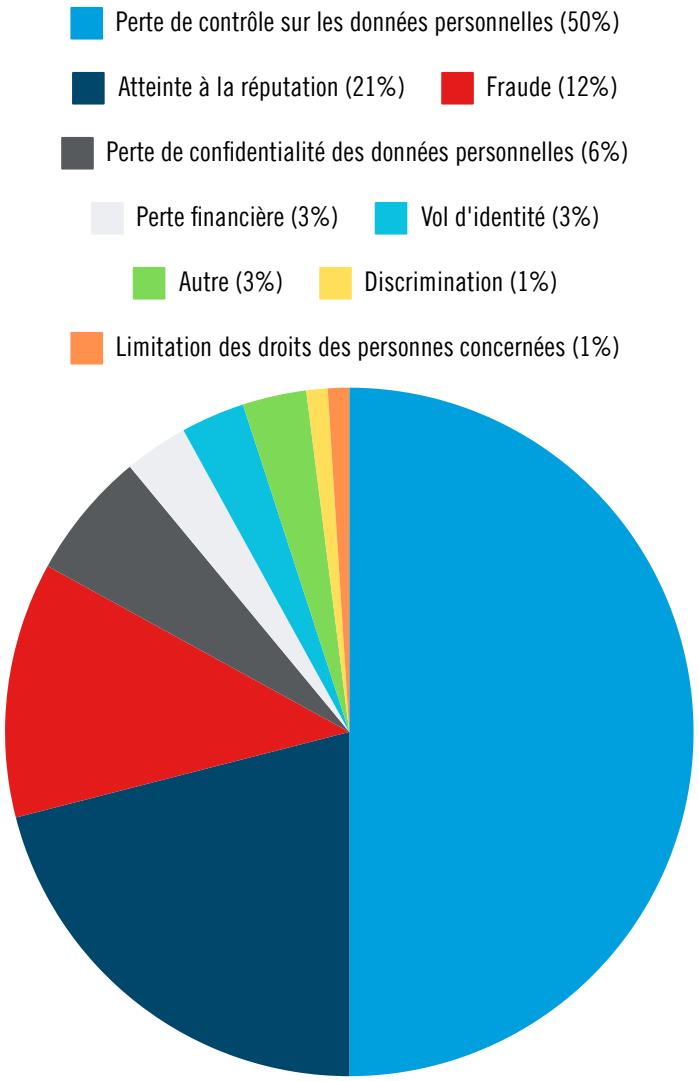
# Pour quelles conséquences?

La **perte de contrôle sur les données personnelles** fait référence à une situation où des individus ne peuvent plus décider comment leurs informations personnelles sont utilisées, partagées ou stockées. Cela peut se produire lorsqu'une entité, comme une entreprise ou une organisation, perd ou compromet des données personnelles, exposant ainsi ces données à un accès non autorisé.

L'**atteinte à la réputation** désigne le dommage causé à l'image publique, à la confiance, ou à la crédibilité d'une personne en raison de la divulgation ou de l'utilisation inappropriée de données personnelles. Cela peut avoir des effets très négatifs, tant sur le plan professionnel que personnel : diffamation, atteinte à la vie privée, impact sur les relations professionnelles.

Le **risque de fraude** dans le contexte des violations de données personnelles fait référence à la possibilité que des individus ou des organisations utilisent des données personnelles volées ou compromises pour commettre des actes frauduleux. Une telle fraude peut inclure diverses formes, allant p.ex. du vol d'identité jusqu'à la fraude financière.

## Nature de l'impact potentiel sur les personnes concernées




Les trois principaux types de violations de données présentent des caractéristiques et des implications très différentes, ce qui signifie que les solutions pour les traiter doivent également être adaptées à chaque cas. Cette diversité rend le travail de la CNPD complexe, car elle doit comprendre une gamme de risques variés et proposer des conseils adaptés à chaque situation.

L'accompagnement des entreprises nécessite une expertise approfondie dans différents domaines, ainsi qu'une flexibilité pour s'ajuster aux spécificités de chaque cas. La CNPD doit ainsi jongler entre des approches variées pour aider les entreprises à naviguer dans un paysage de risques très diversifié.

# Au-delà des chiffres …

Le premier constat que l'on peut faire au moment de ce bilan est **la prise au sérieux par les entreprises de l'obligation de notification**. Les organisations ont fourni des efforts d'adaptation de leur fonctionnement, mais aussi de moyens, de sensibilisation.

Cette progression évolue parallèlement avec la **reconnaissance croissante de l'importance du rôle du DPO** dans une organisation. La perception par les organisations de cette obligation à aussi évolué. Au départ une contrainte, elles ont su en tirer profit en premier lieu car chaque notification est une occasion de comprendre les causes profondes des incidents, les solutions concrètes pour y remédier.

Cette formalisation des problèmes, qui plus est, dans un contexte juridique potentiellement sanctionnable, permet ainsi aux départements concernés d'avoir les arguments nécessaires à l'obtention des budgets permettant de solutionner ces problématiques.

Les organisations ont beaucoup **évolué dans le rapport qu'elles ont avec les autorités de régulation**, développant de nouvelles compétences juridiques et de compliance.

Enfin, elles ont su **mettre en avant la transparence** dans leur communication client, gage de crédibilité.

# Et maintenant ?

Pour l'avenir, la préoccupation des entreprises concerne l'évolution rapide de la technologie, comme l'intégration de l'intelligence artificielle dans les processus de gestion et de production ainsi que la prolifération continue des objets connectés, posant ainsi de nouveaux risques en matière de protection des données, et obligeant les entreprises à rester vigilantes et à adapter sans cesse leur processus et leur organisation.


Dans ce contexte, la CNPD, en dehors de sa mission de surveillance d'une autorité de contrôle, continuera à déployer également beaucoup de moyens pour sensibiliser et guider les entreprises pour leur faciliter la mise en conformité.

CNPD
COMMISSION NATIONALE POUR LA PROTECTION DES DONNÉES

Commission nationale pour la protection des données
15, Boulevard du Jazz I L-4370 Belvaux
Tél. : (+352) 26 10 60 - 1
www.cnpd.lu

Juillet 2024