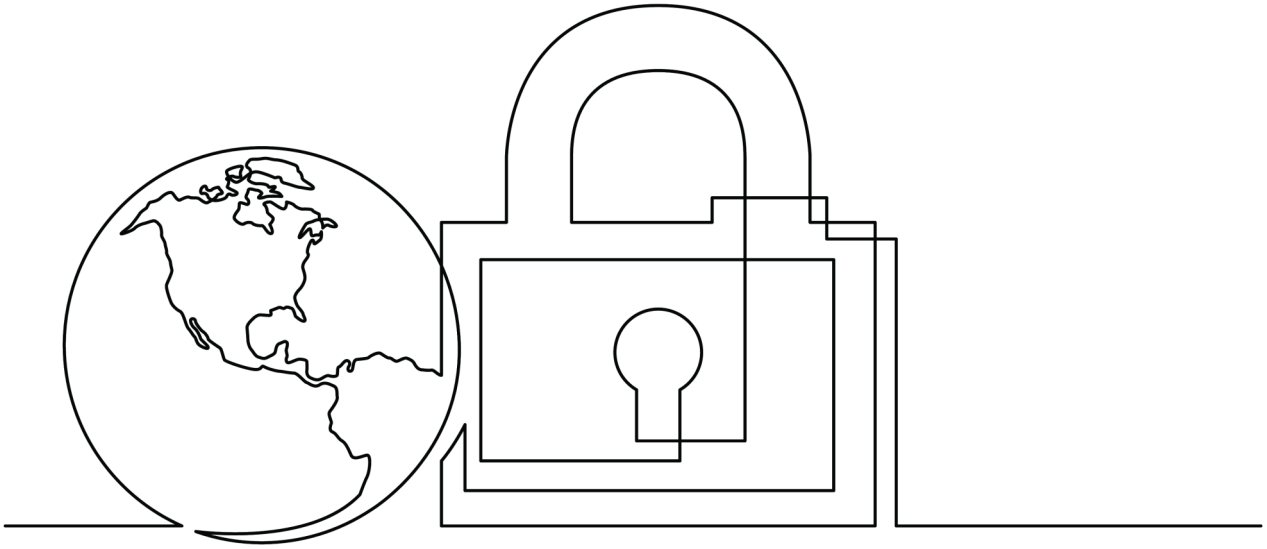


Sécurité des données

L’application du RGPD en Europe

Mathias Avocats

Version : Mai 2020

INTRODUCTION

Deux années se sont écoulées depuis l'entrée en application du Règlement général sur la protection des données (RGPD).

C'est l'occasion pour Mathias Avocats de mettre en lumière les enjeux liés à la sécurité des données à caractère personnel, en revenant sur les décisions des autorités de contrôle européennes en la matière.

L'actualité se fait régulièrement l'écho d'incidents de sécurité et d'attaques informatiques protéiformes auxquels font face les organismes, quels que soient leur taille, leur statut et le secteur dans lequel ils évoluent.

Les décideurs ainsi que tous les acteurs de la sécurité (CISO, DSI, DPO, etc.) ont donc tout intérêt à se tenir informés des analyses menées par les autorités de contrôle. Ces dernières sont riches d'enseignements s'agissant tant des mesures de sécurité attendues, que des mesures constitutives d'un manquement au RGPD. Elles participent donc à une gestion des risques.

Cette veille nous paraît indispensable, a fortiori en temps de crise, afin de vous permettre d'évaluer la pertinence, la robustesse des dispositifs de sécurité mis en place au sein de vos organismes, ainsi que les éventuels axes d'amélioration.

La connaissance de la « jurisprudence » permet à tous les acteurs d'améliorer leurs pratiques, qu'il s'agisse de mettre en conformité un organisme, de l'auditer ou de le défendre devant les autorités de contrôle.

Nous vous souhaitons ainsi une bonne lecture,

Dans l'attente de partager notre expertise avec vous,

Amicalement,

Garance Mathias

Avocat Associée

L’obligation d’assurer la sécurité des données

La sécurité des données à caractère personnel fait l’objet d’une section à part entière au sein du RGPD. Si la disposition phare en matière de sécurité est sans aucun doute l’article 32, l’obligation d’assurer la sécurité des données du responsable du traitement et du sous-traitant apparaît en filigrane dans de nombreuses autres dispositions du RGPD.

Ce fil conducteur doit rester présent dans toute démarche de mise en conformité et, comme le rappelle **le considérant 78**, le responsable du traitement est tenu d’adopter des mesures techniques et organisationnelles appropriées pour garantir que les exigences du règlement sont respectées.

Afin de démontrer cette conformité, il convient :

1. D’adopter des règles internes,
2. De mettre en œuvre des mesures respectant les principes de protection des données dès la conception et de protection des données par défaut, et
3. De tenir compte du droit à la protection des données et de l’état de l’art lors de l’élaboration, la conception, la sélection, l’utilisation d’applications, de services ou de produits qui reposent sur le traitement de données à caractère personnel ou traitent des données pour remplir leurs fonctions.

L’obligation d’assurer la sécurité des données

Article 32 du RGPD

« 1. Compte tenu de **l'état des connaissances**, **des coûts de mise en œuvre** et **de la nature, de la portée, du contexte et des finalités du traitement** ainsi que des **risques**, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, **le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque**, y compris entre autres, selon les besoins :

a) la pseudonymisation et le chiffrement des données à caractère personnel ;

b) des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;

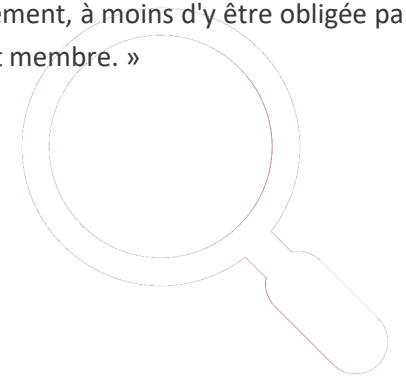
c) des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ;

d) une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

2. **Lors de l'évaluation du niveau de sécurité approprié**, il est tenu compte en particulier des **risques** que présente le traitement, **résultant notamment de la destruction, de la perte, de l'altération, de la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou de l'accès non autorisé à de telles données, de manière accidentelle ou illicite**.

3. L'application d'un code de conduite approuvé comme le prévoit l'article 40 ou d'un mécanisme de certification approuvé comme le prévoit l'article 42 peut servir d'élément pour démontrer le respect des exigences prévues au paragraphe 1 du présent article.

4. Le responsable du traitement et le sous-traitant prennent des mesures afin de garantir que toute personne physique agissant sous l'autorité du responsable du traitement ou sous celle du sous-traitant, qui a accès à des données à caractère personnel, ne les traite pas, excepté sur instruction du responsable du traitement, à moins d'y être obligée par le droit de l'Union ou le droit d'un État membre. »



L'obligation d'assurer la sécurité des données

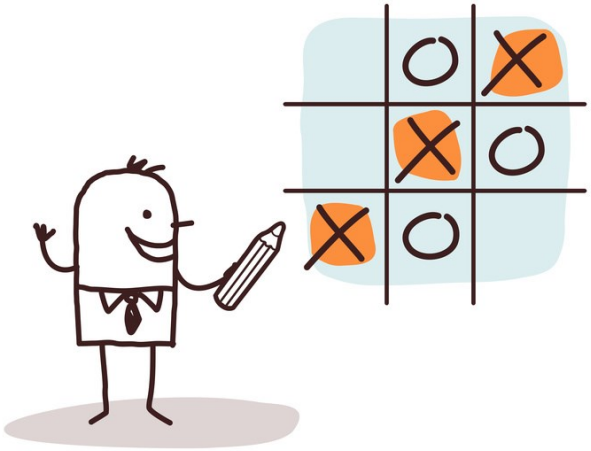
Le responsable du traitement **et** le sous-traitant doivent assurer la sécurité et la confidentialité des données

Les mesures de sécurité doivent être **adaptées et proportionnées** aux risques

Le responsable du traitement **et** le sous-traitant doivent veiller à ce que leurs collaborateurs n'aient accès qu'aux données nécessaires à leurs fonctions et les traitent uniquement dans ce cadre-là (vérifications régulières des accès, de l'utilisation des données, etc.)

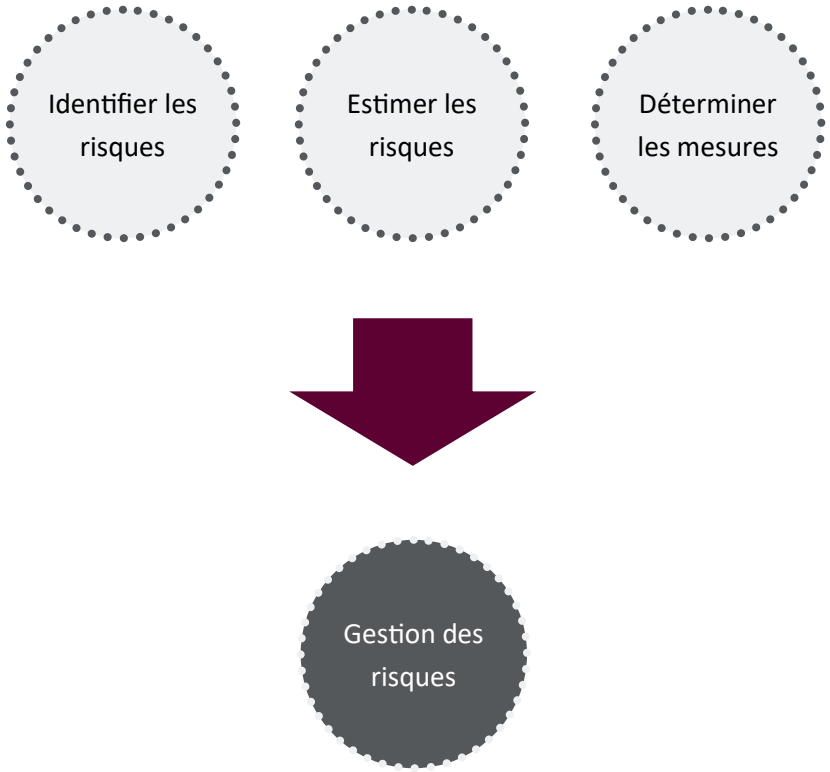
Le RGPD ne définit pas les mesures de sécurité à mettre en œuvre

Les mesures de sécurité doivent être documentées et matérialisées



L'obligation d'assurer la sécurité des données

L'approche par les risques promue par le RGPD



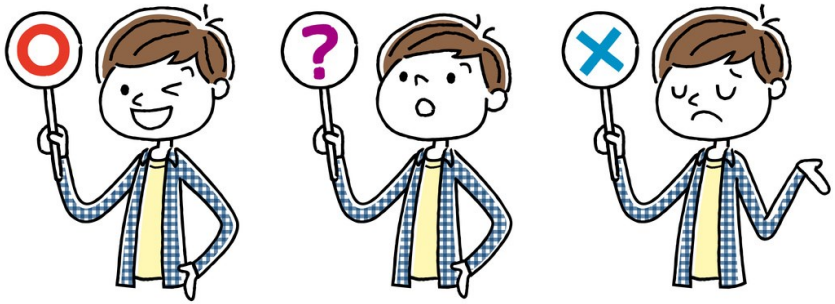
La typologie des risques

Les risques concernent tout incident de sécurité qui porte atteinte principalement à la **confidentialité**, à l'**intégrité** ou à la **disponibilité** des données à caractère personnel.

1. La confidentialité : seules les personnes autorisées peuvent avoir accès aux données. Tout autre accès doit être empêché.
2. L'intégrité : Les données ne doivent pas être altérées de façon fortuites, intentionnelles ou non.
3. La disponibilité : L'accès aux données doit être permanent, sans dysfonctionnements non planifiés.

Source : Cnil, Sécurité des données : mesures d'hygiène pour protéger votre système d'information

Pays	Décision	Manquements relevés	Faits reprochés
Chypre 	**Sanction pécuniaire de 5 000 euros** **7 novembre 2018**	Manquement à l'obligation d'assurer la sécurité et la confidentialité des données	Un patient a déposé une plainte auprès du Commissaire à la protection des données parce que sa demande d'exercice du droit d'accès aux données la concernant n'avait pas été satisfaite par un hôpital. Ce dernier **n'avait pas pu trouver le fichier contenant les données du patient.** Le Commissaire a infligé une amende de 5 000 € compte tenu de la perte du fichier. Pour limiter le montant de l'amende, le Commissaire a pris en compte les mesures prises par l'hôpital pour améliorer la situation. *La source est disponible ici.*



L'obligation d'assurer la sécurité des données

L'état de l'art est l'état des connaissances relatives à la sécurité des systèmes d'information à un instant donné.

⇒ L'article 32, 1 du RGPD fait référence à « l'état des connaissances ».

L'importance de la formation

Pour que les équipes opérationnelles soient à l'état de l'art de la sécurité des systèmes d'information, l'ANSSI recommande que les équipes opérationnelles suivent, à leur prise de poste puis à intervalles réguliers, des formations sur :

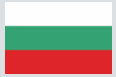
* La législation en vigueur
* Les principaux risques et menaces
* Le maintien en condition de sécurité
* L'authentification et le contrôle d'accès
* Le paramétrage fin et le durcissement des systèmes
* Le cloisonnement réseau
* La journalisation

Il est également recommandé d'insérer une stipulation contractuelle spécifique dans les contrats de prestation pour garantir une formation régulière à la sécurité des systèmes d'information du personnel externe et notamment les infogérants.

Source : ANSSI, Guide d'hygiène numérique https://www.cybermalveillance.gouv.fr/

SOMMAIRE

LES ACTES DE MALVEILLANCE—CYBERATTAQUES

Pays	Décision	Manquements relevés	Faits reprochés
Bulgarie 	**Sanction pécuniaire d'environ 2.5 millions d'euros** **29 août 2019**	Manquement à l'obligation d'assurer la sécurité et la confidentialité des données	Le 15 juillet 2019, un **hacker** a réussi à pénétrer **les serveurs** de l'Agence nationale des impôts bulgare et à télécharger les données personnelles de plus de 5 millions de citoyens bulgares. Une partie des informations piratées a été divulguée aux médias locaux. À la suite de cet incident, l'autorité a diligenté un contrôle au sein de l'Agence et constaté l'insuffisance des mesures techniques et organisationnelles pour assurer la sécurité des données. Elle a ainsi prononcé une sanction pécuniaire d'environ 2,5 millions d'euros à l'encontre de l'Agence. *La source est disponible ici.*

Pays	Décision	Manquements relevés	Faits reprochés
Pologne 	**Sanction pécuniaire de 645 000 euros** **10 septembre 2019**	Manquement au principe de confidentialité des données (*article 5, 1, f) du RGPD*)	Un site de e-commerce a fait l'objet d'une violation de données ayant impacté environ 2.2 millions de personnes. Ont été divulgués les noms, prénoms, numéros de téléphones, adresses postales et électroniques des personnes concernées. De surcroit, pour environ 35 000 personnes, les informations divulguées se rapportaient également à leurs dossiers de demande de prêt échelonnés. Ces dossiers comprenaient le numéro d'identité personnel, le numéro de série des documents d'identité, le niveau de formation, l'adresse officielle, les sources de revenus, le revenu net, le statut marital des personnes concernées, ainsi que les dépenses du foyer et les sommes payées se rapportant à des remboursements de crédits ou au paiement de pensions alimentaires. L'autorité a relevé **l'absence de procédures appropriées afin de gérer l'émergence de trafic réseau inhabituel**. Elle a estimé que la carence de la société à mettre en œuvre les moyens techniques adéquats avait permis l'accès non autorisé aux données des clients et constituait un manquement au principe de confidentialité. L'autorité a également relevé que les mesures d'authentification mises en œuvre étaient inefficaces. Le contrôle de l'autorité a révélé que la violation était également intervenue en raison d'une surveillance ineffective des risques potentiels. L'autorité a relevé d'autres manquements de la société mais indique que la sanction a été prononcée en raison de l'absence de garanties techniques appropriées et de mesures organisationnelles permettant de **surveiller les risques potentiels associés à des comportements atypiques en ligne**. Lors de la détermination de la sanction, l'autorité a conclu que la violation était d'une importance considérable, présentait un caractère sérieux et avait impacté un large nombre de personnes. Elle a également souligné que la violation présentait un risque important pour les personnes concernées de subir des répercussions dommageables, notamment le vol d'identité. Pour déterminer le montant de la sanction, l'autorité a également déclaré avoir tenu compte de certaines circonstances atténuantes telles que les actions entreprises pour mettre fin au manquement, la coopération avec l'autorité et le fait que la société n'avait encore jamais enfreint la réglementation en matière de données personnelles. *La source est disponible ici.*

Assurer la sécurité des serveurs

Le protocole TLS est une solution permettant la protection des flux réseau. Il est utilisé non seulement pour sécuriser le trafic lié aux sites web et à la messagerie électronique mais également pour la protection de flux d'infrastructures internes.

Pour aller plus loin : ANSSI, Recommandations de sécurité relatives à TLS

⇒ Mettre en place des habilitations spécifiques pour l'accès aux outils et interfaces d'administration

⇒ Adopter une politique spécifique de mots de passe pour les administrateurs . La Cnil recommande de changer les mots de passe au minimum lors de chaque départ d'un administrateur et en cas de suspicion de compromission.

⇒ Utiliser des comptes nominatifs pour l'accès aux bases de données et créer des comptes spécifiques à chaque application

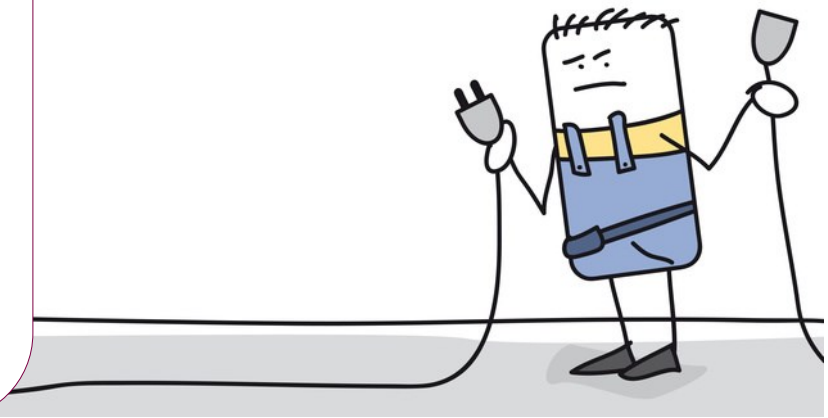
⇒ Installer les mises à jour critiques sans délai des systèmes d'exploitations et des applications. A cette fin, il est possible de programmer une vérification automatique hebdomadaire

⇒ Mettre en œuvre des mesures contre les attaques par injection de code SQL, de scripts, etc.

⇒ Mettre en œuvre le protocole TLS ou un protocole assurant le chiffrement et l'authentification, au minimum pour tout échange de données sur internet et vérifier sa bonne mise en œuvre par des outils appropriés.

A éviter !

- L'utilisation de services non sécurisés, tels que les flux ou les authentifications en clair
- L'utilisation de serveurs hébergeant les bases de données pour d'autres fonctions, comme la navigation sur des sites web ou pour l'accès à la messagerie électronique
- Placer les bases de données sur un serveur directement accessible depuis Internet
- L'utilisation de comptes utilisateurs génériques, partagés entre plusieurs utilisateurs



Source : CNIL, Guide de la sécurité des données personnelles

Assurer la sécurité des serveurs

Quid de la sécurité physique ?

Des mécanismes de sécurité physique doivent faire partie intégrante de la sécurité des systèmes d'information et être à l'état de l'art pour éviter qu'ils ne soient contournés aisément par un attaquant.

L'ANSSI recommande d'identifier les mesures de sécurité physique adéquates et de sensibiliser continuellement les utilisateurs aux risques engendrés par le contournement des règles.

⇒ L'accès aux salles serveurs et aux locaux techniques doivent être contrôlés à l'aide de serrures ou de mécanismes de contrôle d'accès par badge.

⇒ Les accès non accompagnés des prestataires extérieurs aux salles serveurs et aux locaux techniques sont à proscrire, sauf s'il est possible de tracer strictement les accès et de limiter ces derniers en fonction des plages horaires.

⇒ Une revue des droits d'accès doit être réalisée régulièrement afin d'identifier les accès non autorisés.

⇒ Les prises réseau se trouvant dans des zones ouvertes au public doivent être restreintes ou désactivées afin d'empêcher un attaquant de gagner facilement l'accès au réseau de l'entreprise.

Source : ANSSI, Guide d'hygiène informatique

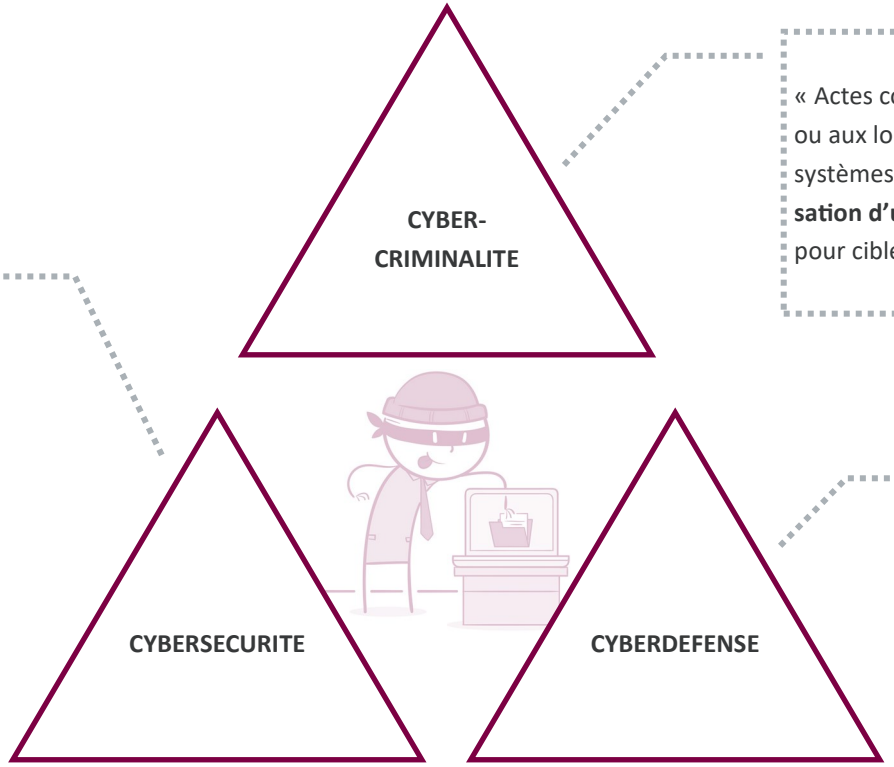
Pays	Décision	Manquements relevés	Faits reprochés
Grèce 	**Avertissement** **9 novembre 2018**	Manquement à l'obligation d'assurer la sécurité et la confidentialité des données	Un groupe de sociétés a été victime d'une **attaque informatique** affectant la confidentialité des données à caractère personnel qu'il traite. Le groupe a informé l'autorité de contrôle et les personnes concernées de la violation de données dans les délais après en avoir eu connaissance. Toutefois, l'autorité de contrôle a constaté qu'il n'avait pas mis en œuvre les mesures techniques et organisationnelles de manière à garantir la sécurité du traitement. Elle a prononcé un avertissement à l'encontre du groupe notamment pour défaut d'installation de mises à jour du logiciel utilisé en matière de sécurité, défaut de mise en place de mécanismes adéquats pour la détection des attaques de sécurité, et défaut de procédures visant à évaluer régulièrement les mesures de sécurité.
Allemagne 	**Sanction pécuniaire de 20 000 euros** **21 novembre 2018**	Mesures techniques et organisationnelles insuffisantes pour garantir la sécurité des données (*article 32, 1 du RGPD*)	Un réseau social a fait l'objet d'une **cyberattaque** en septembre 2018. La société qui exploite le réseau social a communiqué la violation aux personnes concernées et a notifié l'autorité de contrôle dans les délais qui lui étaient impartis. Toutefois, il a été relevé que les mots de passe des utilisateurs étaient conservés en clair dans la base de données de la société, qui a été copiée par les attaquants. Pour l'autorité, il s'agit d'une non-conformité à l'obligation du réseau social de définir des mesures de sécurité adéquates au regard des risques. L'autorité a toutefois déclaré avoir pris en compte, la « coopération exemplaire » dont a fait preuve la société, dans la détermination du montant de la sanction pécuniaire. En effet, la société a été transparente vis-à-vis de l'autorité de contrôle et des personnes concernées, réactive, et a rapidement effectué des investissements financiers importants pour implémenter les correctifs de sécurité nécessaires.

Pays	Décision	Manquements relevés	Faits reprochés
Royaume-Uni 	**Projet de sanction pécuniaire d'environ 204 millions d'euros** **8 juillet 2019**	Manquement à l'obligation d'assurer la sécurité et la confidentialité des données	Une compagnie aérienne a été victime en septembre 2018 d'un incident de sécurité ayant entrainé **le détournement d'une partie du trafic destiné au site internet institutionnel de la société vers un site frauduleux**. Grâce à ce site frauduleux, **les attaquants** ont pu avoir accès aux données à caractère personnel d'environ 500 000 utilisateurs. En tant qu'autorité chef de file, l'ICO a effectué un contrôle au cours duquel elle a relevé que des données relatives à la connexion, aux cartes de paiement, aux réservations de voyage, ainsi que les noms et les adresses des utilisateurs ont notamment été compromises. L'ICO a publié un projet de décision au terme duquel elle envisage de prononcer une sanction pécuniaire d'environ 204 millions d'euros à l'encontre de la compagnie aérienne. L'ICO a précisé que la compagnie a coopéré au cours du contrôle et a amélioré ses outils de sécurité. Enfin, l'autorité a annoncé qu'elle examinera les observations de la compagnie et d'autres autorités de protection des données concernées avant de prendre sa décision finale. *La source est disponible ici.*

Gestion des risques de cyberattaque

« État recherché pour un système d'information lui permettant de **résister à des événements** issus du cyberespace susceptibles de compromettre **la disponibilité, l'intégrité ou la confidentialité** des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles.

La cybersécurité fait appel à des techniques de sécurité des systèmes d'information et s'appuie sur **la lutte contre la cybercriminalité** et sur **la mise en place d'une cyberdéfense**. »



« Actes contrevenants aux traités internationaux ou aux lois nationales, utilisant les réseaux ou les systèmes d'information comme **moyens de réalisation d'un délit ou d'un crime**, ou les ayant pour cible. »

« Ensemble des mesures techniques et non techniques permettant à un État de **défendre dans le cyberespace les systèmes d'information** jugés essentiels. »

Glossaire de l'ANSSI

Gestion des risques de cyberattaque

6 étapes clés pour gérer les risques informatiques

- **Définir un cadre de gouvernance des risques**
- **Comprendre son activité numérique**
- **Connaitre son seuil d'acceptation des risques**
- **Construire ses pires scénarios de risque**
- **Définir sa stratégie de sécurité numérique et de valorisation**
- **Mettre en place des polices d'assurance adaptées**

Pour aller plus loin : ANSSI, Maîtrise du risque numérique

Pays	Décision	Manquements relevés	Faits reprochés
Danemark 	**Proposition de sanction pécuniaire d'environ 13 408 euros pour la première municipalité** **Proposition de sanction pécuniaire d'environ 6 704 euros pour la seconde municipalité** **10 mars 2020**	Manquement à l'obligation d'assurer la sécurité et la confidentialité des données	L'autorité danoise a été notifiée par deux municipalités d'une violation de données à caractère personnel suite au vol d'ordinateurs contenant des données. La première violation a résulté du vol d'un ordinateur au sein même de la mairie, contenant des données personnelles relatives à 20 620 habitants de la commune, dont des données dites sensibles. La seconde violation est intervenue suite au **vol d'un ordinateur** qui se trouvait dans la voiture d'un employé de la mairie. Cet appareil contenait les informations d'environ 1 600 employés de la municipalité. Aucun de ces ordinateurs **n'était protégé par des mesures de chiffrement** et la perte des données par les municipalités soulevait un risque injustifié pour les citoyens. L'autorité a estimé que ces failles de sécurité étaient la conséquence d'un niveau de sécurité insuffisant ce qui générait des risques importants pour tous les citoyens des communes concernées. Le président de l'autorité a souligné que les municipalités traitent un grand nombre de données y compris des données sensibles, sans qu'il soit possible pour les citoyens de s'y opposer. Ainsi, il considère que les municipalités ont une responsabilité particulière à l'égard de la protection des données qu'elles traitent. L'autorité a signalé ces violations à la police et a proposé des sanctions pécuniaires à l'encontre des municipalités. *La source est disponible ici.*

Il est rappelé que le système juridique danois ne permet pas d'imposer des amendes administratives comme prévu par le RGPD. L'amende doit être prononcé par une juridiction nationale compétente autre que l'autorité de contrôle de protection des données sous la forme d'une sanction pénale (*RGPD, considérant 151*).

Pays	Décision	Manquements relevés	Faits reprochés
Hongrie 	**Sanction pécuniaire d'environ 35 000 euros** **21 mars 2019**	Absence de notification d'une violation de données à l'autorité de contrôle (*article 33 du RGPD*) et absence de communication aux personnes concernées (*article 34 du RGPD*)	L'autorité hongroise a reçu une plainte selon laquelle une base de données contenant les données à caractère personnel des adhérents d'un parti politique étaient librement accessibles sur un forum de hackers. Cette base de données contenait les adresses email, les noms complets, les identifiants de connexion ainsi que les mots de passe des utilisateurs. Ces **mots de passe n'étaient pas chiffrés de manière sécurisée** (chiffrement MD5). Cette base de données a été compromise et divulguée grâce à une **vulnérabilité SQLi** de la page internet exploitée par un hackeur. Le parti politique avait été informé de la violation par le hackeur lui-même. Toutefois, cette entité mais n'a informé ni l'autorité de contrôle hongroise, ni les personnes concernées (environ 6000 personnes). Il faisait valoir qu'il n'était pas tenu de notifier la violation parce que les données en question n'étaient pas mises à jour. L'autorité a estimé que le fait que les données ne soient pas mises à jour n'avait aucune incidence sur l'obligation de notification prévue par le RGPD. Par ailleurs, elle a considéré que l'incident présentait un risque élevé car il avait affecté les données d'adhérents ou d'anciens adhérents du parti politique. En outre, elle précise que les données en question relèvent de catégories particulières dès lors qu'elles révèlent les opinions politiques des personnes concernées, ce qui constitue une circonstance aggravante. L'autorité relève également que le parti politique utilisait une technologie de chiffrement obsolète pour sécuriser les mots de passe, ce qui représente également un facteur de risques graves pour les droits et libertés des individus. Elle indique que la disponibilité de ces informations est susceptible d'entrainer d'autres incidents sur les services en ligne utilisés par les personnes concernées. L'autorité a prononcé une sanction d'environ de 35 000 euros pour absence de notification d'une violation de données présentant un risque élevé. *La source est disponible ici.*

Pays	Décision	Manquements relevés	Faits reprochés
Lituanie 	**Sanction pécuniaire de 61 500 euros** **16 mai 2019**	• Manquement aux principes de minimisation des données, de limitation de la conservation et d'intégrité et de confidentialité des données (*article 5,1 du RGPD*) • Mesures techniques et organisationnelles insuffisantes pour garantir la sécurité du traitement (*article 32,1 du RGPD*) • Manquement à l'obligation de notification de la violation de données (*article 33 du RGPD*)	Les données à caractère personnel des clients d'une société de paiement électronique ont été rendues publiques sur un site Internet pendant au moins deux jours en juillet 2018. 9 000 captures d'écran présentant des informations sur les opérations de paiement des clients étaient également accessibles sur ledit site. L'origine de cette violation de données n'est pas connue de manière certaine. L'autorité de contrôle constate que la société n'a pas notifié la violation de données à l'autorité de contrôle et aux personnes concernées. Par ailleurs, elle précise que la société n'avait pas mis en œuvre les mesures techniques et organisationnelles suffisantes pour garantir la sécurité des données. En effet, un seul salarié s'occupait de la sécurité des systèmes d'information de la société. De plus, **les données n'étaient pas chiffrées** et il n'y avait pas de mesures permettant de contrôler l'accès à celles-ci. Par ailleurs, la société traitait de manière régulière une quantité excessive de données. Outre les données relatives aux opérations de paiement (nom, prénom, identifiant du client, numéro de compte etc.), la société traitait les factures électroniques (dates, données des expéditeurs, montants), les messages non lus (dates, sujets et une partie des textes) et d'autres informations sur les prêts, les pensions de retraite et les cartes de crédit de ses clients. En ce qui concerne la durée de conservation des données, bien que celle-ci ait été fixée à dix minutes, la société avait conservé les données pendant 216 jours. En prenant en compte tous ces éléments, l'autorité de contrôle a prononcé une amende de 61 500 euros à l'encontre de la société. Il s'agit de la première sanction prononcée en application du RGPD en Lituanie. Cette sanction a fait l'objet d'une concertation avec l'autorité de protection de Lettonie.

Chiffrer les données pour assurer leur confidentialité

Recommandations de la Cnil :

⇒ L'utilisation des algorithmes :

* AES ou AES-CBC pour le chiffrement symétrique
* RSA-OAEP pour le chiffrement asymétrique

⇒ La protection des clés en établissant des droits d'accès et des mots de passe.

⇒ Le recours à des solutions de chiffrement certifiées ou qualifiées par l'ANSSI ou encore aux logiciels VeraCrypt et GNU Privacy Guard.

⇒ L'utilisation des algorithmes SHA-256, SHA-512 ou SHA-3 pour la fonction de hachage.

A éviter !

Utilisation de technologies obsolètes comme les chiffrements DES et 3DES ou les fonctions de hachage MD5 et SHA1 .

Le chiffrement est le « *procédé de cryptographie grâce auquel on souhaite rendre la compréhension d'un document impossible à toute personne qui ne possède pas la clé de (dé)chiffrement* » (Définition de **l'ANSSI,** *Guide des bonnes pratiques de l'informatique).*

Source : Cnil, Guide de la sécurité des données personnelles

Pays	Décision	Manquements relevés	Faits reprochés
Royaume-Uni 	**Projet de sanction pécuniaire d'environ 110 millions euros** **9 juillet 2019**	Manquement à l'obligation d'assurer la sécurité et la confidentialité des données	L'autorité a procédé à un contrôle suite à un incident de sécurité notifié par un groupe hôtelier en novembre 2018. Des données personnelles relatives à environ 339 millions de clients dans le monde, dont 30 millions de résidents de l'Union européenne et 7 millions de résidents du Royaume-Uni, avaient été divulguées. Il semblerait que la vulnérabilité ait pour origine la compromission des systèmes informatiques d'un groupe hôtelier tiers en 2014. Ce groupe avait été acheté en 2016 par un autre groupe qui n'avait constaté la violation de données qu'en 2018. Lors d'un contrôle effectué en tant qu'autorité chef de file, l'ICO a constaté que **le groupe hôtelier n'avait pas effectué les vérifications nécessaires lors de l'acquisition de la chaîne hôtelière** et n'avait pas pris les mesures nécessaires pour sécuriser ses systèmes d'information. La présidente de l'autorité a souligné que **le principe de responsabilité inclut tant la réalisation de vérifications adéquates lors de l'acquisition de sociétés que la mise en œuvre de mesures permettant de déterminer non seulement quelles données ont été acquises mais également la manière dont elles sont protégées**. L'ICO a publié un projet de décision au terme duquel elle envisage de prononcer une sanction pécuniaire d'environ 110 millions d'euros. L'ICO a souligné la coopération dont le groupe a fait preuve au cours du contrôle et l'amélioration de ses mesures de sécurité. Enfin, l'autorité a annoncé qu'elle examinera les observations du groupe et d'autres autorités de protection des données concernées avant de prendre sa décision finale. *La source est disponible ici.*

Les diligences et vérifications de l'investisseur (acquéreur)

IDENTIFIER LES RESPONSABILITES

⇒ Les données acquises ont-elles été collectées conformément à la réglementation ?

⇒ Quelle est la base légale retenue par l'entité pour traiter des données personnelles ? Dispose-t-elle d'une documentation en conformité avec la règlementation ?

IDENTIFIER LES DONNEES PERSONNELLES ACQUISES LORS DE L'OPERATION

⇒ Quel est le type et le volume de données personnelles traitées ? Notamment, s'agit-il de catégories particulières de données ?

⇒ Comment l'entité collecte, utilise, partage, stocke et purge-t-elle les données personnelles en sa possession ?

⇒ L'entité procède-t-elle à des transferts de données en dehors de l'Union européenne ? Sur quel fondement ces transferts s'opèrent-ils ?

DEMANDER TOUTE DOCUMENTATION NECESSAIRE

Exemples de documents à demander :

* le politique de sécurité des systèmes d'information,
* la charte informatique,
* le registre des violations de données,
* le registre des incidents de sécurité,
* les copies de notification des violations à l'autorité de contrôle et de communication aux personnes concernées,
* le plan de remédiation et le calendrier de mise en œuvre en cas de violation de données,
* les conditions de conservation, archivage et stockage des documents papiers, etc.

PROCEDER A LA SECURISATION DES SYSTEMES D'INFORMATION, LE CAS ECHEANT

⇒ Quelles actions de mise en conformité devront-être réalisées à l'issue de l'acquisition ?

⇒ Quelles sont les actions prioritaires ?

LES ERREURS DE CONCEPTION DES SYSTEMES D'INFORMATION

Pays	Décision	Manquements relevés	Faits reprochés
Suède 	**Sanction pécuniaire d'environ 18 700 euros** **28 avril 2020**	Manquement aux obligations relatives à la notification et à la communication des violations de données	Le National Government Service Centre (NGSC) propose des services de coordination de l'administration des agences gouvernementales (gestion des salaires, e-commerce). L'autorité suédoise a initié un contrôle au sein de cette entité à la suite de multiples notifications de violations de données, résultant d'une **erreur du système informatique pour la gestion des salaires**. Cette erreur permettait l'accès non autorisé aux données personnelles du personnel des autorités ayant recours aux services du NGSC ainsi que du personnel du NGSC lui-même. Le contrôle de l'autorité a révélé que le NGSC avait tardé à informer les agences gouvernementales concernées de la présence de cette erreur ainsi qu'à notifier à l'autorité la violation des données. L'entité a pris près de 5 mois à informer les agences et 3 mois à notifier l'autorité de contrôle. L'autorité a souligné que l'entité agissant en qualité de sous-traitant, il était important d'informer les responsables de traitement dans les meilleurs délais après la découverte d'une violation de données afin de leur permettre de la signaler et de prendre les actions nécessaires pour réduire les risques associés. Par ailleurs, la documentation de la violation réalisée par le NGSC ne faisait pas mention des informations relatives aux données et aux personnes concernées par la violation appartenant à son propre personnel. L'autorité a ordonné à la NGSC de mettre en place les procédures internes pour la documentation des violations des données et de vérifier qu'elles soient respectées. *La source est disponible ici.*

Les obligations de sécurité incombant aux sous-traitants

Au sens du RGPD, le sous-traitant est une personne physique ou morale qui offre une prestation de traitement de données à caractère personnel pour le compte d'un autre organisme, le responsable du traitement. Il doit être lié à ce dernier par un contrat répondant aux exigences de l'article 28 du RGPD. Au regard de l'article 32 du RGPD, le sous-traitant est en outre soumis à une obligation de sécurité au même titre que le responsable du traitement.

Quelles sont les stipulations contractuelles à prévoir ?

⇒ Une obligation de transparence et de traçabilité

- Une telle stipulation pourra permettre de déterminer la procédure d'agrément par le responsable du traitement de sous-traitants ultérieurs. Les parties pourront convenir de la nécessité d'une autorisation expresse du responsable du traitement ou simplement de la faculté de celui-ci de s'opposer au recours à certains sous-traitants ultérieurs.
- Cette stipulation devra également prévoir l'obligation pour le sous-traitant de mettre à la disposition du responsable du traitement toute information qui lui serait nécessaire pour démontrer le respect de ses obligations ou permettre la conduite d'audits.

⇒ L'implémentation des principes de protection des données dès la conception et par défaut dans les pratiques du sous-traitant.

⇒ Une obligation de garantir la sécurité des données traitées

⇒ Une obligation d'assistance, d'alerte et de conseil

- Une telle stipulation pourrait organiser les relations des parties dans le cadre de violation des données en précisant les informations qui devront être communiquées au responsable du traitement et le timing de cette information. Il pourrait également être envisagé de permettre au sous traitant de notifier la violation à l'autorité de contrôle et d'effectuer la communication aux personnes concernées si les parties le souhaitent.

Pour aller plus loin : Cnil, Guide RGPD pour les sous-traitants

Pays	Décision	Manquements relevés	Faits reprochés
Roumanie 	**Sanction pécuniaire de 80 000 euros** **4 novembre 2019**	• Manquement au principe d'intégrité et de confidentialité des données (*article 5, 1, f du RGPD*) • Manquement à l'obligation d'assurer la protection des données dès la conception et par défaut (article *25, 1 du RGPD*) • Mesures techniques et organisationnelles insuffisantes pour assurer un niveau de sécurité adapté aux risques (*article 32, 1, 2 du RGPD)*	L'autorité a procédé à un contrôle au sein d'un établissement bancaire à la suite d'une alerte d'un tiers. Les opérations de paiement de 225 525 clients de cet établissement avaient été enregistrées en double entre le 8 et le 10 octobre 2018. Les inspections ont révélé que l'établissement n'avait pas mis en œuvre de garanties adéquates concernant son système de traitement automatisé des données permettant le règlement des transactions effectuées par carte bancaire. L'autorité de contrôle a considéré que l'établissement bancaire n'avait pas assuré la **protection des données dès la conception et par défaut**, et n'avait pas pris les mesures techniques et organisationnelles pour garantir un niveau de sécurité adapté aux risques. Elle a souligné que l'article 32, 1, d du RGPD vise expressément l'obligation du responsable du traitement de **tester, analyser et évaluer régulièrement l'efficacité des mesures** techniques et organisationnelles employées. Elle a prononcé une sanction pécuniaire de 80 00 euros à l'encontre de l'établissement bancaire. *La source est disponible ici.*

Le principe de **protection des données dès la conception** consiste à anticiper et intégrer les enjeux de protection des données personnelles et de la vie privée des personnes concernées dès la conception de tout système, service, produit ou processus et tout au long de leur cycles de vie (*ICO, Data protection by design and default*).

Pays	Décision	Manquements relevés	Faits reprochés
Roumanie 	**Sanction pécuniaire de 130 000 euros** **27 juin 2019**	• Manquement à l'obligation de mettre en œuvre des mesures techniques et organisationnelles appropriées dès la conception et par défaut (*article 25, 1 du RGPD*) • Manquement au respect du principe de minimisation des données (*article 5, 1, c du RGPD*)	L'autorité de contrôle a été informée le 22 novembre 2018 par un tiers d'une violation de données au sein d'un établissement bancaire. Cette violation était intervenue du 25 mai au 10 décembre 2018 et avait concerné les données à caractère personnel de 337 042 clients de l'établissement. Les destinataires des paiements recevaient communication des données relatives à des tiers et aux transactions qu'ils réalisaient (données bancaires, détails de transactions effectuées). L'autorité a considéré que l'établissement bancaire n'avait pas mis en œuvre, **tant au moment de la détermination des moyens** du traitement qu'au **moment de la mise en œuvre du traitement**, des mesures techniques et organisationnelles appropriées destinées à mettre en œuvre les principes de protection des données, **tels que la minimisation des données**. L'autorité a prononcé une sanction pécuniaire de 130 000 euros à l'encontre de l'établissement bancaire. *La source est disponible ici.*

*« Le responsable du traitement met en œuvre**, tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même**, des mesures techniques et organisationnelles appropriées, telles que la pseudonymisation, qui sont destinées à mettre en œuvre les principes relatifs à la protection des données, par exemple la minimisation des données, de façon effective et à assortir le traitement des garanties nécessaires afin de répondre aux exigences du présent règlement et de protéger les droits de la personne concernée. »* (article 25, 1 du RGPD)

LES INCIDENTS SUR LES SITES INTERNET ET LES APPLICATIONS MOBILES

Pays	Décision	Manquements relevés	Faits reprochés
Roumanie 	**Sanction pécuniaire d'environ 3 000 euros** **5 juillet 2019**	• Manquement au principe d'intégrité et de confidentialité des données (*article 5, 1, f du RGPD*) • Mesures techniques et organisationnelles insuffisantes pour garantir un niveau de sécurité adapté au risque (*article 32, 1 et 2 du RGPD*)	A la suite d'une information portée à sa connaissance par un tiers, l'autorité a procédé à un contrôle. Il s'est avéré qu'un ensemble de fichiers contenant des données personnelles relatives aux transactions réalisées sur un site de services juridiques était **accessible au public via deux liens** entre le 10 décembre 2018 et le 1er février 2019 (noms, prénoms, adresses postales et électroniques, numéros de téléphone, professions et le détail de ces transactions). L'autorité de contrôle a estimé que la société exploitant le site internet n'avait pas mis en œuvre de mesures de adéquates pour garantir un niveau de sécurité adapté aux risques de divulgations et d'accès non-autorisé aux données. Elle a prononcé une sanction pécuniaire d'environ 3 000 euros à l'encontre de la société. *La source est disponible ici.*
Malte 	**Sanction pécuniaire de 5 000 euros** **18 février 2019**	Manquement aux obligations relatives à la notification et à la communication des violations de données	En novembre 2018, l'autorité de contrôle a été avertie par un journal d'un incident de sécurité sur le site Internet de l'Autorité Foncière de Malte qui a conduit à la divulgation d'environ 10 gigabytes de données à caractère personnel. En effet, l'absence de mesures techniques et organisationnelles pour sécuriser le site Internet avait permis **l'indexation des données sur le moteur de recherche Google**. Etaient notamment accessibles, les données relatives aux cartes d'identité et les adresses email des personnes concernées. L'autorité de contrôle a prononcé une sanction pécuniaire de 5 000 euros à l'encontre de l'Autorité Foncière. *La source est disponible ici.*

Pays	Décision	Manquements relevés	Faits reprochés
France 	**Sanction pécuniaire de 400 000 euros** **28 mai 2019**	• Manquement à l'obligation d'assurer la sécurité des données à caractère personnel (*article 32 du RGPD*) • Non-respect du principe de conservation limitée des données à caractère personnel (*article 5, 1 e, du RGPD*)	La Cnil a reçu en août 2018 une plainte d'un utilisateur du site web édité par une société du secteur immobilier, permettant aux candidats à la location de mettre en ligne les pièces justificatives nécessaires à la constitution de leur dossier. A la suite de cette plainte, la Cnil a diligenté un contrôle en ligne, puis un contrôle sur place en septembre 2018. La Cnil a constaté qu'il était possible d'accéder aux documents téléchargés par les candidats à la location **en modifiant les derniers caractères de l'URL** affichée dans son navigateur. La formation restreinte de la Cnil a notamment souligné l'absence de mise en place d'une procédure d'authentification des utilisateurs pour caractériser le manquement à l'obligation d'assurer la sécurité des données à caractère personnel. Par ailleurs, la formation restreinte de la Cnil estime que la société conservait en base active les documents relatifs aux candidats n'ayant pas accédé à la location pour une durée excédant celle nécessaire au regard de la finalité principale de la collecte, à savoir l'attribution de logements. Au regard de ces éléments, la formation restreinte de la Cnil a prononcé une sanction pécuniaire de 400 000 euros à l'encontre de la société et a décidé de la rendre publique. Pour calculer ce montant, elle a déclaré avoir pris en compte la gravité du manquement, le manque de diligence de la société dans la correction de la vulnérabilité, le fait que certaines des données avaient un « caractère intime », ainsi que la situation financière de la société. *La source est disponible ici.*

Pays	Décision	Manquements relevés	Faits reprochés
France 	**Sanction pécuniaire de 180 000 €** **18 juillet 2019**	Mesures techniques et organisationnelles insuffisantes pour garantir la sécurité du traitement (*article 32, 1 du RGPD*)	La Cnil a reçu en juin 2018 un signalement par un utilisateur du site web édité par une société du secteur de l'assurance, permettant à ses clients de demander des devis, de souscrire des contrats et d'accéder à leur espace personnel. Le client de la société a indiqué à la Cnil qu'il pouvait accéder aux données d'autres clients à partir de son compte. La Cnil a également été avisée par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) que l'accès aux données des internautes dudit site web était possible sans procédure d'authentification préalable depuis un moteur de recherche. Le 28 juin 2018, la Cnil a diligenté une procédure de contrôle en ligne. A cette occasion, elle a constaté que les comptes des clients étaient accessibles par **la formulation d'une requête via des mots clés au sein d'un moteur de recherche ou par la modification des adresses URL.** Après avoir été avertie le même jour, la société a informé la Cnil de la prise de mesures correctrices. Toutefois, lors d'un second contrôle dans les locaux de la société, la Cnil a constaté que : •les mesures prises n'étaient pas suffisantes pour empêcher **le référencement sur le moteur de recherche** ; •les mots de passe de connexion aux comptes, **dont le format était imposé par la société**, correspondaient à la date de naissance des clients ; •l'identifiant et le mot de passe de connexion étaient **transmis, aux clients par courriel, en clair dans le corps du message**, après la création de leur compte. La formation restreinte de la Cnil a notamment relevé que les mesures élémentaires de sécurité n'avaient pas été prises dès la conception du site web, comme la mise en place d'une procédure d'authentification et d'une gestion des droits d'accès ainsi que l'utilisation d'un fichier tel que « robots.txt » pour éviter le référencement. Par conséquent, la formation restreinte de la Cnil a prononcé une sanction pécuniaire à hauteur de 180 000 euros ainsi qu'une sanction complémentaire de publicité. Pour prononcer cette sanction, elle a déclaré avoir pris en compte le nombre important de personnes concernées, le volume ainsi que la nature des données. *La source est disponible ici.*

Pays	Décision	Manquements relevés	Faits reprochés
Italie 	**Sanction pécuniaire de 30 000 euros** **23 janvier 2020**	• Manquement au principe de licéité, de loyauté et de transparence (*article 5, 1, a du RGPD*) • Manquement au principe d'intégrité et de confidentialité des données (*article 5, 1, f du RGPD*) • Manquement à l'obligation de déterminer une base légale appropriée (*article 6, 1, c, 2 et 3, b du RGPD*) • Manquement à l'obligation de mettre en œuvre des mesures techniques et organisationnelles adéquates (*article 32 du RGPD*)	En décembre 2018, l'Université de Rome a notifié à l'autorité de contrôle italienne une violation de données. La violation concernait un employé et un étudiant de l'Université qui avaient effectué un signalement sur une plateforme de gestion des alertes et signalements d'infraction mise à leur disposition par l'organisme. En l'espèce, **les noms et coordonnées de ces personnes avaient été divulgués sur des moteurs de recherche par l'indexation d'une liste contenant le détail des signalements effectués**. L'université a signalé l'intégralité du répertoire relatif à la plateforme de signalement à chacun des moteurs de recherche concernés. Dans le cadre d'échanges avec l'autorité, l'Université a fait valoir que la violation était intervenue avant l'entrée en application du RGPD, contestant l'application de ses dispositions au litige. Elle a également soulevé que l'application de signalement utilisée était un produit logiciel disponible sur le marché ne permettant pas au responsable du traitement de procéder à des personnalisations. Enfin, selon l'Université, la violation était intervenue suite à **une mise à jour obligatoire des paramètres de sécurité de l'application (patch système) qui aurait accidentellement écrasé les autorisations d'accès de certaines pages web de l'application de signalement.** L'autorité a rappelé que le responsable du traitement est tenu d'adopter des procédures spéciales « pour tester, vérifier et évaluer régulièrement l'efficacité des mesures techniques et organisationnelles » permettant d'assurer la sécurité du traitement. Elle a également fait référence à ses propres lignes directrices en matière de **chiffrement.** En outre, elle a relevé que : • La suspension de l'application avait eu lieu après la notification de la violation de données ; • **L'accès à l'application de signalement se faisait via une adresse web utilisant le protocole « http »**, lequel ne garanti pas la sécurité de la communication ni en termes de confidentialité et d'intégrité des données échangées, ni d'authenticité du site web affiché. Dans ce contexte, compte tenu de la nature, de l'objet et de la finalité du traitement, ainsi que du risque élevé pour les droits et libertés des personnes concernées, l'autorité de contrôle a retenu que la solution utilisée par l'Université ne pouvait être considérée comme répondant aux exigences de sécurité définies par le RGPD. Ainsi, bien qu'accidentelle et promptement notifiée, l'incident de sécurité ayant entraîné la violation de données justifiait le prononcé d'une sanction pécuniaire. Pour déterminer le montant de cette dernière, l'autorité a déclaré avoir pris en compte notamment la négligence du responsable du traitement. Elle a néanmoins relevé que la violation concernait un faible nombre de personnes (seulement deux) et que l'Université avait adopté en temps utile des mesures correctrices pour remédier à la situation. *La source est disponible ici*

Sécuriser les sites Internet

La Cnil constate la récurrence de certains manquements liés à la sécurité des sites Internet et propose des solutions pour remédier à ces problèmes :

La faiblesse des mots de passe

- ◊ Appliquer les exigences de la CNIL sur la robustesse des mots de passe ;
- ◊ Assurer la sécurité du stockage des mots de passe.

L'absence d'authentification aux comptes

- ◊ Mettre en place un mécanisme d'authentification avec un mot de passe complexe ;
- ◊ Privilégier un mécanisme d'authentification forte si possible.

L'absence de chiffrement des données

- ◊ Prévoir des mesures de chiffrement dès la collecte des données ;
- ◊ Utiliser les technologies de chiffrement recommandées par la Cnil et l'ANSSI.

L'accessibilité des données depuis les URL incrémentales

- ◊ Prévoir un contrôle de droit d'accès dans les infrastructures pour éviter les accès non autorisés à des données grâce au changement des caractères de URL.

L'indexation des données dans un moteur de recherche

- ◊ Utiliser un «robot.txt » pour éviter l'indexation des données.

  ATTENTION cela n'empêche pas l'accessibilité des données mais uniquement les robots d'indexation !

Source : Cnil, Sécurité des sites web : les 5 problèmes les plus souvent constatés

Pour aller plus loin : Le référentiel de la Cnil relatif aux dispositifs d'alertes professionnelles

Mettre en place des mots de passe robustes

	Exemple d'utilisation	Longueur minimum	Composition du mot de passe	Mesures complémentaires
Mot de passe seul	Forum, blog	12	• Majuscules • Minuscules • Chiffres • Caractères spéciaux	Conseiller l'utilisateur sur un bon mot de passe
Avec restriction d'accès (le plus répandu)	Site de e-commerce, compte d'entreprise, webmail	8	Au moins 3 des 4 types suivants : • Majuscules • Minuscules • Chiffres • Caractères spéciaux	Blocage des tentatives multiples (exemples) : • Temporisation d'accès au compte après plusieurs échecs ; • « Captcha » • Verrouillage du compte après 10 échecs
Avec information complémentaire	Banque en ligne	5	Chiffres et/ou lettres	Blocage des tentatives multiples + Information complémentaire communiquée en propre d'une taille d'au moins 7 caractères OU Identification du terminal de l'usager
Avec matériel détenu par la personne	Carte bancaire, téléphone	4	Chiffres	Matériel détenu en propre par la personne (ex : carte SIM, carte bancaire, certificat) + Blocage au bout de 3 tentatives échouées

Source : Cnil, Authentification par mot de passe : les mesures de sécurité élémentaires

Pays	Décision	Manquements relevés	Faits reprochés
Norvège 	**Sanction pécuniaire de 49 300 euros** **18 décembre 2019**	Manquement à l'obligation d'assurer la protection des données dès la conception et par défaut (*article 25, 1 du RGPD*)	La municipalité d'Oslo avait mis en place une **application mobile** permettant la communication entre les employés de l'école, les parents et les élèves. L'autorité a constaté plusieurs manquements tenant principalement au niveau de sécurité de ladite application. L'autorité a souligné dans sa décision que l'une des fonctionnalités de cette application est de permettre aux parents d'informer l'école sur l'absence de leurs enfants, ce qui pourrait conduire à communiquer des données relevant des catégories particulières comme les données de santé de l'enfant. Or, l'autorité a constaté qu'il n'y avait aucune mesure empêchant la communication de ces données et l'application ne fournissait aucune indication précisant que la communication de telles données devrait être évitée. Conformément au principe de protection par défaut, l'autorité indique que des mesures alternatives seraient plus appropriées, telles que des listes déroulantes ou des cases à cocher. L'autorité a également précisé que la mauvaise sécurisation de l'accès à l'application avait permis aux personnes non-autorisées d'accéder aux données relatives à plus de 63 000 élèves et de les modifier. Enfin, l'autorité a constaté que l'application présentait d'autres **vulnérabilités en raison de tests de sécurité inadéquats** avant le lancement de celle-ci. Pour ces raisons, l'autorité a prononcé dans un premier temps une sanction pécuniaire de 200 000 euros à l'encontre de la municipalité. Elle a ensuite réduit le montant de cette sanction à 120 000 euros pour tenir compte des efforts déployés par la municipalité pour remédier aux manquements constatés. *La source est disponible ici.*

Comment tester une application mobile ?

Pourquoi tester son application mobile ?

- S'assurer du bon fonctionnement de l'application
- S'assurer de l'absence de certaines erreurs
- Réduire les risques d'atteinte aux données personnelles

Quels types de tests mettre en œuvre selon la Cnil?

⇒ **Les tests de développement**

Ces tests permettent de vérifier l'adéquation entre les spécifications et le fonctionnement de l'application finale.

⇒ **Les tests de sécurité**

Ces tests permettent de vérifier que l'application garde un fonctionnement acceptable même lorsqu'on s'éloigne de son utilisation normale. Il s'agit également de vérifier que l'application ne présente pas de vulnérabilité pouvant permettre à un tiers de compromettre sa sécurité.

Pour aller plus loin : Cnil, Guide du développeur

A éviter !

L'utilisation de données « réelles » pendant la phase de développement et de test revient à les détourner de leur finalité initiale et à augmenter les risques en terme de sécurité (altération des données, perte des données, divulgation de données, etc.).

Bonnes pratiques recommandées par la Cnil

⇒ Mettre en place un système d'intégration continue afin de lancer les tests automatiquement après chaque modification dans votre code source,

⇒ Construire un jeu de données fictives qui ressemblera aux données traitées par l'application. Une telle pratique permet de s'assurer qu'une divulgation de ces données n'entraînera aucun impact pour les personnes.

Source : Cnil, Tester vos applications

LES INCIDENTS DANS LE CADRE DES TRAITEMENTS NON AUTOMATISES

Pays	Décision	Manquements relevés	Faits reprochés
Islande 	**Sanction pécuniaire d'environ 20 643 euros** **5 mars 2020**	Manquement à l'obligation de mettre en œuvre des mesures techniques et organisationnelles pour garantir la confidentialité des données (*articles 5,1,f, et 32 du RGPD*)	Un ancien employé du Centre national de médecine pour la dépendance a reçu des boîtes contenant ses affaires personnelles. Toutefois, il s'est avéré que **ces boîtes contenaient également des dossiers médicaux** de 252 anciens patients et des dossiers contenant les noms d'environ 3 000 personnes ayant suivi un programme de réhabilitation pour abus d'alcool et de drogues. Après avoir mené une enquête, l'autorité a conclu que cette violation des données était le résultat d'un manque de mise en œuvre de politiques et de mesures techniques et organisationnelles appropriées pour protéger les données. Elle a ainsi prononcé une sanction pécuniaire d'environ 20 643 euros. Pour déterminer le montant de la sanction, l'autorité a pris en compte le caractère sensible des données et l'étendue du traitement comme circonstances aggravantes. Elle a aussi pris en compte le caractère non-lucratif des activités du Centre et le fait qu'il avait déployé « des efforts considérables » pour améliorer son traitement de données personnelles, et ce avant la découverte de la violation. *La source est disponible ici.*

« Le présent règlement s'applique au traitement de données à caractère personnel, automatisé en tout ou en partie, ***ainsi qu'au traitement non automatisé de données à caractère personnel*** *contenues ou appelées à figurer dans un fichier. »* (article 2, 1 du RGPD)

Pays	Décision	Manquements relevés	Faits reprochés
Roumanie 	**Sanction pécuniaire de 15 000 euros** **2 juillet 2019**	Mesures techniques et organisationnelles insuffisantes pour garantir la sécurité du traitement (*article 32,1 du RGPD*)	L'autorité roumaine a diligenté une procédure de contrôle suite à une notification de violation des données par une société. Cette violation est intervenue lorsqu'**une liste papier imprimée a été photographiée par une personne non-autorisée.** Cette liste contenait les données relatives à 46 clients participant à un petit déjeuner organisé par un hôtel appartenant au responsable du traitement. Certaines de ces données ont ensuite été divulguées en ligne. L'autorité a sanctionné la société pour ne pas avoir pris de mesures de nature à garantir que les employés ayant accès aux données personnelles ne procèdent au traitement des données qu'à la demande du responsable du traitement, ou en vertu d'une obligation légale. L'autorité a également constaté que le responsable du traitement n'avait pas pris de mesures techniques et organisationnelles afin de garantir un niveau de sécurité adapté au risque de traitement accidentel ou illégal des données, notamment le risque d'accès ou de divulgations non-autorisée des données. Par conséquent, elle a prononcé une sanction pécuniaire de 15 000 euros à l'encontre du responsable du traitement. *La source est disponible ici.*

Le **traitement** est *« toute opération ou tout ensemble d'opérations **effectuées ou non à l'aide de procédés automatisés** et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction. »* (article 4, 2 du RGPD)

Pays	Décision	Manquements relevés	Faits reprochés
Royaume-Uni 	**Sanction pécuniaire d'environ 320 000 euros** **20 décembre 2019**	• Manquement au principe d'intégrité et de confidentialité des données (*article 5, 1, f, du RGPD*) • Mesures techniques et organisationnelles insuffisantes pour assurer la sécurité des données (*article 32 du RGPD*) • Manquement à l'obligation d'information des personnes concernées (*articles 13 et 14 du RGPD*) • Violation de l'obligation de traiter les données personnelles conformément aux exigences du RGPD (*article 24,1 du RGPD*)	Une pharmacie **archivait** environ 500 000 documents dans des **conteneurs non verrouillés à l'arrière de ses locaux**, dont certains étaient **endommagés par l'eau**. Ces documents contenaient les noms et prénoms, les adresses, les dates de naissance ou encore les données médicales et les ordonnances appartenant à un nombre inconnu de personnes. Après avoir été avertie par l'Agence britannique de réglementation des médicaments et des produits de santé, l'ICO a lancé une procédure de contrôle. L'autorité a rappelé que constitue un manquement au titre du RGPD le fait de ne pas traiter les données d'une manière garantissant un niveau de sécurité adéquate aux risques de traitements non-autorisés ou illégaux et de perte, de destruction ou de dégradation accidentelle des données. Au cours de la procédure, l'ICO a également constaté que l'information fournie aux personnes concernées n'était pas suffisante. Ces dernières n'étaient pas informées notamment de l'identité du responsable du traitement, de la durée de conservation de leurs données, de leurs droits ou encore de la source des données pour ce qui concerne les collectes indirectes. À l'issue de cette procédure, l'ICO a prononcé une sanction pécuniaire d'environ 320 000 euros. Pour calculer le montant de cette sanction, l'ICO n'a pris en compte que la période à partir du 25 mai 2018, la date d'entrée en vigueur du RGPD. L'ICO a également ordonné à la pharmacie de prendre les mesures nécessaires pour se conformer aux exigences du RGPD **dans les trois mois, à compter de sa décision.** *La source est disponible ici.*

Définir un processus de gestion des archives

Comment ? Ce processus doit déterminer :

⇒ Quelles données devront être archivées ? Pour quelle raison ? Pour combien de temps ?

(Obligation légale de conservation ? Gestion des réclamations ? Du contentieux ? Intérêt administratif en matière commerciale, civile ou fiscale ? A des fins de recherche scientifique, historiques ou à des fins statistiques ?)

⇒ Comment et où ces données seront stockées ?

Bonnes pratiques recommandées par la Cnil

⇒ Prévoir des modalités d'accès spécifiques aux données archivées, tenant compte du caractère ponctuel et exceptionnel de leur utilisation.

⇒ Mettre en œuvre un fonctionnement homogène du système de purge en adoptant, par exemple, les mêmes modalités pour la gestion du droit à l'effacement et pour la purge ou l'anonymisation des données.

Source : Cnil, Limiter la conservation des données, Sécurité : Archiver de manière sécurisée

Les cycles de conservation des données

1. La base active

La purge régulière des données en base active permet de garantir que les données sont conservées et accessibles par les services opérationnels uniquement le temps nécessaire à l'accomplissement de l'objectif poursuivi par le traitement.

2. L'archivage intermédiaire

Les données archivée ne doivent pas être conservées en base active, même en y apposant la mention « archivées ». L'archivage intermédiaire permet de limiter l'accès à ces données à un service spécifique bénéficiant d'une habilitation pour y accéder et pour éventuellement les désarchiver, le cas échéant.

3. L'archivage définitif ou la suppression

A éviter !

L'archivage ou le stockage des données d'une manière ne permettant pas de garantir :

⇒ L'intégrité des données (dégâts des eaux, pluie, etc.)

⇒ La confidentialité des données (conteneurs non verrouillés, véhicules personnels, etc.)

DES MESURES D’AUTHENTIFICATION DEFAILLANTES

Authentification des personnes concernées

Pays	Décision	Manquements relevés	Faits reprochés
Allemagne 	**Sanction pécuniaire de 9.55 millions d'euros** **9 décembre 2019**	Mesures techniques et organisationnelles insuffisantes pour garantir la sécurité du traitement (*article 32 du RGPD)*	L'autorité a été informée qu'en appelant la ligne d'assistance d'un opérateur de télécommunications, il était possible d'obtenir des informations détaillées sur un client **en fournissant uniquement son nom et sa date de naissance**. Au regard de l'article 32 du RGPD, cette **procédure d'authentification** a été jugée insuffisante par l'autorité de contrôle qui a demandé à l'opérateur de prendre des mesures pour protéger les traitements de manière systématique. Dans un premier temps, l'opérateur a renforcé sa procédure d'authentification par la demande d'informations supplémentaires. Il a ensuite entamé des travaux pour introduire une nouvelle procédure d'authentification. Ces nouvelles modalités ne sont pas détaillées dans la décision. L'autorité de contrôle a prononcé une sanction pécuniaire de 9,55 millions d'euros pour l'insuffisance des mesures techniques et organisationnelles. Dans sa décision, elle a souligné que l'opérateur s'était montré très coopératif, mais que le manquement en question constituait un risque pour l'ensemble de la base de données de la clientèle. *La source est disponible ici.*

Authentification des employés

Pays	Décision	Manquements relevés	Faits reprochés
Pays-Bas 	**Sanction pécuniaire de 460 000 euros** **18 juin 2019**	Mesures techniques et organisationnelles insuffisantes pour assurer la sécurité du traitement (*article 32 du RGPD)*	L'autorité néerlandaise a procédé à un contrôle au sein d'un hôpital après avoir appris que 197 employés du personnel de cet hôpital avaient accédé au dossier médical d'une célébrité néerlandaise. L'autorité a contrôlé la conformité de l'hôpital aux exigences de l'article 32, et plus spécifiquement les standards de sécurité applicables au secteur de la santé. Au cours du contrôle, l'autorité a constaté que l'hôpital n'avait pas pris les mesures de sécurité nécessaires en matière d'authentification. Plus précisément, l'hôpital **n'avait pas mis en place une procédure d'authentification à deux facteurs** conformément aux standards en la matière. L'autorité a également constaté que l'hôpital ne contrôlait pas suffisamment les accès. Il opérait un contrôle aléatoire de six dossiers de patients par an, ce qui ne constitue pas selon l'autorité une mesure de sécurité adaptée aux risques, compte tenu notamment de l'ampleur du traitement de données par l'hôpital. L'autorité a rappelé que l'exigence en la matière consiste en un « contrôle systématique, intelligent et orienté sur le risque ». Elle souligne que le contrôle des accès doit être systématique et cohérent. Ainsi elle a jugé que le fait qu'un contrôle ou un contrôle aléatoire soit déclenché par une plainte n'est pas une mesure suffisante. Elle a ainsi prononcé une sanction pécuniaire de 460 000 euros à l'encontre de l'hôpital pour l'insuffisance de la sécurité des dossiers de patients en interne.

Pays	Décision	Manquements relevés	Faits reprochés
France 	**Sanction pécuniaire de 20 000 euros** **Assortie d'une astreinte de 200 euros par jour de retard si non-conformité à l'issue d'un délai de deux mois** **13 juin 2019**	• Manquement au principe de minimisation des données (*article 5, 1. c du RGPD*) • Manquement à l'obligation d'informer les personnes concernées (*articles 12 et 13 du RGPD*) • Manquement à l'obligation d'assurer la sécurité et la confidentialité des données (*article 32 du RGPD*) • Régularisé suite à la mise en demeure : manquement au principe de limitation de la conservation (*article 5, 1, e du RGPD*)	Entre 2013 et 2017, la Cnil a reçu huit plaintes de salariés d'une société, relatives à un dispositif de vidéosurveillance. Après l'envoi infructueux de plusieurs courriers entre 2013 et 2016, l'autorité a procédé à un contrôle sur place le 16 février 2018. Celui-ci a révélé une série de manquements. L'une des caméras filmait en continu les postes de travail de 6 salariés et les images étaient conservées pour une durée excessive. Les salariés n'étaient pas informés formellement de l'existence du dispositif. Par ailleurs, **les postes de travail des collaborateurs n'étaient pas verrouillés par mot de passe**, de même que celui du dirigeant, sur lequel un logiciel permettait de consulter les images captées. Enfin, **tous avaient accès, via un mot de passe commun, à une boite de messagerie électronique pour la société**. Celle-ci ne disposait pas de mesures de traçabilité permettant de retracer les actions effectuées par chacun. Le 26 juillet 2018, la Cnil a mis en demeure la société de régulariser ses manquements, notamment en ne conservant les images que quinze jours, en cessant de filmer en continu les 6 salariés, en informant les salariés, et en mettant en œuvre une série de mesures de sécurité. La société a mis en œuvre la nouvelle durée de conservation, mais ne s'est pas conformée aux autres injonctions de la Cnil, ce que celle-ci a constaté lors d'un second contrôle le 10 octobre 2018. L'autorité a prononcé une sanction pécuniaire publique de 20 000 euros, assortie d'une astreinte de 200 euros par jour de retard. Le montant et la publicité sont justifiés par la Cnil par l'absence de collaboration de la société, la « particulière sensibilité » du dispositif de vidéosurveillance, la pluralité des manquements en cause ainsi que leur persistance et leur gravité. Toutefois, la Cnil indique également avoir tenu compte des mesures prises par la société au cours de l'instruction, du fait qu'il s'agisse d'une microentreprise et de sa situation financière difficile. *La source est disponible ici.*

Sécuriser l'accès aux données par la mise en place d'un moyen d'authentification

Comment ? Le mot de passe constitue un moyen d'authentification répandu, peu couteux et simple à mettre en place. Toutefois, il ne permet pas d'assurer un niveau de sécurité élevé. Pour cette raison, il doit répondre à certaines exigences élémentaires, formulées par la CNIL dans sa délibération n°2017-012 du 19 janvier 2017.

Pratiques à bannir :

- créer ou utiliser un compte partagé par plusieurs personnes.
- conserver les mots de passe en clair.

4 étapes pour assurer la sécurité des mots de passe

1. Respecter les exigences de la CNIL en termes de la complexité du mot de passe et mettre en place des mesures complémentaires (restriction d'accès, etc.).
2. Assurer la sécurité de la fonction d'authentification elle-même : elle doit utiliser un algorithme public réputé fort et sa mise en œuvre logicielle doit être exempté de vulnérabilités.
3. Conserver les mots de passe de manière sécurisée : privilégier la fonction cryptographique pour assurer une conservation sécurisée.
4. Renouveler les mots de passe avec une périodicité déterminée en fonction de la complexité des mots de passe, des données traitées et des risques éventuels.

Source : Cnil, Guide de la sécurité des données personnelles

Sécuriser l'accès aux données par la mise en place d'un moyen d'authentification

Bonne pratique

Privilégier un **mécanisme** d'authentification forte pour assurer qu'un employé n'accède qu'aux données nécessaires au regard de ses fonctions.

Qu'est ce qu'un mécanisme d'authentification forte ?

Selon les recommandations de la CNIL, l'authentification est qualifiée de forte lorsque le mécanisme comporte au moins deux des facteurs suivants :

- ⇒ Ce que l'on sait, par exemple un mot de passe;
- ⇒ Ce que l'on a, par exemple une carte à puce;
- ⇒ Une caractéristique propre à la personne, par exemple une empreinte digitale.

ATTENTION, l'utilisation de la biométrie est notamment soumise à une analyse d'impact sur la vie privée (AIPD).

Source : Cnil, Guide de la sécurité des données personnelles,

La sécurité des données de santé

Qu'est-ce qu'une donnée de santé ?

Les données concernant la santé sont des données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soin de santé, qui révèlent des informations sur l'état de santé de cette personnes (article 4, RGPD).

Ces données devraient comprendre l'ensemble des données se rapportant à l'état de santé d'une personne concernée sui révèlent des informations sur **l'état de santé physique ou mentale passé, présent ou futur de la personne concernée** (considérant 35, RGPD).

Les données concernant la santé appartiennent aux catégories particulières de données, visées à l'article 9 du RGPD.

A ce titre, elles doivent faire l'objet d'une protection renforcée.

Pour rappel, conformément à l'article 9, 4 du RGPD, « *les états membres peuvent maintenir ou introduire des* ***conditions supplémentaires****, y compris des limitations, en ce qui concerne le traitement de données génétiques, des données biométriques ou des* ***données concernant la santé*** ».

⇒ En droit français, en application de l'article L.1111-8 du Code de la santé publique, l'hébergement de données de santé est soumis à un régime particulier de certification et/ou d'agrément suivant le support et le service proposé (hébergeurs sur support papier, hébergeurs sur support numérique dans le cadre d'un archivage électronique).

La sécurité des données de santé

Les recommandations de la Cnil

LES ARCHITECTURES CLIENT-SERVEUR

⇒ Anticiper le rapatriement des données ou le transfert de fichiers sur micro-ordinateur en fonction des habilitations de chacun. Il conviendra de limiter au strict minimum le transfert de fichiers complets et le volume des informations rapatrier. Il conviendra enfin de journaliser les requêtes au niveau du serveur.

⇒ Séparer les réseaux de gestion administrative et de suivi médical.

CONNEXION A INTERNET

⇒ En cas de connexion d'un des serveurs du réseau à Internet, il conviendra de prévoir des mesures particulières telles que la séparation physique des deux réseaux, la mise en place d'un firewall ou des barrières de protection logicielles.

⇒ Lorsque des données de santé sont transférées via internet, il conviendra de chiffrer la communication.

GESTION DES MOTS DE PASSE

⇒ Définir un code utilisateur individuel distinct du nom de l'utilisateur.

⇒ Interdire dès la conception la réutilisation des trois derniers mots de passe (blocage du système).

GESTION DES MODALITES DE CONNEXION ET DE DECONEXION

⇒ Rendre impossible la connexion à plusieurs sous le même code et le même mot de passe.

⇒ Afficher systématiquement aux utilisateurs les dates et heures de dernière connexion.

JOURNALISATION DES CONNEXIONS

⇒ Après plusieurs frappes incorrectes successives du mot de passe, bloquer l'accès et demander à l'utilisateur de prendre contact avec le responsable du système.

⇒ Mettre en œuvre une procédure de déconnexion automatique en cas de non-utilisation du système pendant un temps donné.

Source : Cnil, Données de santé : un impératif, la sécurité

DES MESURES D’HABILITATION OU DE TRACABILITE DEFAILLANTES

Pays	Décision	Manquements relevés	Faits reprochés
Italie 	**Sanction pécuniaire de 50 000 euros** **4 avril 2019**	Mesures techniques et organisationnelles insuffisantes pour garantir la sécurité et la confidentialité des données (*article 32, 1 du RGPD*)	Au cours de l'été 2017, une faille de sécurité avait été identifiée sur plusieurs sites reliés à un mouvement politique italien. A la suite d'une procédure de contrôle, l'autorité italienne avait identifié des défauts de sécurité et ordonné au responsable du traitement concerné d'y mettre fin, notamment en prescrivant l'adoption d'une série de mesures palliatives sous trente jours, ainsi que le renforcement de la sécurité des systèmes d'information et la mise en conformité au RGPD (notamment principe de minimisation) dans un délai plus long. Le responsable du traitement en cause avait dans les délais impartis mis en place les mesures palliatives. Par le biais de contrôles complémentaires, l'autorité a suivi la mise en œuvre dans le temps de la mise en conformité au RGPD. Par une décision du 4 avril 2019, l'autorité italienne constate que bien que des mesures de sécurité aient été mises en œuvre, il subsiste des manquements à l'obligation d'assurer la sécurité des données, en particulier en raison de **l'absence de traçabilité complète des accès à la base de données,** du partage d'identifiants entre plusieurs personnes en charge de l'une des plateformes contrôlées, de **l'absence de définition de profils d'habilitation** pour restreindre l'accès aux données selon les domaines d'exploitation. Ces éléments ayant déjà été relevés dans la procédure de contrôle initiale, l'autorité italienne prononce à l'encontre du responsable du traitement une sanction pécuniaire de 50 000 euros, en raison de la durée du manquement, du fait qu'il concerne des données relevant d'une catégorie particulière de données (opinion politique), qu'il concerne un nombre significatif de personnes concernées et au regard du caractère obsolète et inadéquat des mesures de sécurité implémentées. Toutefois, l'autorité de contrôle note également les progrès en termes de sécurité depuis le contrôle initial, et le fait que le responsable de traitement soit une association et non une société.

Pays	Décision	Manquements relevés	Faits reprochés
Portugal 	**Sanction pécuniaire de 400 000 euros** **11 octobre 2018**	• Violation du principe d'intégrité et de confidentialité des données (*article 5, 1 f du RGPD*) • Manquement au principe de minimisation des données (*article 5, 1 c du RGPD*) • Mesures techniques et organisationnelles insuffisantes pour garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement (*article 32, 1 b du RGPD*)	L'entité sanctionnée est un hôpital. La CNDP lui reproche l'insuffisante sécurisation de son système d'information, et l'absence de mesures techniques et organisationnelles permettant de sécuriser les données des patients. Notamment : • Des collaborateurs non autorisés ont pu accéder à des données de patients ; • Le personnel disposant d'un accès à la base de l'hôpital a **accès à l'intégralité des données** de tous les patients (pas de différenciation des niveaux d'accès en fonction des besoins), et peut également **accéder à des données de patients d'autres hôpitaux,** sans que cela ne soit justifié ; • L'hôpital n'est pas en mesure d'assurer en continu la surveillance de son système d'information pour assurer l'intégrité et la confidentialité des données.

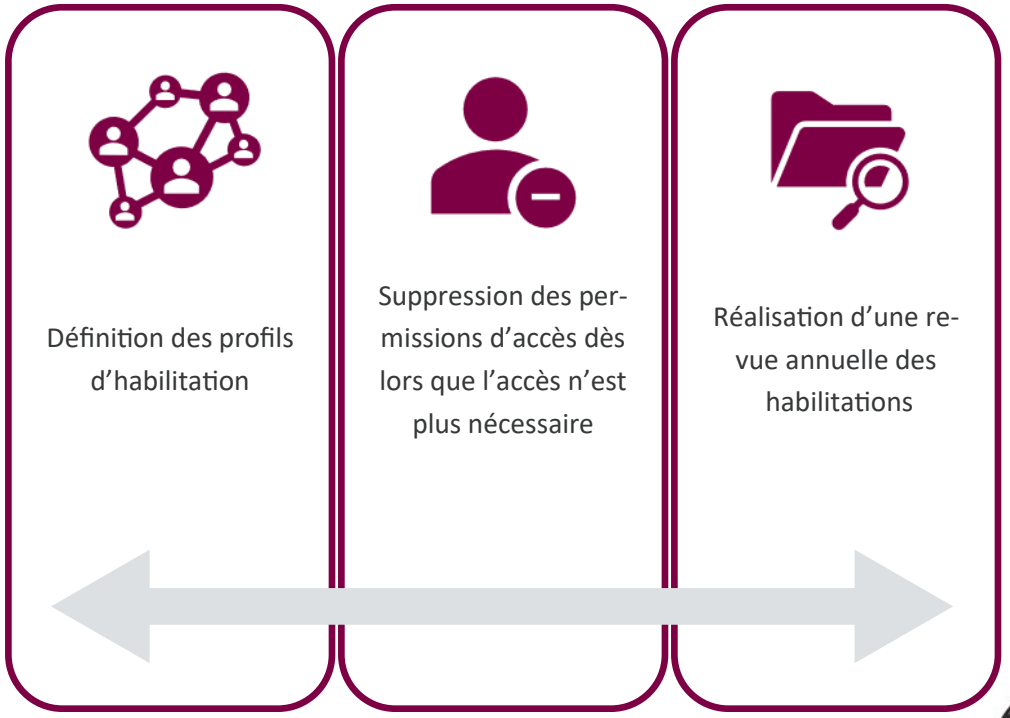
Pays	Décision	Manquements relevés	Faits reprochés
Norvège 	**Sanction pécuniaire de 170 000 euros** **19 mars 2019**	Manquement à l'obligation d'assurer la confidentialité et la sécurité des données à caractère personnel (*article 5,1,f et article 32 du RGPD*)	L'Autorité de contrôle norvégienne a constaté que l'accès à certains fichiers informatiques d'une municipalité n'était pas sécurisé de manière adéquate. Ces fichiers comportaient les identifiants de connexion et les mots de passe de plus de 35 000 comptes appartenant aux élèves et personnels des écoles primaires de cette municipalité. L'Autorité a estimé qu'en raison d'un défaut de sécurité du système de connexion aux fichiers litigieux, **des personnes non-autorisées pouvaient consulter les identifiants et les mots de passe contenus dans ces fichiers,** ainsi qu'à diverses données (date de naissance, nom, école, adresse, etc.). Elles pouvaient alors accéder aux plateformes des écoles primaires et donc aux données à caractère personnel y figurant (par exemple évaluation des élèves par les enseignants etc.). L'Autorité a jugé que la municipalité n'avait pas mis en œuvre les mesures techniques et organisationnelles nécessaires à garantir la sécurité des ces données. Ce manquement a été aggravé par le fait que la violation de données concernait plus de 35 000 personnes, dont une majorité de mineurs. De plus, la municipalité a été avertie à plusieurs reprises du faible niveau de sécurité mis en œuvre. L'Autorité norvégienne rappelle l'importance pour les autorités publiques de connaitre leurs responsabilités, en soulignant qu'elles mettent souvent en œuvre des traitements sur lesquels les personnes concernées n'ont pas de maitrise. Par conséquent, elle a prononcé une sanction pécuniaire de 170 000 euros à l'encontre de la municipalité. *La source est disponible ici.*

Pays	Décision	Manquements relevés	Faits reprochés
Roumanie 	**Sanction pécuniaire d'environ 20 000 euros** **7 novembre 2019**	Manquement à l'obligation d'assurer la sécurité du traitement (*articles 32, 1, 2, 4 du RGPD*)	L'autorité a procédé à un contrôle suite à une notification de violation des données en date du 13 septembre 2019. L'autorité a relevé que le responsable du traitement n'avait pas adopté de mesures techniques et organisationnelles adéquates lui permettant de s'assurer que les personnes physiques sous son autorité ayant accès aux données personnelles se conforment à ses instructions conformément à l'article 32, 4 du RGPD. Le responsable du traitement n'avait pris aucune mesure appropriée afin de garantir la sécurité de données au regard du risque de divulgation ou d'accès non autorisé aux données personnelles. Ces manquements ont permis un **accès non autorisé par un employé à une application de réservation** contenant les données personnelles de 22 clients de la société et à la divulgation non autorisée de ces information en ligne. *La source est disponible ici.*

Pays	Décision	Manquements relevés	Faits reprochés
Roumanie 	**Sanction pécuniaire d'environ 500 euros** **29 novembre 2019**	• Manquement au principe de protection des données dès la conception et par défaut (*article 25 du RGPD*) • Mesures techniques et organisationnelles insuffisantes pour assurer la sécurité du traitement (*article 32 du RGPD*) • Manquement aux obligations de transparence et d'information des personnes concernées (*articles 12 et 13 du RGPD*).	L'autorité a procédé à un contrôle suite à une plainte relative à l'accès, l'usage et la divulgation à de nombreuses personnes, sans base légale, d'images issues du système de vidéo-surveillance d'une association. Le contrôle a démontré que l'association n'avait pas adopté les mesures techniques et organisationnelles pour assurer la protection des données personnelles collectées via le dispositif de vidéo-surveillance. L'autorité a, donc, ordonné à l'association de mettre en œuvre des mesures correctives dans un délai de 30 jours, et notamment : • d'intégrer les principes de protection des données tels que la limitation de la conservation des images ; • de **limiter le nombre de personnes ayant accès au dispositif** de vidéo-surveillance ; • de fournir des instructions claires aux personnes agissant sous l'autorité de l'association conformément à l'article 32, 4 du RGPD. L'autorité a également ordonné à l'association de mettre en place des mesures correctives dans un délai de 10 jours pour assurer l'information des personnes concernées, telles que l'affichage des panneaux d'information. *La source est disponible ici.*

Gérer les habilitations pour limiter l'accès aux données

Les recommandations de la Cnil



Bonnes pratiques

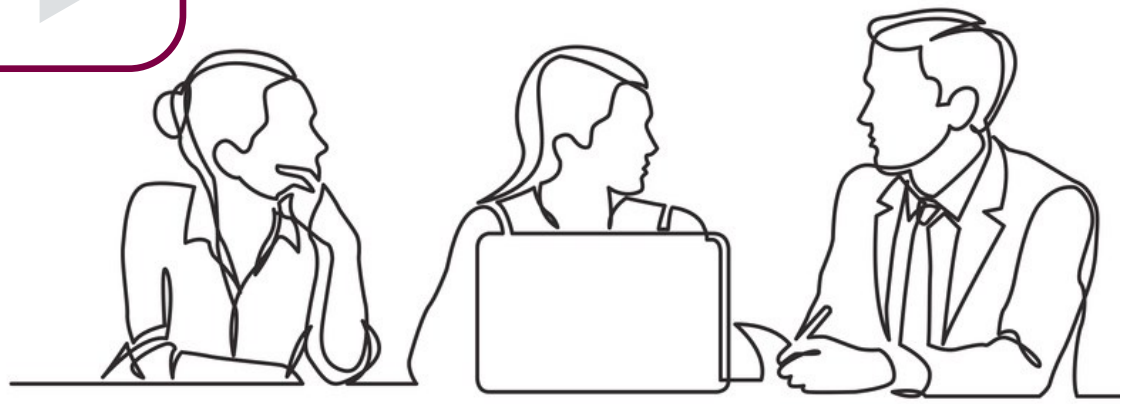
⇒ Créer un compte unique pour chaque personne.

⇒ Définir les droits d'accès et leur étendue en fonction des besoins des personnes dans le cadre de leurs fonctions.

⇒ Retirer les autorisations temporaires dès que la durée déterminée arrive à son échéance.

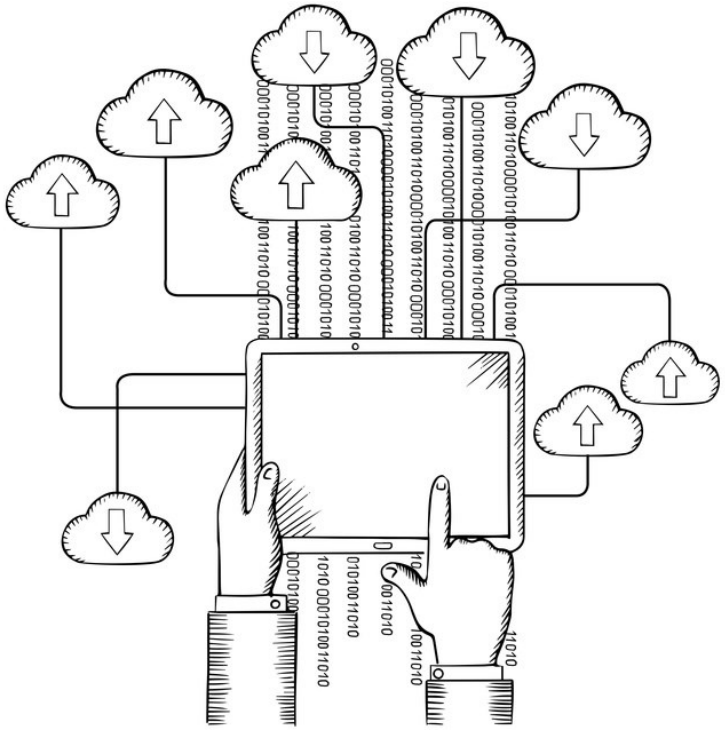
⇒ Supprimer les comptes des personnes qui ont quitté l'entité ou changé de fonction.

Source : Cnil, Guide de la sécurité des données personnelles



Gérer les incidents pour identifier les accès non-autorisés

Comment ? L'établissement d'un système de journalisation est nécessaire pour la gestion des traces et des incidents. Un tel système permettrait d'enregistrer les activités des personnes ayant accès aux données et les anomalies éventuelles.



Penser à :

⇒ Informer les utilisateurs de l'existence d'un système de journalisation.

⇒ Mettre en place les mesures de sécurité nécessaires pour protéger les équipements de journalisation ainsi que les informations journalisées.

⇒ Etablir des procédures pour examiner régulièrement les journaux d'évènements et assurer la notification des anomalies éventuelles au responsable du traitement.

Bonnes pratiques

La Cnil recommande de définir une politique de contrôle d'accès qui inclut notamment :

⇒ Les procédures à appliquer à l'arrivée, au départ ou au changement de fonctions d'une personne.

⇒ Les conséquences en cas de non-respect des mesures de sécurité.

⇒ Les mesures de restriction et de contrôle de l'attribution et de l'utilisation des accès aux données.

Source : Cnil, Guide de la sécurité des données personnelles

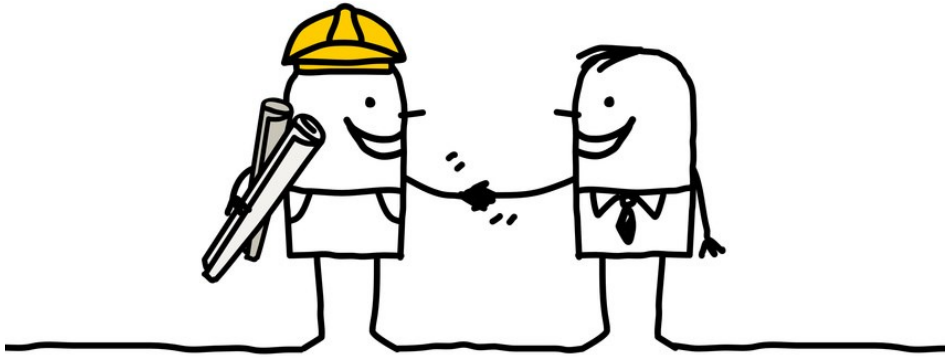
LA DIVULGATION DE DONNEES ACCIDENTELLE OU NON-AUTORISEE PAR LE RESPONSABLE DU TRAITEMENT

Pays	Décision	Manquements relevés	Faits reprochés
Allemagne 	**Sanction pécuniaire de 105 000 euros** **Décembre 2019**	Manquement à l'obligation d'assurer la sécurité et la confidentialité des données	Une **confusion de patients** lors de leur admission s'est produite au sein d'un hôpital. Par suite, des factures erronées ont été émises. L'autorité de contrôle de Rhénanie-Palatinat a constaté des défaillances techniques et organisationnelles dans la gestion des patients et la protection de la vie privée. Par conséquent, elle a prononcé une sanction pécuniaire de 105 000 euros à l'encontre de l'hôpital. *La source est disponible ici.*
Grèce 	**Avertissement** **9 novembre 2018**	Manquement à l'obligation de notification dans les délais (*article 33 du RGPD*)	Un établissement bancaire **a communiqué par erreur les données à caractère personnel relatives à certains de ses clients à d'autres. Il a notifié la violation de données à l'autorité de contrôle deux jours après le délai de 72 heures et a procédé à la communication aux personnes concernées.** L'autorité de contrôle a prononcé un avertissement à l'encontre de l'établissement bancaire pour le non-respect des délais prévus par le RGPD.

Pays	Décision	Manquements relevés	Faits reprochés
Roumanie 	**Sanction pécuniaire d'environ 2 000 euros** **25 novembre 2019**	• Manquement au principe d'exactitude des données (*article 5, 1, d du RGPD*) • Manquement à l'obligation de mettre en œuvre des mesures techniques et organisationnelles appropriées (*article 32, 1, b et 2 du RGPD*).	L'autorité a procédé à un contrôle suite à une plainte selon laquelle **une personne recevait à son adresse des factures émises à destination d'une autre personne**, cliente du responsable du traitement. La plainte indiquait que l'individu avait informé le responsable du traitement de la situation mais celui-ci n'avait pas donné de suites. Lors du contrôle, le responsable du traitement n'avait pas été en mesure de démontrer l'exactitude des données traitées. L'autorité a également relevé que le responsable du traitement n'avait pas mis en œuvre de mesures techniques et organisationnelles appropriées afin de garantir la confidentialité des données, ce qui avait rendu possible la violation de données, objet de la plainte. *La source est disponible ici.*
Islande 	**Sanction pécuniaire d'environ 8 945 euros** **5 mars 2020**	Manquement à l'obligation de mettre en œuvre des mesures techniques et organisationnelles pour garantir la confidentialité des données (*articles 5,1,f et 32 du RGPD*)	L'autorité islandaise a sanctionné un établissement scolaire suite à une violation de données personnelles. **Un professeur avait envoyé aux élèves et leurs parents, soit 57 personnes au total, un courriel contenant en pièce jointe un document. Le professeur pensait que ce document contenait des informations relatives à la prise de rendez-vous pédagogiques.** Or, **la pièce jointe contenait les informations relatives à un groupe d'élèves (18 au total) différent**. Les données concernaient le bien-être des élèves, leurs performances scolaires, leurs conditions sociales, ainsi que leurs problèmes personnels. Pour l'un des mineurs, les informations concernaient l'intervention des services de la protection de l'enfance. Par ailleurs, certaines données portaient sur la santé physique ou mentale de certains élèves. *La source est disponible ici.*

Pays	Décision	Manquements relevés	Faits reprochés
Roumanie 	**Trois sanctions pécuniaires pour un total de 14 000 euros** **10 décembre 2019**	• Manquement au principe d'exactitude des données (*article 5, 1, d du RGPD*) • Mesures techniques et organisationnelles insuffisantes pour garantir la sécurité du traitement (*articles 25 et 32 du RGPD*) • Manquement à l'obligation de notification à l'autorité de contrôle d'une violation de données à caractère personnel (*article 33 du RGPD*)	L'autorité roumaine a procédé à un contrôle suite à une plainte selon laquelle **un établissement de crédit avait envoyé des documents contenant les données personnelles d'une personne tierce à un individu**. **Ce dernier a signalé cette erreur au responsable** du traitement ainsi qu'à son centre d'appel sans que celle-ci n'ait été rectifiée. En effet, la personne recevait toujours les documents sur son adresse email. Le contrôle de l'autorité a révélé que la société traitait des données sans démontrer l'application effective de mécanismes permettant de vérifier et de valider l'exactitude des données collectées et traitées afin de garantir leur confidentialité. Il a également été relevé que le responsable du traitement n'avait pas mis en œuvre de mesures de sécurité suffisantes afin d'empêcher l'accès ou la divulgation non autorisée de données personnelles à des tiers. L'entité n'a pas, non plus, notifié l'autorité de contrôle de **cette violation de données** dans un délai de 72h. *La source est disponible ici.*

Pays	Décision	Manquements relevés	Faits reprochés
Espagne 	**Sanction pécuniaire de 2 500 euros** **14 février 2020**	• Manquement au principe d'intégrité et de confidentialité (*article 5, 1, f du RGPD*) • Manquement au principe de responsabilité (*article 5, 2 du RGPD*)	Un couple propriétaire d'un immeuble, dont la vente avait été confiée à une entité de gestion immobilière, avait saisi l'autorité de contrôle d'une plainte en avril 2019. Les plaignants soulignaient que, lors du processus de vente de l'immeuble, les données à caractère personnel les concernant avaient été divulguées aux acquéreurs potentiels par courriel. En effet, les prospects avaient reçu **le contrat d'acquisition de l'immeuble contenant les données à caractère personnel.** L'autorité a relevé que **la divulgation par courriel d**es données à caractère personnel des plaignants constituait un manquement au principe d'intégrité et de confidentialité des données personnelles ainsi qu'au principe de responsabilité, imposant au responsable de traitement de démontrer sa conformité. L'autorité a prononcé une sanction pécuniaire d'un montant de 2 500 euros à l'encontre de l'entité. *La source est disponible ici*



Pays	Décision	Manquements relevés	Faits reprochés
Roumanie 	**Sanction pécuniaire de 150 000 euros prononcée contre le premier responsable du traitement** **Sanction pécuniaire de 20 000 euros prononcée contre le second responsable du traitement** **1er octobre 2019**	<u>En ce qui concerne le premier responsable du traitement</u> : •Mesures techniques et organisationnelles insuffisantes (*articles 32-1, 32-2, 32-4 du RGPD*) <u>En ce qui concerne le second responsable du traitement</u> : •Mesures techniques et organisationnelles insuffisantes (*articles 32-1, 32-2, 32-4 du RGPD*) •Manquement à l'obligation de notifier la violation de données (*article 33, 1 du RGPD*)	L'autorité roumaine a diligenté un contrôle au sein d'un établissement bancaire suite à une notification de violation des données personnelles. Deux salariés dudit établissement bancaire avaient utilisé **les documents d'identité de personnes physiques, transmises par les employés d'une société de crédit via l'application WhatsApp**, afin d'interroger le système du Bureau des crédits. En effet, cette procédure permet de déterminer l'éligibilité des individus à l'obtention d'un prêt grâce à la réalisation de simulations permettant de noter les dossiers. Au total, 1194 simulations ont été réalisées pour 1177 individus. Pour 124 personnes concernées, la base de données de l'Administration fiscale a également été interrogée. Ces simulations ont été réalisées grâce à une application propre à l'établissement bancaire et **les décisions négatives ont été communiquées à la société de crédit en violation des procédures internes**. L'autorité a relevé que cette situation avait abouti à l'accès non autorisé aux données personnelles traitées par l'application de l'établissement bancaire ainsi qu'à la divulgation non autorisée de données personnelles par les collaborateurs de cette entité. À l'issue de la procédure engagée contre ces deux entités, l'autorité a estimé que l'établissement bancaire : • n'avait pas mis en œuvre de mesures appropriées lui permettant de s'assurer que les personnes physiques agissant sous son autorité et ayant accès aux données personnelles ne procèdent à leur traitement qu'à sa demande, sauf en cas d'obligation légale ; •n'avait pas mis en œuvre les mesures techniques et organisationnelles permettant de garantir un niveau de sécurité adéquat et n'avait pas évalué les risques que le traitement présentait. Concernant la société de crédit, l'autorité a motivé la sanction par le manquement de l'entité à son obligation de sécurité ainsi que l'absence de notification de la violation de données, alors qu'elle avait eu connaissance de cet incident, dès décembre 2018. *La source est disponible ici.*

Sensibiliser les utilisateurs aux enjeux de sécurité

Que préconise la CNIL ?

Organiser des séances de formation et de sensibilisation, informer des mises à jour des règles sur la sécurité, faire des rappels périodiques par courriel, etc.

Expliquer les opérations de traitement des données dans des documents auxquels les utilisateurs peuvent se référer.

Rédiger une charte informatique qui doit être annexé au règlement intérieur de l'entité responsable du traitement.

Prévoir la signature d'un engagement de confidentialité ou insérer dans les contrats de travail une clause de confidentialité spécifique aux données à caractère personnel.

Source : Cnil, Guide de la sécurité des données personnelles

Les séances de formation et de sensibilisation devraient porter notamment sur :

⇒ Les objectifs et enjeux rencontrés par l'entité en matière de sécurité ;

⇒ Les données considérées comme sensibles ;

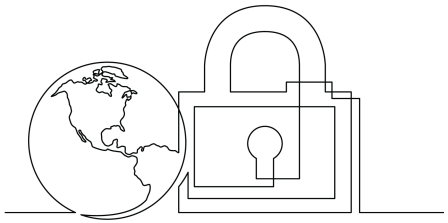
⇒ Les lois et les réglementations applicables ;

⇒ Les règles et consignes de sécurité à respecter au quotidien ;

Etc.

Source : ANSSI, Guide d'hygiène informatique

Abonnez-vous à notre Newsletter !



Mathias Avocats

Cabinet d'avocats indépendant spécialisé dans le droit du numérique (IP/IT/Data).

Nous accompagnons nos clients, de manière pragmatique, au gré des évolutions juridiques et technologiques. Nous les assistons également dans leur contentieux (juridictions judiciaires, autorités de contrôle).

Nous collaborons avec des avocats partenaires exerçant dans le monde entier.

Nos interventions allient la rigueur, la créativité et l'efficacité d'une équipe dédiée et mobilisée aux côtés de ses clients.

Suivez l'actualité juridique sur notre blog

www.avocats-mathias.com/blog

Avertissement

Le présent panorama réalisé à date n'a pas pour objectif de dresser un recensement exhaustif des sanctions prononcées par les autorités de contrôle. Les autorités de contrôle peuvent notamment prononcer des décisions non publiques.

Il a été constitué à partir des informations mises à la disposition du public par ces autorités et par le CEPD. Certaines décisions ont fait l'objet d'une libre traduction afin d'être évoquées dans le présent panorama, en l'absence de traduction officielle.

Les informations contenues dans le présent document ne constituent pas des conseils juridiques et ne peuvent s'y substituer.

Mathias Avocats

Avez-vous une question ?

Une équipe dédiée pour vous accompagner dans la réalisation de vos ambitions.

01 43 80 02 01

contact@avocats-mathias.com

19, rue Vernier – 75017 Paris

Retrouvez les conseils pratiques de nos avocats sur Twitter :

@GaranceMathias