Lignes directrices 01/2021

Exemples concernant la notification de violations de données à caractère personnel

Adoptées le 14 décembre 2021

Version 2.0

Historique des versions

Version 2.0	14 12 2021	Adoption des lignes directrices après consultation publique
Version 1.0	14 01 2021	Adoption des lignes directrices pour consultation publique

Table des matières

LE COMITÉ EUROPÉEN DE LA PROTECTION DES DONNÉES,

vu l'article 70, paragraphe 1, point e), du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (ci-après le «RGPD»),

vu l'accord sur l'Espace économique européen, et notamment son annexe XI et son protocole 37, tels que modifiés par la décision du Comité mixte de l'EEE nº 154/2018 du 6 juillet 2018[1],

vu les articles 12 et 22 de son règlement intérieur,

vu la communication de la Commission au Parlement européen et au Conseil intitulée «La protection des données: un pilier de l'autonomisation des citoyens et de l'approche de l'Union à l'égard de la transition numérique - deux années d'application du règlement général sur la protection des données»[2],

A ADOPTÉ LES LIGNES DIRECTRICES SUIVANTES

1 INTRODUCTION

1. Le RGPD introduit, dans certains cas, l'obligation de notifier une violation de données à caractère personnel à l'autorité de contrôle nationale compétente (ci-après l'«autorité de contrôle») et de communiquer la violation aux personnes physiques dont les données à caractère personnel ont été affectées par la violation (articles 33 et 34).

2. Le groupe de travail «article 29» a déjà publié en octobre 2017 des orientations générales sur la notification des violations de données, analysant les sections pertinentes du RGPD (lignes directrices sur la notification de violations de données à caractère personnel en vertu du règlement 2016/679, WP 250) (ci-après les «lignes directrices WP250»)[3]. Toutefois, en raison de leur nature et de leur calendrier, ces lignes directrices n'ont pas abordé de manière suffisamment détaillée toutes les questions pratiques. Par conséquent, il est apparu nécessaire de disposer de lignes directrices axées sur la pratique et fondées sur les cas, qui s'appuient sur l'expérience acquise par les autorités de contrôle depuis que le RGPD est applicable.

3. Le présent document est destiné à compléter les lignes directrices WP250 et reflète les expériences communes des autorités de contrôle de l'EEE depuis l'entrée en vigueur du RGPD. Son objectif est d'aider

[1] Dans le présent document, on entend par «États membres» les «États membres de l'EEE».

[2] COM(2020) 264 final du 24 juin 2020.

[3] G29 WP250 rév.1, 6 février 2018, Lignes directrices sur la notification de violations de données à caractère personnel en vertu du règlement (CE) n° 2016/679 — approuvées par le comité européen de la protection des données, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052

les responsables du traitement à décider de la manière de traiter les violations de données et des facteurs à prendre en considération lors de l'évaluation des risques.

4. Dans le cadre de toute tentative de remédier à une violation, le responsable du traitement et le sous-traitant doivent, en premier lieu, être en capacité d'identifier un tel cas. Dans le RGPD, la «violation de données à caractère personnel» est définie, à l'article 4, point 12), comme étant «une violation de la sécurité des données entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données».

5. Dans son avis 03/2014 sur la notification des violations de données à caractère personnel[4] et dans ses lignes directrices WP250, le GT29 a expliqué que les violations pouvaient être classées selon les trois principes bien connus en matière de sécurité de l'information suivants:

   - «violation de la confidentialité» – la divulgation ou l'accès non autorisés ou accidentels à des données à caractère personnel;
   - «violation de l'intégrité» – l'altération non autorisée ou accidentelle de données à caractère personnel;
   - «violation de la disponibilité» – la destruction ou la perte accidentelles ou non autorisées de l'accès à des données à caractère personnel[5].

6. Une violation peut potentiellement avoir une série d'effets négatifs importants sur les individus, qui peuvent entraîner un préjudice physique, matériel ou moral. Le RGPD explique que cela peut inclure la perte de contrôle sur leurs données à caractère personnel, la limitation de leurs droits, la discrimination, le vol ou l'usurpation d'identité, la perte financière, le renversement non autorisé du processus de pseudonymisation, l'atteinte à la réputation et la perte de confidentialité de données à caractère personnel protégées par le secret professionnel. Elle peut également inclure tout autre dommage économique ou social important pour ces personnes. L'une des obligations les plus importantes du responsable du traitement est d'évaluer ces risques pour les droits et libertés des personnes concernées et de mettre en œuvre les mesures techniques et organisationnelles appropriées pour y faire face.

7. En conséquence, le RGPD impose au responsable du traitement:

   - de documenter toute violation de données à caractère personnel, en indiquant les faits concernant la violation des données à caractère personnel, ses effets et les mesures prises pour y remédier[6];

[4] G29 WP213, 25 mars 2014, Avis 03/2014 sur la notification des violations de données à caractère personnel, p. 5, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm#maincontentSec4.

[5] Voir les lignes directrices WP 250, p. 7. — Il convient de tenir compte du fait qu'une violation de données peut concerner soit une catégorie, soit plusieurs catégories simultanément ou de manière combinée.

[6] Article 33, paragraphe 5, du RGPD.

- de notifier la violation de données à caractère personnel à l'autorité de contrôle, à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques[7];
- de communiquer la violation de données à caractère personnel à la personne concernée lorsque la violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique[8].

8. Les violations de données sont des problèmes en soi, mais elles peuvent également être des symptômes d'un régime de sécurité des données vulnérable et potentiellement obsolète, elles peuvent également indiquer qu'il convient de remédier aux faiblesses du système. D'une manière générale, il est toujours préférable de prévenir les violations de données en se préparant à l'avance, étant donné que plusieurs de leurs conséquences sont par nature irréversibles. Avant qu'un responsable du traitement puisse évaluer *pleinement* le risque découlant d'une violation causée par une forme d'attaque, il convient d'identifier la cause première du problème, afin de déterminer si les vulnérabilités qui ont donné lieu à l'incident sont toujours présentes et sont donc toujours exploitables. Dans de nombreux cas, le responsable du traitement est en mesure de déceler que l'incident est susceptible d'engendrer un risque et doit donc être notifié. Dans d'autres cas, il n'est pas nécessaire de reporter la notification jusqu'à ce que le risque et l'incidence de la violation aient été pleinement évalués, étant donné que l'évaluation complète des risques peut avoir lieu parallèlement à la notification et que les informations ainsi obtenues peuvent être communiquées à l'autorité de contrôle de manière échelonnée sans autre retard indu[9].

9. La violation devrait être notifiée lorsque le responsable du traitement estime qu'elle est susceptible d'engendrer un risque pour les droits et libertés de la personne concernée. Les responsables du traitement devraient procéder à cette évaluation au moment où ils prennent connaissance de la violation. Le responsable du traitement ne devrait pas attendre un examen technico-légal détaillé et des mesures d'atténuation (précoces) avant d'évaluer si la violation de données est susceptible ou non d'entraîner un risque et devrait donc être notifiée.

10. Si un responsable du traitement évalue lui-même le risque comme improbable, mais que ce dernier finit par se matérialiser, l'autorité de contrôle compétente peut faire usage de ses pouvoirs correctifs et recourir à des sanctions.

11. Chaque responsable du traitement et sous-traitant devrait disposer de plans et de procédures pour traiter d'éventuelles violations de données. Les organisations devraient disposer de lignes hiérarchiques claires et de personnes responsables de certains aspects du processus de récupération.

12. La formation et la sensibilisation du personnel du responsable du traitement et du sous-traitant aux questions de protection des données, axées sur la gestion des violations de données à caractère personnel (identification d'un incident de violation de données à caractère personnel et autres mesures à prendre, etc.) sont également essentielles pour les responsables du traitement et les sous-traitants. Cette formation devrait être répétée régulièrement, en fonction du type d'activité de traitement et de la taille

[7] Article 33, paragraphe 1, du RGPD.

[8] Article 34, paragraphe 1, du RGPD.

[9] Article 33, paragraphe 4, du RGPD.

du responsable du traitement, en tenant compte des tendances les plus récentes et des alertes provenant de cyberattaques ou d'autres incidents de sécurité.

13. Le principe de responsabilité et le concept de protection des données dès la conception pourraient intégrer une analyse qui viendrait alimenter un «guide du traitement des violations de données à caractère personnel» d'un responsable du traitement et d'un sous-traitant, qui vise à établir des faits pour chaque aspect du traitement à chaque étape majeure de l'opération. Un tel document préparé à l'avance fournirait une source d'information beaucoup plus rapide pour permettre aux responsables du traitement et aux sous-traitants d'atténuer les risques et de remplir leurs obligations sans retard injustifié. Cela garantirait que si une violation de données à caractère personnel devait se produire, les personnes au sein de l'organisation sauraient ce qu'il convient de faire et que l'incident serait plus que probablement traité plus rapidement qu'en l'absence de mesures d'atténuation ou de plan.

14. Bien que les cas présentés ci-dessous soient fictifs, ils reposent sur des cas typiques tirés de l'expérience collective des autorités de contrôle en matière de notifications de violations de données. Les analyses proposées se rapportent explicitement aux cas examinés, mais dans le but d'aider les responsables du traitement à évaluer leurs propres violations de données. Toute modification des circonstances des cas décrits ci-dessous peut entraîner des niveaux de risque différents ou plus importants, ce qui nécessite des mesures différentes ou supplémentaires. Ces lignes directrices structurent les cas en fonction de certaines catégories de violations (par exemple, les attaques par rançongiciel). Certaines mesures d'atténuation sont nécessaires dans chaque cas lorsqu'il s'agit de traiter une certaine catégorie de violations. Ces mesures ne sont pas nécessairement répétées dans chaque analyse relevant de la même catégorie de violations. Pour les cas appartenant à la même catégorie, seules les différences sont indiquées. Par conséquent, le lecteur doit lire tous les cas pertinents pour la catégorie de violations concernée afin d'identifier et de distinguer toutes les mesures appropriées à prendre.

15. La documentation interne relative à une violation est une obligation indépendante des risques liés à la violation et doit être exécutée dans chaque cas. Les cas présentés ci-dessous tentent d'apporter un éclairage sur la question de savoir s'il convient ou non de notifier la violation à l'autorité de contrôle et de la communiquer aux personnes concernées.

2 RANÇONGICIEL

16. Une cause fréquente d'une notification de violation de données est une attaque par rançongiciel subie par le responsable du traitement. Dans ces cas, un code malveillant chiffre les données à caractère personnel, et l'auteur de l'attaque demande ensuite au responsable du traitement une rançon en échange du code de déchiffrement. Ce type d'attaque peut généralement être qualifié de violation de la disponibilité, mais souvent aussi de violation de la confidentialité.

2.1 CAS N° 01: rançongiciel avec sauvegarde appropriée et sans exfiltration

Les systèmes informatiques d'une petite entreprise manufacturière ont été exposés à une attaque par rançongiciel et les données stockées dans ces systèmes ont été chiffrées. Le responsable du traitement a utilisé le chiffrement au repos, de sorte que toutes les données consultées par le rançongiciel ont été stockées sous une forme chiffrée à l'aide d'un algorithme de chiffrement de pointe. La clé de déchiffrement n'a pas été compromise lors de l'attaque, c'est-à-dire que l'auteur de l'attaque ne pouvait ni y accéder, ni l'utiliser indirectement. En conséquence, l'auteur de l'attaque n'a eu accès qu'à des données à caractère personnel chiffrées. En particulier, ni le système de messagerie électronique de la société, ni les systèmes clients utilisés pour y accéder n'ont été affectés. L'entreprise utilise l'expertise d'une entreprise de cybersécurité externe pour enquêter sur l'incident. Des fichiers journaux retraçant tous les flux de données quittant l'entreprise (y compris les courriers électroniques sortants) sont disponibles. Après avoir analysé les fichiers de journalisation et les données collectées par les systèmes de détection que l'entreprise a déployés, une enquête interne soutenue par la société de cybersécurité externe a déterminé *avec certitude* que l'auteur de l'attaque avait uniquement chiffré les données, sans les exfiltrer. Les fichiers journaux ne montrent aucun flux de données vers l'extérieur au cours de la période de l'attaque. Les données à caractère personnel concernées par la violation concernent les clients et les employés de l'entreprise, soit quelques dizaines de personnes au total. Une sauvegarde était facilement disponible et les données ont été rétablies quelques heures après la perpétration de l'attaque. La violation n'a eu aucune conséquence sur le fonctionnement quotidien du responsable du traitement. Il n'y a eu aucun retard dans les paiements des salariés ou dans le traitement des demandes des clients.

17. En l'espèce, les éléments suivants ont été obtenus à partir de la définition d'une «violation de données à caractère personnel»: une violation de la sécurité a entraîné une altération non autorisée des données à caractère personnel conservées et l'accès non autorisé à de telles données.

2.1.1 Cas N° 01 — Mesures préalables et évaluation des risques

18. Comme pour tous les risques posés par des acteurs extérieurs, la probabilité qu'une attaque par rançongiciel soit couronnée de succès peut être considérablement réduite en renforçant la sécurité de l'environnement de contrôle des données. La plupart de ces violations peuvent être évitées en veillant à ce que des mesures de sécurité organisationnelles, physiques et technologiques appropriées soient mises en œuvre. Il s'agit, par exemple, d'une bonne gestion des correctifs et de l'utilisation d'un système approprié de détection des logiciels malveillants. Le fait de disposer d'un système de sauvegarde approprié et séparé contribuera à atténuer les conséquences d'une attaque réussie si elle devait se produire. En outre, un programme d'éducation, de formation et de sensibilisation à la sécurité des employés (SETA) contribuera à prévenir et à reconnaître ce type d'attaque. (Une liste des mesures recommandées figure à la section 2.5.) Parmi ces mesures, une gestion des correctifs adéquate qui garantit que les systèmes sont à jour et que toutes les vulnérabilités connues des systèmes déployés sont réparées est l'une des plus importantes, étant donné que la plupart des attaques par rançongiciel exploitent des vulnérabilités bien connues.

19. Lors de l'évaluation des risques, le responsable du traitement devrait enquêter sur la violation et déterminer le type de code malveillant afin de comprendre les conséquences possibles de l'attaque. Parmi ces risques à prendre en considération figure le risque que les données aient été exfiltrées sans laisser de trace dans les journaux des systèmes.

20. Dans cet exemple, l'auteur de l'attaque a eu accès à des données à caractère personnel et la confidentialité du texte chiffré contenant des données à caractère personnel a été compromise. Toutefois, aucune donnée susceptible d'avoir été exfiltrée ne peut être lue ou utilisée par l'auteur de l'attaque, du

moins pour le moment. La technique de chiffrement utilisée par le responsable du traitement est conforme à l'état de la technique. La clé de déchiffrement n'a pas été compromise et ne pouvait probablement pas non plus être déterminée par d'autres moyens. En conséquence, les risques liées à la confidentialité pour les droits et libertés des personnes physiques sont réduits au minimum, empêchant ainsi les progrès cryptanalytiques qui rendent les données chiffrées intelligibles à l'avenir.

21. Le responsable du traitement devrait tenir compte du risque encouru par les personnes physiques du fait de la violation[10]. Dans ce cas, il semble que les risques pour les droits et libertés des personnes concernées résultent du manque de disponibilité des données à caractère personnel et que la confidentialité des données à caractère personnel ne soit pas compromise[11]. Dans cet exemple, les effets négatifs de la violation ont été atténués assez peu de temps après la survenance de la violation. Le fait de disposer d'un régime de sauvegarde adéquat[12] rend les effets de la violation moins graves et le responsable du traitement a pu y recourir efficacement.

22. En ce qui concerne la gravité des conséquences pour les personnes concernées, seules des conséquences mineures ont pu être identifiées étant donné que les données concernées ont été rétablies en quelques heures, que la violation n'a pas eu de conséquences sur le fonctionnement quotidien du responsable du traitement et n'a eu aucun effet significatif sur les personnes concernées (par exemple, le versement des salaires ou le traitement des demandes des clients).

2.1.2 CAS N° 01 — Atténuation et obligations

23. En l'absence de sauvegarde, peu de mesures peuvent être prises par le responsable du traitement pour remédier à la perte de données à caractère personnel, et les données doivent être à nouveau collectées. Toutefois, dans ce cas particulier, les conséquences de l'attaque pourraient être effectivement maîtrisées en rétablissant tous les systèmes compromis vers un état propre connu pour être exempt de code malveillant, en réglant les vulnérabilités et en rétablissant les données touchées peu après l'attaque. En

---

[10] Pour des orientations sur les opérations de traitement «susceptibles d'engendrer un risque élevé», voir le groupe de travail Article 29 «Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est «susceptible d'engendrer un risque élevé» aux fins du règlement 2016/679», WP248 rév. 01, approuvé par le comité européen de la protection des données, https://ec.europa.eu/newsroom/article29/items/611236, p. 9.

[11] Techniquement, le chiffrement des données impliquera un «accès» aux données originales et, dans le cas d'un rançongiciel, la suppression de l'original — le code de rançongiciel doit avoir accès aux données pour les chiffrer, et supprimer les données originales. L'auteur d'une attaque peut prendre une copie de l'original avant la suppression, mais les données à caractère personnel ne seront pas toujours extraites. Au fur et à mesure que l'enquête d'un responsable du traitement progresse, de nouvelles informations peuvent être mises au jour et faire changer cette évaluation. L'accès qui entraîne, de manière illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel ou un risque pour la sécurité d'une personne concernée, même en l'absence d'interprétation des données, peut être aussi sévère que l'accès avec interprétation des données à caractère personnel.

[12] Les procédures de sauvegarde devraient être structurées, cohérentes et reproductibles. Des exemples de procédures de sauvegarde sont la méthode 3-2-1 et la méthode GFS (grandfather-father-son). Toute méthode devrait toujours être testée pour vérifier l'efficacité de la couverture et quand les données doivent être rétablies. Les essais devraient également être répétés à intervalles réguliers, en particulier lorsque des changements surviennent dans l'opération de traitement ou dans le cadre de celle-ci afin de garantir l'intégrité du système.

l'absence de sauvegarde, les données sont perdues et la gravité peut s'accroître, car il peut aussi en aller de même pour les risques ou les incidences pour les personnes.

24. La ponctualité d'une restauration efficace des données à partir de la sauvegarde facilement disponible est une variable essentielle lors de l'analyse de la violation. La définition d'un délai approprié pour rétablir les données compromises dépend des circonstances uniques de la violation en cause. Le RGPD dispose qu'une violation de données à caractère personnel doit être notifiée dans les meilleurs délais et, si possible, au plus tard après 72 heures. Par conséquent, il pourrait être établi que le dépassement du délai de 72 heures n'est pas souhaitable en tout état de cause, mais lorsque l'on traite des cas présentant un niveau de risque élevé, le respect même de ce délai peut être considéré comme insatisfaisant.

25. Dans ce cas, à la suite d'une analyse d'impact détaillée et d'un processus de réponse aux incidents, le responsable du traitement a établi que la violation était peu susceptible d'engendrer un risque pour les droits et libertés des personnes physiques, de sorte qu'aucune communication aux personnes concernées n'est nécessaire et que la violation ne nécessite pas de notification à l'autorité de contrôle. Toutefois, comme toutes les violations de données, elle devrait être documentée conformément à l'article 33, paragraphe 5. L'organisation peut également avoir besoin (ou être ultérieurement obligée par l'autorité de contrôle) de mettre à jour et de corriger ses mesures et procédures organisationnelles et techniques de gestion de la sécurité des données à caractère personnel et d'atténuation des risques. Dans le cadre de cette mise à jour et de cette correction, l'organisation devrait mener une enquête approfondie sur la violation et déterminer les causes et les méthodes utilisées par l'auteur de l'attaque afin d'éviter tout événement similaire à l'avenir.

Actions nécessaires fondées sur les risques recensés		
Documentation interne	Notification à l'autorité de contrôle	Communication aux personnes concernées
✓	X	X

2.2 CAS N° 02: rançongiciel sans sauvegarde adéquate

L'un des ordinateurs utilisés par une entreprise agricole a été exposé à une attaque par rançongiciel et ses données ont été chiffrées par l'auteur de l'attaque. L'entreprise utilise l'expertise d'une entreprise externe chargée de la cybersécurité pour surveiller son réseau. Des fichiers de journalisation retraçant tous les flux de données quittant l'entreprise (y compris les courriers électroniques sortants) sont disponibles. Après avoir analysé les fichiers journaux et les données collectées par les autres systèmes de détection, l'enquête interne appuyée par la société de cybersécurité, a déterminé que l'auteur de l'attaque avait uniquement chiffré les données, sans les exfiltrer. Les fichiers journaux ne montrent aucun flux de données vers l'extérieur au cours de la période de l'attaque. Les données à caractère personnel concernées par la violation concernent les employés et les clients de l'entreprise, soit une dizaine de personnes au total. Aucune catégorie particulière de données n'a été affectée. Aucune sauvegarde n'était disponible sous forme électronique. La plupart des données ont été rétablies à partir de sauvegardes papier. Le rétablissement des données a pris 5 jours ouvrables et a entraîné des retards mineurs dans la livraison des commandes aux clients.

2.2.1 CAS N° 02 — Mesures préalables et évaluation des risques

26. Le responsable du traitement des données aurait dû adopter les mêmes mesures préalables que celles mentionnées à la partie 2.1 et à la section 2.9. La principale différence par rapport au cas précédent est l'absence de sauvegarde électronique et l'absence de chiffrement au repos. Il en résulte des différences critiques dans les étapes suivantes.

27. Lors de l'évaluation des risques, le responsable du traitement devrait étudier la méthode d'infiltration et déterminer le type de code malveillant afin de comprendre les conséquences possibles de l'attaque. Dans cet exemple, le rançongiciel chiffrait les données à caractère personnel sans les exfiltrer. En conséquence, il semble que les risques pour les droits et libertés des personnes concernées résultent du manque de disponibilité des données à caractère personnel et que la confidentialité des données à caractère personnel ne soit pas compromise. Un examen approfondi des fichiers journaux de pare-feu et de ses implications est essentiel pour déterminer le risque. Le responsable du traitement devrait présenter les conclusions factuelles de ces enquêtes sur demande.

28. Le responsable du traitement doit garder à l'esprit que si l'attaque est plus sophistiquée, le logiciel malveillant possède la fonctionnalité de modifier les fichiers journaux et de supprimer la trace. Ainsi, étant donné que les journaux ne sont pas transmis ou reproduits sur un serveur de journalisation central, même après une enquête approfondie qui a établi que les données à caractère personnel n'ont pas été exfiltrées par l'auteur de l'attaque, le responsable du traitement ne peut affirmer que l'absence d'enregistrement du journal prouve l'absence d'exfiltration, de sorte que la probabilité d'une violation de la confidentialité ne peut être totalement écartée.

29. Le responsable du traitement devrait évaluer les risques de cette violation[13] si l'auteur de l'attaque a eu accès aux données. Au cours de l'évaluation des risques, le responsable du traitement devrait également tenir compte de la nature, de la sensibilité, du volume et du contexte des données à caractère personnel concernées par la violation. Dans ce cas, aucune catégorie particulière de données à caractère personnel n'est touchée et la quantité de données objets de la violation et le nombre de personnes concernées sont faibles.

30. La collecte d'informations précises sur l'accès non autorisé est essentielle pour déterminer le niveau de risque et prévenir une nouvelle attaque ou la poursuite d'une attaque. Si les données avaient été copiées à partir de la base de données, cela aurait évidemment constitué un facteur d'augmentation des risques. En cas d'incertitude quant aux spécificités de l'accès illicite, le scénario le plus défavorable devrait être pris en considération et le risque devrait être évalué en conséquence.

31. L'absence de base de données de sauvegarde peut être considérée comme un facteur renforçant les risques en fonction de la gravité des conséquences, pour les personnes concernées, du manque de disponibilité des données.

2.2.2 CAS N° 02 — Atténuation et obligations

32. En l'absence de sauvegarde, peu de mesures peuvent être prises par le responsable du traitement pour remédier à la perte de données à caractère personnel, et les données doivent être à nouveau collectées, à moins qu'une autre source ne soit disponible (par exemple, des courriels de confirmation des commandes). En l'absence de sauvegarde, les données peuvent être perdues et la gravité dépendra de l'impact pour les personnes.

[13] Pour des orientations sur les traitements «susceptibles d'engendrer un risque élevé», voir la note de bas de page 10 ci-dessus.

33. La restauration des données ne devrait pas s'avérer excessivement problématique[14] si les données sont toujours disponibles sur papier, mais en l'absence d'une base de données électronique de sauvegarde, une notification à l'autorité de contrôle est jugée nécessaire, étant donné que la restauration des données a pris du temps et pourrait entraîner des retards dans la livraison des commandes aux clients et qu'une quantité considérable de métadonnées (par exemple, les journaux, les horodatages) pourrait ne pas être récupérable.

34. L'information des personnes concernées sur la violation peut également dépendre de la durée de l'indisponibilité des données à caractère personnel et des difficultés qu'elle pourrait entraîner dans le fonctionnement du responsable du traitement (par exemple, retards dans le versement des salaires). Étant donné que ces retards de paiement et de livraison peuvent entraîner des pertes financières pour les personnes dont les données ont été compromises, on pourrait également soutenir que la violation est susceptible d'engendrer un risque élevé. En outre, il pourrait ne pas être possible d'éviter d'informer les personnes concernées si leur contribution est nécessaire pour rétablir les données chiffrées.

35. Ce cas sert d'exemple à une attaque par rançongiciel présentant un risque pour les droits et libertés des personnes concernées, mais n'atteignant pas un risque élevé. Il devrait être documenté conformément à l'article 33, paragraphe 5, et notifié à l'autorité de contrôle conformément à l'article 33, paragraphe 1. L'organisation peut également avoir besoin (ou être tenue par l'autorité de contrôle) de mettre à jour et de corriger ses mesures et procédures organisationnelles et techniques de gestion de la sécurité des données à caractère personnel et d'atténuation des risques.

Actions nécessaires fondées sur les risques recensés		
Documentation interne	Notification à l'autorité de contrôle	Communication aux personnes concernées
✓	✓	**X**

[14] Cela dépendra de la complexité et de la structure des données à caractère personnel. Dans les scénarios les plus complexes, le rétablissement de l'intégrité des données, la cohérence avec les métadonnées, la garantie de relations correctes au sein des structures de données et le contrôle de l'exactitude des données peuvent nécessiter des ressources et des efforts considérables.

2.3 CAS N° 03: Rançongiciel avec sauvegarde et sans exfiltration dans un hôpital

Le système d'information d'un hôpital/centre de soins a été exposé à une attaque par rançongiciel et une part importante de ses données a été chiffrée par l'auteur de l'attaque. L'entreprise utilise l'expertise d'une entreprise de cybersécurité externe pour surveiller son réseau. Des fichiers de journalisation retraçant tous les flux de données quittant l'entreprise (y compris les courriers électroniques sortants) sont disponibles. Après avoir analysé les fichiers de journalisation et les données collectées par les autres systèmes de détection, l'enquête interne appuyée par la société de cybersécurité, a déterminé que l'auteur de l'attaque avait uniquement chiffré les données, sans les exfiltrer. Les fichiers journaux ne montrent aucun flux de données vers l'extérieur au cours de la période de l'attaque. Les données à caractère personnel concernées par la violation concernent les employés et les patients, qui représentaient des milliers de personnes. Des sauvegardes étaient disponibles sous forme électronique. La plupart des données ont été rétablies, mais cette opération a duré 2 jours ouvrables et a entraîné des retards importants dans le traitement des patients en cas d'intervention chirurgicale annulée/reportée, ainsi qu'une baisse du niveau de service en raison de

2.3.1 CAS N° 03 — Mesures préalables et évaluation des risques

36. Le responsable du traitement des données aurait dû adopter les mêmes mesures préalables que celles mentionnées à la partie 2.1 et à la section 2.5. La principale différence par rapport au cas précédent réside dans la gravité élevée des conséquences pour une partie substantielle des personnes concernées[15].

37. La quantité de données concernées par la violation et le nombre de personnes concernées sont élevés, car les hôpitaux traitent généralement de grandes quantités de données. L'indisponibilité des données a une forte incidence sur une partie substantielle des personnes concernées. En outre, il existe un risque résiduel de gravité élevée pour la confidentialité des données des patients.

38. Le type de violation, la nature, la sensibilité et le volume des données à caractère personnel concernées par la violation sont importants. Bien qu'une sauvegarde des données ait existé et qu'elle puisse être rétablie en quelques jours, un risque élevé subsiste en raison de la gravité des conséquences, pour les personnes concernées, du manque de disponibilité des données au moment de l'attaque et dans les jours suivants.

2.3.2 CAS N° 03 — Atténuation et obligations

39. Une notification à l'autorité de contrôle est jugée nécessaire, étant donné que des catégories particulières de données à caractère personnel sont concernées et que la restauration des données pourrait prendre beaucoup de temps, ce qui entraînerait des retards importants dans les soins prodigués aux patients. L'information des personnes concernées sur la violation est nécessaire en raison de l'impact pour les patients, même après la restauration des données chiffrées. Si les données relatives à tous les patients traités à l'hôpital au cours des dernières années ont été chiffrées, seuls les patients qui devaient être traités à l'hôpital pendant la période où le système informatique n'était pas disponible ont été touchés. Le responsable du traitement devrait communiquer directement la violation de données à ces patients.

[15] Pour des orientations sur les traitements «susceptibles d'engendrer un risque élevé», voir la note de bas de page 10 ci-dessus.

La communication directe aux autres patients dont certains n'ont peut-être pas séjourné à l'hôpital depuis plus de vingt ans peut ne pas être exigée en raison de l'exception prévue à l'article 34, paragraphe 3, point c). Dans un tel cas, il est plutôt procédé à une communication publique[16] ou à une mesure similaire permettant aux personnes concernées d'être informées de manière tout aussi efficace. Dans ce cas, l'hôpital devrait rendre publique l'attaque par rançongiciel et ses effets.

40. Le présent cas sert d'exemple à une attaque par rançongiciel présentant un risque élevé pour les droits et libertés des personnes concernées. Il devrait être documenté conformément à l'article 33, paragraphe 5, notifié à l'autorité de contrôle conformément à l'article 33, paragraphe 1, et communiqué aux personnes concernées conformément à l'article 34, paragraphe 1. L'organisation doit également mettre à jour et corriger ses mesures et procédures organisationnelles et techniques en matière de sécurité des données à caractère personnel et d'atténuation des risques.

Actions nécessaires fondées sur les risques recensés		
Documentation interne	Notification à l'autorité de contrôle	Communication aux personnes concernées
✓	✓	✓

2.4 CAS N° 04: rançongiciel sans sauvegarde et avec exfiltration

Le serveur d'une entreprise de transport public a été exposé à une attaque par rançongiciel et ses données ont été chiffrées par l'auteur de l'attaque. D'après les conclusions de l'enquête interne, l'auteur de l'attaque a non seulement chiffré les données, mais les a aussi exfiltrées. Ont été visées par l'attaque des données à caractère personnel des clients et des salariés, ainsi que celles de milliers de personnes utilisant les services de l'entreprise (par exemple, l'achat de billets en ligne). Outre les données d'identité de base, les numéros de carte d'identité et les données financières telles que les données relatives à la carte de crédit sont concernés par la violation. Une base de données de sauvegarde existait, mais elle a également été chiffrée par l'auteur de l'attaque.

2.4.1 CAS N° 04 — Mesures préalables et évaluation des risques

41. Le responsable du traitement des données aurait dû adopter les mêmes mesures préalables que celles mentionnées à la partie 2.1 et à la section 2.5. Bien qu'un système de sauvegarde ait été prévu, il a également été visé par l'attaque. La prise de telles dispositions soulève à elle seule des questions sur la qualité des mesures de sécurité informatique antérieures du responsable du traitement et devrait faire l'objet d'un examen plus approfondi au cours de l'enquête, étant donné que, dans un régime de sauvegarde bien conçu, les sauvegardes multiples doivent être stockées en toute sécurité sans accès à

[16] Le considérant 86 du RGPD explique que «[i]*l convient que de telles communications aux personnes concernées soient effectuées aussi rapidement qu'il est raisonnablement possible et en coopération étroite avec l'autorité de contrôle, dans le respect des directives données par celle-ci ou par d'autres autorités compétentes, telles que les autorités répressives. Par exemple, la nécessité d'atténuer un risque immédiat de dommage pourrait justifier d'adresser rapidement une communication aux personnes concernées, alors que la nécessité de mettre en œuvre des mesures appropriées empêchant la poursuite de la violation des données à caractère personnel ou la survenance de violations similaires peut justifier un délai plus long pour la communication*».

partir du système principal, faute de quoi elles pourraient être compromises dans le cadre d'une même attaque. En outre, les attaques par rançongiciel peuvent ne pas être découvertes pendant des jours, chiffrant lentement des données rarement utilisées. Cela peut rendre inutiles de multiples sauvegardes, de sorte que les sauvegardes devraient également être réalisées de manière périodique et isolée. Cela augmenterait la capacité à restaurer les informations, même en cas de très nombreuses données perdues.

42. Cette violation concerne non seulement la disponibilité des données, mais aussi la confidentialité, étant donné que l'auteur de l'attaque peut avoir modifié et/ou copié des données provenant du serveur. Par conséquent, ce type de violation entraîne un risque élevé[17].

43. La nature, la sensibilité et le volume des données à caractère personnel augmentent encore les risques, car le nombre de personnes concernées est élevé, tout comme la quantité globale de données à caractère personnel concernées. Outre les données d'identité de base, les documents d'identité et les données financières telles que les données relatives à la carte de crédit sont également concernés. Une violation de données concernant ces types de données présente un risque élevé en soi et, si elles sont traitées ensemble, elles pourraient être utilisées, entre autres, à des fins d'usurpation d'identité ou de fraude.

44. En raison d'une mauvaise gestion technique du serveur ou de contrôles organisationnels déficients, les fichiers de sauvegarde ont été affectés par le rançongiciel, ce qui a empêché la restauration des données et accru le risque.

45. Cette violation de données présente un risque élevé pour les droits et libertés des personnes, car elle pourrait entraîner à la fois une perte matérielle (par exemple, une perte financière étant donné que les données des cartes de crédit ont été affectées) et un préjudice moral (par exemple, usurpation d'identité ou fraude dans la mesure où les données des cartes d'identité ont été visées).

2.4.2 CAS N° 04 — Atténuation et obligations

46. La communication aux personnes concernées est essentielle pour qu'elles puissent prendre les mesures nécessaires pour éviter des dommages matériels (par exemple bloquer leur carte de crédit).

47. En plus de documenter la violation conformément à l'article 33, paragraphe 5, une notification à l'autorité de contrôle est également obligatoire dans ce cas (article 33, paragraphe 1) et le responsable du traitement est également tenu de communiquer la violation aux personnes concernées (article 34, paragraphe 1). Pour ce qui est de la seconde obligation, une telle communication pourrait être effectuée sur une base individuelle, mais pour les personnes dont les données de contact ne sont pas disponibles, le responsable du traitement devrait le faire publiquement, à condition que cette communication ne soit pas susceptible d'entraîner des conséquences négatives supplémentaires pour les personnes concernées, par exemple au moyen d'une notification sur son site web. Dans ce dernier cas, une communication précise et claire est requise, à la vue de tous sur la page d'accueil du responsable du traitement, avec des renvois exacts aux dispositions du RGPD concernées. L'organisation peut également être amenée à mettre à jour et à corriger ses mesures et procédures organisationnelles et techniques en matière de sécurité des données à caractère personnel et d'atténuation des risques.

Actions nécessaires fondées sur les risques recensés

[17] Pour des orientations sur les traitements «*susceptibles d'engendrer un risque élevé*», voir la note de bas de page 10 ci-dessus.

Documentation interne	Notification à l'autorité de contrôle	Communication aux personnes concernées
✓	✓	✓

2.5 Mesures organisationnelles et techniques pour prévenir/atténuer les effets des attaques par rançongiciel

48. Le fait qu'une attaque de rançongiciel ait pu avoir lieu est généralement le signe d'une ou de plusieurs vulnérabilités dans le système du responsable du traitement. Cela vaut également dans les cas de rançongiciels dans lesquels les données à caractère personnel ont été chiffrées, mais n'ont pas été exfiltrées. Indépendamment de l'issue et des conséquences de l'attaque, l'importance d'une évaluation globale du système de sécurité des données — en mettant particulièrement l'accent sur la sécurité informatique — ne saurait être suffisamment soulignée. Les faiblesses et les lacunes de sécurité identifiées doivent être documentées et corrigées sans délai.

49. Mesures recommandées:

(La liste des mesures suivantes n'est en aucun cas exclusive ou exhaustive. L'objectif est plutôt de fournir des idées de prévention et des solutions possibles. Chaque activité de traitement étant différente, le responsable du traitement devrait décider quelles mesures sont les plus adaptées à la situation donnée.)

- Tenir à jour le micrologiciel, le système d'exploitation et le logiciel d'application sur les serveurs, les machines clientes, les éléments actifs du réseau et toute autre machine du même LAN (y compris les appareils Wi-Fi). Veiller à ce que des mesures de sécurité informatique appropriées soient en place, en veillant à leur efficacité et en les tenant régulièrement à jour lorsque le traitement ou les circonstances changent ou évoluent. Il s'agit notamment de tenir des registres détaillés de quel correctif est appliqué à tel ou tel horodatage.
- Concevoir et organiser des systèmes et des infrastructures de traitement pour segmenter ou isoler les systèmes et réseaux de données afin d'éviter la propagation de logiciels malveillants au sein de l'organisation et vers des systèmes externes.
- L'existence d'une procédure de sauvegarde actualisée, sécurisée et testée. Les supports de sauvegarde à moyen et long terme devraient être séparés du stockage des données opérationnelles et hors de portée de tiers, même en cas d'attaque réussie (par exemple, sauvegarde progressive quotidienne et sauvegarde hebdomadaire complète).
- Mettre en œuvre un programme contre les logiciels malveillants approprié, maintenu à jour, efficace et intégré.
- Disposer d'un pare-feu et d'un système de détection et de prévention des intrusions appropriés, actualisés, efficaces et intégrés. Diriger le trafic réseau à travers le pare-feu/détection d'intrusion, même dans le cas d'un bureau à domicile ou d'un travail mobile (par exemple, en utilisant des connexions VPN associées à des mécanismes de sécurité organisationnels lors de l'accès à l'internet).
- Former les employés aux méthodes de reconnaissance et de prévention des attaques informatiques. Le responsable du traitement devrait fournir des moyens permettant de déterminer si les courriels et messages obtenus par d'autres moyens de communication sont authentiques et dignes de confiance. Les employés devraient être formés à reconnaître quand une telle attaque s'est produite, comment déconnecter le poste du réseau et s'acquitter de leur obligation de le signaler immédiatement au responsable de la sécurité.
- Insister sur la nécessité d'identifier le type de code malveillant pour voir les conséquences de l'attaque et être en mesure de trouver les mesures appropriées pour atténuer le risque. En cas d'attaque par rançongiciel réussie et d'absence de sauvegarde, des outils tels que ceux du projet «No more ransom»

(nomoreransom.org) peuvent être utilisés pour extraire des données. Toutefois, si une sauvegarde sûre est disponible, il est recommandé de rétablir les données à partir de celle-ci.

- Transmettre ou répliquer tous les journaux sur un serveur de journaux central (y compris, le cas échéant, signature ou horodatage cryptographique des entrées de journaux).
- Chiffrement fort et authentification multifactorielle, en particulier pour les accès à aux systèmes informatiques, gestion appropriée des clés et des mots de passe.
- Effectuer des tests de vulnérabilité et d'intrusion de façon périodique.
- Mettre en place un centre de réponse aux incidents de sécurité informatique (CSIRT) ou une équipe d'intervention en cas d'urgence informatique (CERT) au sein de l'organisation, ou rejoindre un CSIRT/CERT collectif. Créer un plan de réaction aux incidents, un plan de rétablissement après sinistre et un plan de continuité des activités, et veiller à ce que ces derniers soient testés de manière approfondie.
- Lors de l'évaluation des contre-mesures, l'analyse des risques devrait être réexaminée, testée et mise à jour.

3 ATTAQUES AVEC EXFILTRATIONS DE DONNÉES

50. Les attaques qui exploitent des vulnérabilités dans les services offerts par le responsable du traitement à des tiers sur l'internet, par exemple au moyen d'attaques par injection (par exemple, injection SQL, traversée de répertoires), piratage de sites web et méthodes similaires, peuvent ressembler à des attaques par rançongiciel en ce sens que le risque découle de l'action d'un tiers non autorisé, mais ces attaques visent généralement à copier, exfiltrer et abuser de données à caractère personnel à des fins malveillantes. Il s'agit donc principalement de violations de la confidentialité et, éventuellement, de l'intégrité des données. Dans le même temps, si le responsable du traitement a connaissance des caractéristiques de ce type de violations, les responsables du traitement disposent de nombreuses mesures qui peuvent réduire sensiblement le risque de voir une attaque réussir.

3.1 CAS N° 05: exfiltration des données relatives aux demandes d'emploi à partir d'un site web

Une agence pour l'emploi a été victime d'une cyberattaque, qui a placé un code malveillant sur son site internet. Ce code malveillant a rendu les informations à caractère personnel soumises au moyen de formulaires de candidature en ligne et stockées sur le serveur web accessibles à des personnes non autorisées. 213 de ces formulaires sont susceptibles d'être affectés, après analyse des données concernées, il a été établi qu'aucune catégorie particulière de données n'avait été affectée par la violation. La boîte à outils de logiciels malveillants installée possédait des fonctionnalités qui permettaient à l'auteur de l'attaque de supprimer tout historique d'exfiltration et permettait également de surveiller le traitement sur le serveur et d'obtenir la saisie des données à caractère personnel. La boîte à outils n'a été découverte qu'un mois après son installation.

3.1.1 CAS N° 05 — Mesures préalables et évaluation des risques

51. La sécurité de l'environnement du responsable du traitement des données est extrêmement importante, étant donné que la plupart de ces violations peuvent être évitées en veillant à ce que tous les systèmes soient constamment mis à jour, que les données sensibles soient chiffrées et que les applications soient développées conformément à des normes de sécurité élevées telles que l'authentification renforcée, des

mesures contre les attaques par force brute, les attaques, l'«échappement» ou le «nettoyage»[18], les saisies utilisateurs, etc. Des audits périodiques de sécurité informatique, des évaluations de la vulnérabilité et des tests de d'intrusion sont également nécessaires pour détecter à l'avance ces types de vulnérabilités et les corriger. Dans ce cas particulier, les outils de contrôle de l'intégrité des fichiers dans l'environnement de production auraient pu contribuer à détecter l'injection de code. (Une liste des mesures recommandées figure à la section 3.7).

52. Le responsable du traitement devrait toujours commencer à enquêter sur la violation en identifiant le type d'attaque et ses méthodes, afin d'évaluer les mesures à prendre. Pour que ce soit rapide et efficace, le responsable du traitement des données devrait disposer d'un plan de réaction aux incidents précisant les mesures rapides et nécessaires pour prendre le contrôle de l'incident. En l'espèce, le type de violation était un facteur d'accroissement des risques étant donné que non seulement la confidentialité des données était réduite, mais l'attaquant avait également les moyens d'apporter des modifications au système, de sorte que l'intégrité des données était également mise en doute.

53. La nature, la sensibilité et le volume des données à caractère personnel concernées par la violation devraient être évalués afin de déterminer dans quelle mesure la violation a affecté les personnes concernées. Bien qu'aucune catégorie particulière de données à caractère personnel n'ait été affectée, les données consultées contiennent des informations considérables sur les personnes physiques à partir des formulaires en ligne, et ces données pourraient être utilisées de diverses manières (ciblage par un marketing non sollicité, usurpation d'identité, etc.), de sorte que la gravité des conséquences devrait accroître le risque pour les droits et libertés des personnes concernées[19].

3.1.2 CAS N° 05 — Atténuation et obligations

54. Si possible, après avoir résolu le problème, la base de données doit être comparée à celle stockée dans une sauvegarde sécurisée. L'expérience tirée de la violation devrait être mise à profit pour la mise à jour de l'infrastructure informatique. Le responsable du traitement devrait ramener tous les systèmes informatiques concernés dans un état de propreté connu, remédier à la vulnérabilité et mettre en œuvre de nouvelles mesures de sécurité afin d'éviter des violations de données similaires à l'avenir, par exemple des contrôles d'intégrité des dossiers et des audits de sécurité. Si des données à caractère personnel ont été non seulement exfiltrées, mais également supprimées, le responsable du traitement doit prendre des mesures systématiques pour récupérer les données à caractère personnel dans l'état dans lequel elles se trouvaient avant la violation. Il peut s'avérer nécessaire de restaurer les données à partir des sauvegardes complètes, des sauvegardes incrémentales postérieures et, éventuellement, de rejouer l'ensemble des modifications apportées au traitement depuis la dernière sauvegarde incrémentale, ce qui exige que le responsable du traitement soit en mesure de reproduire les modifications apportées depuis la dernière sauvegarde. Cela pourrait exiger que le responsable du traitement fasse concevoir le système de manière à conserver les fichiers d'entrée quotidiens dans le cas où ils nécessiteraient un nouveau traitement et exige une méthode de conservation solide et une politique de conservation appropriée.

55. Compte tenu de ce qui précède, étant donné que la violation est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, les personnes concernées devraient être informées

[18] L'échappement ou le nettoyage des saisies utilisateurs est une forme de validation des saisies qui garantit que seules des données correctement formatées sont introduites dans un système d'information.

[19] Pour des orientations sur les traitements «*susceptibles d'engendrer un risque élevé*», voir la note de bas de page 10 ci-dessus.

définitivement de cette violation (article 34, paragraphe 1), ce qui signifie bien entendu que l'autorité de contrôle concernée devrait également intervenir sous la forme d'une notification de violation de données. La documentation de la violation est obligatoire en vertu de l'article 33, paragraphe 5, du RGPD et facilite l'évaluation de la situation.

Actions nécessaires fondées sur les risques recensés		
Documentation interne	Notification à l'autorité de contrôle	Communication aux personnes concernées
✓	✓	✓

3.2 CAS N° 06: exfiltration d'un mot de passe haché à partir d'un site web

Une vulnérabilité par injection SQL a été exploitée pour accéder à une base de données du serveur d'un site de cuisine. Les utilisateurs étaient uniquement autorisés à choisir des pseudonymes arbitraires comme noms d'utilisateur. L'utilisation d'adresses électroniques à cette fin a été découragée. Les mots de passe stockés dans la base de données ont été hachés à l'aide d'un algorithme fort et le sel n'a pas été compromis. Données concernées: mots de passe hachés de 1 200 utilisateurs. Dans un souci de sécurité, le responsable du traitement a informé les personnes concernées de la violation par courriel et leur a demandé de modifier leurs mots de passe, en particulier si le même mot de passe était utilisé pour d'autres services.

3.2.1 CAS N° 06 — Mesures préalables et évaluation des risques

56. Dans ce cas particulier, la confidentialité des données est compromise, mais les mots de passe figurant dans la base de données ont été hachés au moyen d'une méthode actualisée, ce qui réduirait le risque en ce qui concerne la nature, la sensibilité et le volume des données à caractère personnel. Ce cas ne présente aucun risque pour les droits et libertés des personnes concernées.

57. En outre, aucune information de contact (adresse électronique ou numéro de téléphone, par exemple) des personnes concernées n'a été compromise, ce qui signifie qu'il n'existe pas de risque significatif pour les personnes concernées d'être ciblées par des tentatives de fraude (par exemple, réception de courriels par hameçonnage ou de messages textuels et d'appels téléphoniques frauduleux). Aucune catégorie particulière de données à caractère personnel n'a été concernée.

58. Certains noms d'utilisateurs pourraient être considérés comme des données à caractère personnel, mais l'objet du site web ne permet pas de connotations négatives. Bien qu'il y ait lieu de noter que l'évaluation des risques peut changer[20], si le type de site web et les données consultées peuvent révéler des catégories particulières de données à caractère personnel (par exemple, le site web d'un parti politique ou d'un syndicat). L'utilisation d'un chiffrement de pointe pourrait atténuer les effets négatifs de la violation. Veiller à ce qu'un nombre limité de tentatives de connexion soit autorisé empêchera le succès des attaques par force brute visant à se connecter, réduisant ainsi largement les risques imposés par les auteurs d'attaques qui connaissent déjà les noms d'utilisateur.

3.2.2 CAS N° 06 — Atténuation et obligations

59. Dans certains cas, la communication aux personnes concernées pourrait être considérée comme une circonstance atténuante, étant donné que les personnes concernées sont également en mesure de prendre les mesures nécessaires pour éviter d'autres dommages résultant de la violation, par exemple en

[20] Pour des orientations sur les traitements «*susceptibles d'engendrer un risque élevé*», voir la note de bas de page 10 ci-dessus.

modifiant leur mot de passe. Dans ce cas, la notification n'était pas obligatoire, mais dans de nombreux cas, elle peut être considérée comme une bonne pratique.

60. Le responsable du traitement devrait corriger la vulnérabilité et mettre en œuvre de nouvelles mesures de sécurité afin d'éviter à l'avenir des violations de données similaires, telles que, par exemple, des audits de sécurité systématiques sur le site web.

61. La violation devrait être documentée conformément à l'article 33, paragraphe 5, mais aucune notification ou communication n'est nécessaire.

62. En outre, il est fortement recommandé de communiquer aux personnes concernées une violation impliquant des mots de passe, même lorsque les mots de passe ont été stockés à l'aide d'un hachage salé avec un algorithme conforme à l'état de la technique. L'utilisation de méthodes d'authentification permettant de ne pas devoir traiter les mots de passe du côté serveur est préférable. Les personnes concernées devraient avoir le choix de prendre des mesures appropriées en ce qui concerne leurs propres mots de passe.

Actions nécessaires fondées sur les risques recensés		
Documentation interne	Notification à l'autorité de contrôle	Communication aux personnes concernées
✓	X	X

3.3 CAS N° 07: Attaque par bourrage d'identifiants sur un site web bancaire

Une banque a subi une cyberattaque contre l'un de ses sites web bancaires en ligne. L'attaque visait à énumérer tous les identifiants d'utilisateur possibles à l'aide d'un mot de passe commun fixe. Les mots de passe sont composés de 8 chiffres. En raison de la vulnérabilité du site web, dans certains cas, des informations concernant les personnes concernées (nom, prénom, sexe, date et lieu de naissance, code fiscal, codes d'identification de l'utilisateur) ont été divulguées à l'auteur de l'attaque, même si le mot de passe utilisé n'était pas correct ou si le compte bancaire n'était plus actif. Cela a touché quelque 100 000 personnes concernées. Sur celles-ci, l'auteur de l'attaque s'est connecté avec succès à quelque 2 000 comptes qui utilisaient le mot de passe commun essayé par l'auteur de l'attaque. Après cela, le responsable du traitement a pu identifier toutes les tentatives de connexion illégitimes. Le responsable du traitement a pu confirmer que, selon les contrôles de lutte contre la fraude, aucune transaction n'avait été effectuée par ces comptes au cours de l'attaque. La banque avait connaissance de la violation de données parce que son centre d'opérations de sécurité a détecté un grand nombre de demandes de connexion dirigées vers le site web. En réponse, le responsable du traitement a bloqué la possibilité de se connecter au site web en le désactivant et en obligeant les comptes compromis à réinitialiser leur mot de passe. Le responsable du traitement n'a communiqué la violation qu'aux utilisateurs possédant les comptes compromis, c'est-à-dire aux utilisateurs dont les mots de passe ont été compromis ou dont les données ont été divulguées.

3.3.1 CAS N° 07 — Mesures préalables et évaluation des risques

63. Il est important de mentionner que les responsables du traitement de données à caractère hautement personnel[21] ont une plus grande responsabilité en ce qui concerne la sécurité adéquate des données, par exemple en disposant d'un centre d'opération de sécurité et d'autres mesures de prévention, de détection et de réaction aux incidents. Le non-respect de ces normes plus élevées se traduira certainement par des mesures plus sévères au cours de l'enquête de l'autorité de contrôle.

64. La violation concerne des données financières allant au-delà des informations relatives à l'identité et à l'identifiant de l'utilisateur, ce qui la rend particulièrement grave. Le nombre de personnes touchées est élevé.

65. Le fait qu'une violation puisse se produire dans un environnement aussi sensible met en évidence d'importantes lacunes en matière de sécurité des données dans le système du responsable du traitement et peut indiquer que l'examen et l'actualisation des mesures concernées sont «nécessaires», conformément aux articles 24, paragraphe 1, 25, paragraphe 1, et 32, paragraphe 1, du RGPD. Les données visées par l'attaque permettent l'identification unique des personnes concernées et contiennent d'autres informations les concernant (y compris leur sexe, leur date et leur lieu de naissance). En outre, elles peuvent être utilisées par l'auteur de l'attaque pour deviner les mots de passe des clients ou mener une campagne d'hameçonnage à l'intention des clients de la banque.

66. Pour ces raisons, la violation de données a été jugée susceptible d'engendrer un risque élevé pour les droits et libertés de toutes les personnes concernées[22]. Par conséquent, la survenance de dommages matériels (par exemple, pertes financières) et non matériels (usurpation d'identité ou fraude) est un résultat concevable.

3.3.2 CAS N° 07 — Atténuation et obligations

67. Les mesures du responsable du traitement mentionnées dans la description du cas sont adéquates. À la suite de cette violation, il a également corrigé la vulnérabilité du site web et pris d'autres mesures pour empêcher de futures violations de données similaires, telles que l'ajout d'une authentification à deux facteurs sur le site web concerné et le passage à une authentification du client renforcée.

68. Le fait de documenter la violation conformément à l'article 33, paragraphe 5, du RGPD et d'en informer l'autorité de contrôle n'est pas facultatif dans ce scénario. En outre, le responsable du traitement devrait informer les 100 000 personnes concernées (y compris les personnes concernées dont les comptes n'ont pas été compromis), conformément à l'article 34 du RGPD.

Actions nécessaires fondées sur les risques recensés		
Documentation interne	Notification à l'autorité de contrôle	Communication aux personnes concernées
✓	✓	✓

[21] Telles que l'information des personnes concernées sur les méthodes de paiement telles que les numéros de carte, les comptes bancaires, les paiements en ligne, les fiches de paie, les relevés bancaires, les études économiques ou toute autre information susceptible de révéler des informations économiques concernant les personnes concernées.

[22] Pour des orientations sur les traitements «*susceptibles d'engendrer un risque élevé*», voir la note de bas de page 10 ci-dessus.

3.4 Mesures organisationnelles et techniques pour prévenir/atténuer les effets d'attaques de piratage informatique

69. Tout comme dans le cas d'attaques par rançongiciel, indépendamment de l'issue et des conséquences de l'attaque, la réévaluation de la sécurité informatique est obligatoire pour les responsables du traitement dans des cas similaires.

70. Mesures recommandées[23]:

(*La liste des mesures suivantes n'est en aucun cas exclusive ni exhaustive. L'objectif est plutôt de fournir des idées de prévention et des solutions possibles. Chaque activité de traitement étant différente, le responsable du traitement devrait décider quelles mesures sont les plus adaptées à la situation donnée.*)

- Procéder à un chiffrement et à une gestion des clés sophistiqués, en particulier lorsque des mots de passe, des données sensibles ou financières sont en cours de traitement. Le hachage cryptographique et le salage pour des informations secrètes (mots de passe) sont toujours préférés au chiffrement des mots de passe. Il est préférable de recourir à des méthodes d'authentification qui évitent de devoir traiter les mots de passe du côté serveur.
- Tenir à jour du système (logiciel et micrologiciel). Veiller à ce que toutes les mesures de sécurité informatique soient en place, en veillant à leur efficacité et en les mettant régulièrement à jour lorsque le traitement ou les circonstances changent ou évoluent. Afin de pouvoir démontrer le respect de l'article 5, paragraphe 1, point f), conformément à l'article 5, paragraphe 2, du RGPD, le responsable du traitement devrait tenir un registre de toutes les mises à jour effectuées, y compris le moment où elles ont été appliquées.
- Utiliser des méthodes d'authentification renforcée telles que l'authentification à deux facteurs et les serveurs d'authentification, complétées par une politique actualisée en matière de mot de passe.
- Les normes de développement sécurisées comprennent le filtrage de saisies utilisateurs (en utilisant, dans la mesure du possible, une liste blanche), l'échappement des saisies utilisateurs et des mesures de prévention de la force brute (telles que la limitation de la quantité maximale de réessais). Les «pare-feux d'applications web» peuvent contribuer à l'utilisation efficace de cette technique.
- Des privilèges d'utilisateurs solides et une politique de gestion du contrôle d'accès sont en place.
- Utiliser des pare-feux, des systèmes de détection d'intrusion et d'autres systèmes de défense périphériques appropriés, modernes, efficaces et intégrés.
- Procéder à des audits systématiques de la sécurité informatique et à des évaluations de la vulnérabilité (tests d'intrusion).
- Procéder à des examens et à des tests réguliers afin de garantir que les sauvegardes peuvent être utilisées pour rétablir toute donnée dont l'intégrité ou la disponibilité a été compromise.
- Pas d'identifiant de session dans l'URL en texte clair.

[23] Pour le développement d'applications web sécurisées, voir également: https://www.owasp.org/index.php/Main_Page

4 SOURCE DE RISQUES INTERNES D'ORIGINE HUMAINE

71. Il convient de souligner le rôle des erreurs humaines dans les violations de données à caractère personnel, en raison de leur apparence commune. Étant donné que ces types de violations peuvent être à la fois intentionnels et non intentionnels, il est très difficile pour les responsables du traitement d'identifier les vulnérabilités et d'adopter des mesures pour les éviter. La Conférence internationale des Commissaires à la protection des données et à la vie privée a reconnu l'importance de s'attaquer à ces facteurs humains et a adopté, en octobre 2019, la résolution sur le rôle des erreurs humaines dans les violations de données à caractère personnel[24]. Cette résolution souligne qu'il convient de prendre des mesures de sauvegarde appropriées pour prévenir les erreurs humaines et fournit une liste non exhaustive de ces mesures de sauvegarde et approches.

4.1 CAS N° 08: exfiltration des données commerciales par un salarié

Pendant sa période de préavis, le salarié d'une société copie les données commerciales de la base de données de la société. L'employé n'est autorisé à accéder aux données que pour accomplir ses tâches professionnelles. Quelques mois plus tard, après avoir cessé de travailler, il utilise les données ainsi obtenues (données de contact de base) pour alimenter un nouveau traitement de données dont il est responsable du traitement afin de contacter les clients de l'entreprise pour les

4.1.1 CAS N° 08 — Mesures préalables et évaluation des risques

72. En l'espèce, aucune mesure préalable n'a été prise pour empêcher l'employé de copier les informations de contact de la clientèle de la société, étant donné qu'il avait besoin — et a eu — un accès légitime à ces informations pour ses tâches professionnelles. Étant donné que l'accomplissement de la plupart des tâches liées à la clientèle nécessite une sorte d'accès des salariés aux données à caractère personnel, ces violations de données peuvent être les plus difficiles à prévenir. Les limitations de la portée de l'accès peuvent limiter le travail que le salarié concerné est en mesure d'effectuer. Toutefois, des politiques d'accès bien pensées et un contrôle constant peuvent contribuer à prévenir de telles violations.

73. Comme à l'accoutumée, il convient de prendre en considération, lors de l'évaluation des risques, le type de violation ainsi que la nature, la sensibilité et le volume des données à caractère personnel concernées. Ces types de violations sont généralement des violations de la confidentialité, étant donné que la base de données est habituellement laissée intacte, son contenu étant «simplement» copié en vue d'une utilisation ultérieure. La quantité de données concernées est généralement faible ou moyenne également. Dans ce cas particulier, aucune catégorie particulière de données à caractère personnel n'a été affectée, l'employé n'avait besoin que des coordonnées des clients pour pouvoir entrer en contact avec eux après avoir quitté l'entreprise. Par conséquent, les données concernées ne sont pas sensibles.

74. Bien que le seul objectif de l'ancien employé qui a copié les données de manière malveillante puisse se limiter à obtenir les informations de contact de la clientèle de la société à ses propres fins commerciales, le responsable du traitement n'est pas en mesure de considérer que le risque pour les personnes concernées est faible, étant donné qu'il n'a aucune assurance, quelle qu'elle soit, quant aux intentions du

[24] http://globalprivacyassembly.org/wp-content/uploads/2019/10/AOIC-Resolution-FINAL-ADOPTED.pdf

salarié. Ainsi, si les conséquences de la violation peuvent se limiter à de la sollicitation commerciale non désirée, il n'est pas exclu, en fonction de la finalité du traitement mis en place par l'ancien salarié, que les données volées fassent l'objet d'un abus supplémentaire et plus grave[25].

4.1.2 CAS N° 08 — Atténuation et obligations

75. Il est difficile d'atténuer les effets négatifs de la violation dans le cas susmentionné. Il pourrait s'avérer nécessaire d'engager une action juridique immédiate pour empêcher l'ancien employé d'abuser et de diffuser davantage les données. L'objectif devrait ensuite être d'éviter des situations similaires à l'avenir. Le responsable du traitement pourrait essayer d'ordonner à l'ancien employé de cesser d'utiliser les données, mais le succès de cette action est au mieux incertain. Des mesures techniques appropriées telles que l'impossibilité de copier ou de télécharger des données sur des appareils amovibles peuvent être utiles.

76. Il n'existe pas de solution universelle pour ces types de cas, mais une approche systématique peut contribuer à les prévenir. Par exemple, l'entreprise peut envisager, dans la mesure du possible, de retirer certaines formes d'accès aux employés qui ont fait part de leur intention de quitter ou de mettre en œuvre des journaux d'accès afin que l'accès non désiré puisse être enregistré et signalé. Le contrat signé avec les salariés devrait comporter des clauses interdisant de telles actions.

77. Dans l'ensemble, étant donné que la violation en question n'engendrera pas un risque élevé pour les droits et libertés des personnes physiques, une notification à l'autorité de contrôle suffira. Toutefois, l'information des personnes concernées pourrait également être bénéfique pour le responsable du traitement, étant donné qu'il pourrait être préférable qu'elles apprennent la fuite de données de la part de l'entreprise plutôt que de l'ancien employé qui tente de les contacter. La documentation relative aux violations de données conformément à l'article 33, paragraphe 5, est une obligation légale.

Actions nécessaires fondées sur les risques recensés		
Documentation interne	Notification à l'autorité de contrôle	Communication aux personnes concernées
✓	✓	X

[25] Pour des orientations sur les traitements «*susceptibles d'engendrer un risque élevé*», voir la note de bas de page 10 ci-dessus.

4.2 CAS N° 09: transmission accidentelle de données à un tiers de confiance

Un agent d'assurance a remarqué que — grâce aux paramètres défectueux d'un fichier Excel reçu par courriel — il était en mesure d'accéder à des informations relatives à une vingtaine de clients ne relevant pas de son champ d'application. Il est tenu par le secret professionnel et a été le seul destinataire du courriel. L'accord entre le responsable du traitement des données et l'agent d'assurance oblige celui-ci à signaler sans retard injustifié toute violation de données à caractère personnel au responsable du traitement. Par conséquent, l'agent a immédiatement signalé l'erreur au responsable du traitement, qui a corrigé le dossier et l'a envoyé à nouveau, en lui demandant de supprimer l'ancien message. Conformément à l'arrangement susmentionné, l'agent doit confirmer la suppression dans une déclaration écrite, ce qu'il a fait. Les informations obtenues ne comprennent pas de catégories particulières de données à caractère personnel, mais seulement les coordonnées et les données relatives à l'assurance elle-même (type d'assurance, montant). Après avoir analysé les données à caractère personnel concernées par la violation, le responsable du traitement n'a identifié aucune caractéristique particulière du côté des personnes physiques ou du responsable du traitement susceptibles d'avoir une incidence sur le niveau d'impact de la violation.

4.2.1 CAS N° 09 — Mesures préalables et évaluation des risques

78. En l'espèce, la violation ne résulte pas d'un acte intentionnel d'un employé, mais d'une erreur humaine non intentionnelle due à de l'inattention. Ces types de violations peuvent être évités ou leur fréquence réduite par a) la mise en œuvre de programmes de formation, d'éducation et de sensibilisation dans le cadre desquels les employés acquièrent une meilleure compréhension de l'importance de la protection des données à caractère personnel, b) la réduction des échanges de fichiers par courriel et utilisation, à la place, de systèmes spécifiques pour le traitement des données des clients, par exemple, c) la double vérification des fichiers avant l'envoi, d) la séparation de la création et de l'envoi de fichiers.

79. Cette violation de données ne concerne que la confidentialité des données, et leur intégrité et leur accessibilité sont laissées intactes. La violation de données ne concernait qu'une vingtaine de clients, de sorte que la quantité de données concernées peut être considérée comme faible. En outre, les données à caractère personnel concernées ne contiennent pas de données sensibles. Le fait que le sous-traitant ait immédiatement contacté le responsable du traitement après avoir pris connaissance de la violation de données peut être considéré comme un facteur d'atténuation des risques. (La possibilité que des données aient été transmises à d'autres agents d'assurance doit également être évaluée et, si elle est confirmée, des mesures appropriées doivent être prises.) En raison des mesures appropriées prises après la violation de données, cette dernière n'aura probablement aucune incidence sur les droits et libertés des personnes concernées.

80. La combinaison du faible nombre de personnes touchées, de la détection immédiate de la violation et des mesures prises pour en réduire les effets au minimum fait que ce cas particulier ne présente aucun risque.

4.2.2 CAS N° 09 — Atténuation et obligations

81. En outre, d'autres circonstances d'atténuation des risques sont également en jeu: l'agent est tenu au secret professionnel; il a lui-même signalé le problème au responsable du traitement; et il a supprimé le fichier sur demande. La sensibilisation et, le cas échéant, la prise de mesures supplémentaires pour vérifier les documents contenant des données à caractère personnel contribueront probablement à éviter des cas similaires à l'avenir.

82. En plus de documenter la violation conformément à l'article 33, paragraphe 5, il n'est pas nécessaire de prendre d'autres mesures.

Actions nécessaires fondées sur les risques recensés		
Documentation interne	Notification à l'autorité de contrôle	Communication aux personnes concernées
✓	X	X

4.3 Mesures organisationnelles et techniques visant à prévenir/atténuer les effets des sources de risques internes d'origine humaine

83. Une combinaison des mesures mentionnées ci-dessous — appliquées en fonction des caractéristiques uniques du cas devrait contribuer à réduire la probabilité qu'une violation similaire se reproduise.

84. Mesures recommandées:

(*La liste des mesures suivantes n'est en aucun cas exclusive ni exhaustive. L'objectif est plutôt de fournir des idées de prévention et des solutions possibles. Chaque activité de traitement étant différente, le responsable du traitement devrait décider quelles mesures sont les plus adaptées à la situation donnée.*)

- Mettre en œuvre, de manière périodique, des programmes de formation, d'éducation et de sensibilisation des employés concernant leurs obligations en matière de respect de la vie privée et de sécurité, ainsi que détecter et signaler les menaces pesant sur la sécurité des données à caractère personnel[26]. Élaborer un programme de sensibilisation pour rappeler aux employés les erreurs les plus courantes entraînant des violations de données à caractère personnel et comment les éviter.
- Mettre en place des pratiques, des procédures et des mesures solides et efficaces en matière de protection des données et de protection de la vie privée[27].
- Évaluer les pratiques, procédures et systèmes en matière de protection de la vie privée afin de garantir une efficacité constante[28].
- Mettre en place des politiques adéquates de contrôle des accès et visant à contraindre les utilisateurs à suivre les règles.
- Contraindre l'utilisateur à s'authentifier lorsqu'il accède à des données à caractère personnel sensibles.
- Désactiver le compte lié à l'entreprise de l'utilisateur dès que la personne quitte l'entreprise.
- Vérifier les flux de données inhabituels entre le serveur de fichiers et les postes de travail des employés.
- Mettre en place la sécurité de l'interface d'E/S dans le BIOS ou par l'utilisation d'un logiciel contrôlant l'utilisation des interfaces informatiques (verrouiller ou déverrouiller, par exemple, USB/CD/DVD, etc.).
- Revoir la politique d'accès des salariés (par exemple, enregistrer l'accès aux données sensibles et exiger de l'utilisateur qu'il introduise une raison de nature commerciale, de sorte que ces données soient disponibles en vue des audits).

---

[26] Section 2), point ii), de la résolution sur le rôle des erreurs humaines dans les violations de données à caractère personnel.

[27] Section 2), point iii), de la résolution sur le rôle des erreurs humaines dans les violations de données à caractère personnel.

[28] Section 2), point iii), de la résolution sur le rôle des erreurs humaines dans les violations de données à caractère personnel.

- Désactiver les services d'informatique en nuage ouverts.
- Interdire l'utilisation de services de courriel tiers.
- Désactiver la fonction de capture d'écran dans le système d'exploitation.
- Mettre en œuvre une politique de bureau propre.
- Régler le verrouillage automatique de tous les ordinateurs après un certain temps d'inactivité.
- Utiliser des mécanismes [par exemple, jeton (sans fil) pour se connecter/ouvrir des comptes verrouillés] pour les changements rapides d'utilisateur dans des environnements partagés.
- Utiliser des systèmes dédiés pour la gestion des données à caractère personnel qui appliquent des mécanismes de contrôle d'accès appropriés et qui préviennent les erreurs humaines, comme l'envoi de communications à un mauvais destinataire. L'utilisation de tableurs et d'autres documents Office n'est pas un moyen approprié de gérer les données des clients.

5 APPAREILS PERDUS OU VOLÉS ET DOCUMENTS PAPIER

85. Un cas fréquent est la perte ou le vol d'appareils portables. Dans ces cas, le responsable du traitement doit prendre en considération le type de données stockées sur le support, les traitements accessibles depuis le poste et les mesures prises avant la violation afin de garantir un niveau de sécurité approprié. Tous ces éléments ont une incidence sur les effets potentiels de la violation de données. L'évaluation des risques pourrait s'avérer difficile, étant donné que le dispositif n'est plus disponible.

86. Ces types de violations peuvent toujours être classés en tant que violations de la confidentialité. Toutefois, s'il n'y a pas de sauvegarde pour la base de données volée, le type de violation peut également constituer une violation de la disponibilité et une violation de l'intégrité.

87. Les scénarios ci-dessous montrent comment les circonstances susmentionnées influencent la probabilité et la gravité de la violation de données.

5.1 CAS N° 10: matériel volé stockant des données à caractère personnel chiffrées

Deux tablettes ont été volées dans une garderie d'enfants. Les tablettes contenaient une application contenant des données à caractère personnel sur les enfants fréquentant le centre d'accueil de jour. Ces données concernées étaient le nom, la date de naissance, et des informations relatives à l'éducation des enfants. Tant les tablettes chiffrées qui ont été éteintes au moment de l'effraction que l'application étaient protégées par un mot de passe fort. Les données de sauvegarde étaient effectivement et facilement accessibles au responsable du traitement. Après avoir pris connaissance du vol, la garderie a émis à distance une commande pour effacer les

5.1.1 CAS N° 10 — Mesures préalables et évaluation des risques

88. Dans ce cas particulier, le responsable du traitement a pris des mesures adéquates pour prévenir et atténuer les effets d'une éventuelle violation de données en utilisant le chiffrement du dispositif, en introduisant une protection adéquate des mots de passe et en garantissant la sauvegarde des données stockées sur les tablettes. (Une liste des mesures recommandées figure à la section 5.7).

89. Après avoir pris connaissance d'une violation, le responsable du traitement devrait évaluer la source de risque, les systèmes à l'appui du traitement des données, le type de données à caractère personnel concernées et les incidences potentielles de la violation sur les personnes concernées. La violation de données décrite ci-dessus aurait porté sur la confidentialité, la disponibilité et l'intégrité des données concernées, mais en raison des procédures appropriées du responsable du traitement avant et après la violation de données, aucun de ces types de violation ne s'est produit.

5.1.2 CAS N° 10 — Atténuation et obligations

90. La confidentialité des données à caractère personnel sur les appareils n'a pas été compromise en raison de la forte protection par mot de passe tant sur les tablettes que sur les applications. Les tablettes ont été créées de telle sorte que la mise en place d'un mot de passe signifie également que les données figurant sur l'appareil sont chiffrées. Cela a encore été renforcé par l'action du responsable du traitement visant à effacer à distance tout ce qui se trouve sur les appareils volés.

91. En raison des mesures prises, la confidentialité des données a également été maintenue intacte. En outre, la sauvegarde a permis de garantir la disponibilité continue des données à caractère personnel, de sorte qu'aucune incidence négative potentielle n'aurait pu se produire.

92. Compte tenu de ces faits, il était peu probable que la violation de données décrite ci-dessus engendre un risque pour les droits et libertés des personnes concernées, de sorte qu'aucune notification à l'autorité de contrôle ou aux personnes concernées affectées par la violation n'était nécessaire. Toutefois, cette violation de données doit également être documentée conformément à l'article 33, paragraphe 5.

Actions nécessaires fondées sur les risques recensés		
Documentation interne	Notification à l'autorité de contrôle	Communication aux personnes concernées
✓	X	**X**

5.2 CAS N° 11: matériel volé stockant des données à caractère personnel non chiffrées

L'appareil portable électronique d'un employé d'une société prestataire de services a été volé. L'ordinateur portable volé contenait les données relatives aux nom, prénom, sexe, adresse et date de naissance de plus de 100 000 clients. En raison de l'indisponibilité de l'appareil volé, il n'a pas été possible de déterminer si d'autres catégories de données à caractère personnel étaient également concernées. L'accès au disque dur de l'ordinateur portable n'était protégé par aucun mot de passe. Les données à caractère personnel pourraient être rétablies à partir des sauvegardes quotidiennes disponibles.

5.2.1 CAS N° 11 — Mesures préalables et évaluation des risques

93. Aucune mesure de sécurité préalable n'ayant été prise par le responsable du traitement, les données à caractère personnel stockées sur l'ordinateur portable volé étaient facilement accessibles au voleur ou à toute autre personne entrant ultérieurement en possession de l'appareil.

94. Cette violation de données concerne la confidentialité des données stockées sur l'appareil volé.

95. L'ordinateur portable contenant les données à caractère personnel était vulnérable dans ce cas parce qu'il ne possédait pas de protection ou de chiffrement par mot de passe. L'absence de mesures de sécurité de base renforce le niveau de risque pour les personnes concernées affectées par la violation. En outre, l'identification des personnes concernées affectées est également problématique, ce qui accroît également la gravité de la violation. Le nombre considérable de personnes concernées touchées par la violation augmente le risque, mais aucune catégorie particulière de données à caractère personnel n'a été concernée par la violation de données.

96. Au cours de l'évaluation des risques[29], le responsable du traitement devrait tenir compte des conséquences potentielles et des effets négatifs de la violation de la confidentialité. Du fait de la violation, les personnes concernées peuvent subir une fraude à l'identité reposant sur les données disponibles sur l'appareil volé, de sorte que le risque est jugé élevé.

5.2.2 CAS N° 11 — Atténuation et obligations

97. Le chiffrement des appareils et l'utilisation d'une protection forte par mot de passe de la base de données stockée auraient pu empêcher que la violation de données engendre un risque pour les droits et libertés des personnes concernées.

98. Compte tenu de ces circonstances, la notification de l'autorité de contrôle est requise, de sorte que la notification des personnes concernées est également nécessaire.

Actions nécessaires fondées sur les risques recensés		
Documentation interne	Notification à l'autorité de contrôle	Communication aux personnes concernées
✓	✓	✓

5.3 CAS N° 12: dossiers papier contenant des données sensibles volés

Un journal de bord papier a été volé dans un centre de traitement de la toxicomanie. Ce livre contenait les données d'identité et de santé de base des patients admis dans le centre thérapeutique. Les données n'étaient stockées que sur papier et aucune sauvegarde n'était disponible pour les médecins traitant les patients. Le livre n'était pas conservé dans un tiroir ou une salle fermés à clé, le responsable du traitement ne disposait d'aucun régime de contrôle d'accès ni d'aucune autre mesure de sauvegarde pour la documentation papier.

5.3.1 CAS N° 12 — Mesures préalables et évaluation des risques

99. Aucune mesure de sécurité préalable n'ayant été prise par le responsable du traitement, les données à caractère personnel conservées dans ce livre étaient facilement accessibles à la personne qui les a trouvées. En outre, en raison de la nature des données à caractère personnel conservées dans le livre, l'absence de données de sauvegarde constitue un facteur de risque très grave.

100. Cette affaire sert d'exemple de violation de données à haut risque. En raison de l'absence de précautions de sécurité appropriées, des données sensibles concernant la santé conformément à l'article 9, paragraphe 1, du RGPD ont été perdues. Étant donné qu'en l'espèce une catégorie particulière de données à caractère personnel était concernée, les risques potentiels pour les personnes concernées ont été accrus, ce qui devrait également être pris en considération par le responsable du traitement qui évalue le risque[30].

101. Cette violation concerne la confidentialité, la disponibilité et l'intégrité des données à caractère personnel concernées. En raison de cette violation, le secret médical est rompu et des tiers non autorisés peuvent avoir accès aux informations médicales privées des patients, ce qui peut avoir de graves répercussions sur la vie privée du patient. La violation de la disponibilité peut également perturber la continuité du

[29] Pour des orientations sur les traitements «*susceptibles d'engendrer un risque élevé*», voir la note de bas de page 10 ci-dessus.

[30] Pour des orientations sur les traitements «*susceptibles d'engendrer un risque élevé*», voir la note de bas de page 10 ci-dessus.

traitement des patients. Étant donné que la modification/suppression de parties du contenu du livre ne peut être exclue, l'intégrité des données à caractère personnel est également compromise.

5.3.2 CAS N° 12 — Atténuation et obligations

102. Lors de l'évaluation des mesures de sauvegarde, le type de support devrait également être pris en considération. Le carnet de patients étant un document physique, sa protection aurait dû être organisée différemment de celle d'un appareil électronique. La pseudonymisation des noms des patients, le stockage du livre dans un local protégé et dans un tiroir ou une pièce fermés à clé, ainsi qu'un contrôle d'accès approprié avec authentification lors de l'accès à celui-ci, auraient pu empêcher la violation des données.

103. La violation de données décrite ci-dessus peut avoir de graves répercussions sur les personnes concernées; par conséquent, la notification de l'autorité de contrôle et la communication de la violation aux personnes concernées sont obligatoires.

Actions nécessaires fondées sur les risques recensés		
Documentation interne	ification à l'autorité de contrôle	ommunication aux personnes concernées
✓	✓	✓

5.4 Mesures organisationnelles et techniques visant à prévenir/atténuer les effets de la perte ou du vol de dispositifs

104. Une combinaison des mesures mentionnées ci-dessous — appliquées en fonction des caractéristiques uniques du cas - devrait contribuer à réduire la probabilité qu'une violation similaire se reproduise.

105. Mesures recommandées:

(*La liste des mesures suivantes n'est en aucun cas exclusive ni exhaustive. L'objectif est plutôt de fournir des idées de prévention et des solutions possibles. Chaque activité de traitement étant différente, le responsable du traitement devrait décider quelles mesures sont les plus adaptées à la situation donnée.*)

- Activer le chiffrement de l'appareil (tel que BitLocker, Veracrypt ou DM-Crypt).
- Utiliser le code/mot de passe sur tous les appareils. Crypter tous les appareils électroniques mobiles d'une manière qui nécessite l'introduction d'un mot de passe complexe pour le déchiffrement.
- Utiliser l'authentification multifactorielle.
- Activer les fonctionnalités des dispositifs hautement mobiles qui permettent de les localiser en cas de perte ou de mauvais placement.
- Utiliser le logiciel/application MDM (gestion de terminaux mobiles) et la localisation. Utiliser des filtres anti-reflets. Éteindre les dispositifs laissés sans surveillance.
- Si cela est possible et approprié au traitement des données en question, sauvegarder les données à caractère personnel non pas sur un appareil mobile, mais sur un serveur central.
- Si le poste de travail est connecté à l'environnement LAN professionnel, procéder à une sauvegarde automatique à partir des dossiers de travail, à condition que des données à caractère personnel y soient obligatoirement stockées.
- Utiliser un VPN sécurisé (par exemple, qui nécessite une clé d'authentification avec deuxième facteur distincte pour l'établissement d'une connexion sécurisée) pour connecter les appareils mobiles aux serveurs.
- Fournir des serrures physiques aux employés afin de leur permettre de sécuriser physiquement les appareils mobiles qu'ils utilisent quand ils sont sans surveillance.
- Réglementer de manière appropriée l'utilisation de l'appareil en dehors de l'entreprise.

- Réglementer de manière appropriée l'utilisation de l'appareil à l'intérieur de l'entreprise.
- Utiliser le logiciel/application MDM (gestion de terminaux mobiles) et activer la fonction d'effacement des données à distance.
- Utiliser une gestion centralisée des appareils avec des droits minimaux concernant l'installation de logiciels par les utilisateurs finaux.
- Installer des contrôles d'accès physiques.
- Éviter de stocker des informations sensibles dans des appareils mobiles ou des disques durs. S'il est nécessaire d'accéder au système interne de l'entreprise, il convient d'utiliser des canaux sécurisés comme indiqué précédemment.

6 ERREUR DE COURRIER

106. La source de risque est une erreur humaine interne dans ce cas également, mais en l'espèce, la violation n'est pas due à une action malveillante. Elle est le résultat d'un manque d'attention. Comme le responsable du traitement dispose de peu de moyens d'action une fois qu'un tel événement s'est produit, la prévention est encore plus importante dans ces cas que dans d'autres types de violations.

6.1 CAS N° 13: erreur de courrier postal

Deux commandes de chaussures ont été emballées par une société de vente au détail. En raison d'une erreur humaine, deux factures ont été mélangées, de sorte que les deux produits et les factures correspondantes ont été envoyés à la mauvaise personne. Cela signifie que les deux clients ont reçu la commande de l'autre, y compris la facture contenant les données à caractère personnel. Après avoir pris connaissance de la violation, le responsable du traitement a rappelé les commandes et les a envoyées aux bons destinataires.

6.1.1 CAS N° 13 — Mesures préalables et évaluation des risques

107. Les factures contenaient les données à caractère personnel requises pour une livraison réussie (nom, adresse, plus l'objet acheté et son prix). Il est important de déterminer comment l'erreur humaine a pu se produire en premier lieu et, si, en tout état de cause, elle aurait pu être évitée. Dans le cas d'espèce, le risque est faible, étant donné qu'il n'y a pas de catégories particulières de données à caractère personnel ou d'autres données dont l'abus pourrait avoir des effets négatifs substantiels, que la violation ne résulte pas d'une erreur systémique de la part du responsable du traitement et que seules deux personnes sont concernées. Aucun effet négatif sur les personnes n'a pu être identifié.

6.1.2 CAS N° 13 — Atténuation et obligations

108. Le responsable du traitement devrait prévoir un retour gratuit des articles et des factures qui les accompagnent, et il devrait également prier les destinataires ayant reçu les articles erronés de détruire ou de supprimer toutes les copies éventuelles des factures contenant les données à caractère personnel de l'autre personne.

109. Même si la violation ne présente pas en soi de risque élevé pour les droits et libertés des personnes concernées et que, par conséquent, la communication aux personnes concernées n'est pas requise en vertu de l'article 34 du RGPD, la communication de la violation à ces personnes ne peut être évitée, étant donné que leur coopération est nécessaire pour atténuer le risque.

Actions nécessaires fondées sur les risques recensés		
Documentation interne	Notification à l'autorité de contrôle	Communication aux personnes concernées
✓	X	X

6.2 CAS N° 14: données à caractère personnel hautement confidentielles envoyées par courriel par erreur

Le service de l'emploi d'un office de l'administration publique a envoyé un courriel — concernant les formations à venir — aux personnes inscrites dans son système en tant que demandeurs d'emploi. Par erreur, un document contenant toutes les données personnelles de ces demandeurs d'emploi (nom, adresse électronique, adresse postale, numéro de sécurité sociale) a été joint à ce message. Le nombre de personnes touchées est supérieur à 60 000. L'office a ensuite contacté tous les destinataires et leur a demandé de supprimer le message précédent et de ne pas utiliser les informations qu'il contenait.

6.2.1 CAS N° 14 — Mesures préalables et évaluation des risques

110. Des règles plus strictes auraient dû être mises en œuvre pour l'envoi de tels messages. L'introduction de mécanismes de contrôle supplémentaires doit être envisagée.

111. Le nombre de personnes touchées est considérable et le fait que leur numéro de sécurité sociale soit concerné, ainsi que d'autres données à caractère personnel plus basiques, accentue encore le risque, qui peut être considéré comme élevé[31]. La diffusion éventuelle des données par l'un des destinataires ne peut être contenue par le responsable du traitement.

6.2.2 CAS N° 14 — Atténuation et obligations

112. Comme indiqué plus haut, les moyens d'atténuer efficacement les risques d'une violation similaire sont limités. Bien que le responsable du traitement ait demandé la suppression du message, cela ne saurait contraindre les destinataires à le faire et, par conséquent, il ne peut être certain qu'ils répondent à la demande.

113. L'exécution des trois actions indiquées ci-dessous devrait aller de soi dans un cas comme celui de l'espèce.

Actions nécessaires fondées sur les risques recensés		
Documentation interne	Notification à l'autorité de contrôle	Communication aux personnes concernées
✓	✓	✓

6.3 CAS N° 15: données à caractère personnel transmises par courrier par erreur

Une liste des participants à un cours portant sur l'anglais juridique qui se déroule dans un hôtel pendant 5 jours est envoyée par erreur à 15 anciens participants au lieu d'être envoyée à l'hôtel. La liste contient les noms, adresses électroniques et préférences alimentaires des 15 participants. Seuls deux participants ont rempli leurs préférences alimentaires, faisant part de leur intolérance au lactose. Aucun des participants n'a une identité protégée. Le responsable du traitement découvre l'erreur immédiatement après l'envoi de la liste et en informe les destinataires et leur demande de supprimer la liste.

[31] Pour des orientations sur les traitements «*susceptibles d'engendrer un risque élevé*», voir la note de bas de page 10 ci-dessus.

6.3.1 CAS N° 15 — Mesures préalables et évaluation des risques

114. Des règles strictes auraient dû être mises en œuvre pour l'envoi de messages contenant des données à caractère personnel. L'introduction de mécanismes de contrôle supplémentaires doit être envisagée.

115. Les risques découlant de la nature, de la sensibilité, du volume et du contexte des données à caractère personnel sont faibles. Les données à caractère personnel comprennent des données sensibles sur les préférences alimentaires de deux des participants. Même si les informations indiquant qu'une personne est intolérante au lactose sont des données relatives à la santé, le risque que ces données soient utilisées de manière préjudiciable devrait être considéré comme relativement faible. Si, dans le cas des données relatives à la santé, il est généralement supposé que la violation est susceptible d'engendrer un risque élevé pour la personne concernée[32], dans le même temps, dans ce cas particulier, aucun risque de voir la violation causer un préjudice physique, matériel ou moral pour la personne concernée en raison de la divulgation non autorisée d'informations relatives à l'intolérance au lactose ne peut être identifié. Contrairement à certaines autres préférences alimentaires, l'intolérance au lactose ne peut normalement pas être liée à des convictions religieuses ou philosophiques. La quantité de données visées par la violation et le nombre de personnes concernées sont également très faibles.

6.3.2 CAS N° 15 — Atténuation et obligations

116. En résumé, on peut affirmer que la violation n'a pas eu d'effet significatif sur les personnes concernées. Le fait que le responsable du traitement ait immédiatement contacté les destinataires après avoir pris connaissance de l'erreur peut être considéré comme une circonstance atténuante.

117. Si un courriel est envoyé à un destinataire incorrect/non autorisé, il est recommandé au responsable du traitement d'envoyer un courriel de suivi en mettant en copie les destinataires accidentels afin de présenter des excuses, de leur demander de supprimer le courriel en cause et de les informer qu'ils n'ont pas le droit d'utiliser les adresses électroniques qui leur ont été indiquées.

118. Compte tenu de ces faits, il était peu probable que cette violation de données engendre un risque pour les droits et libertés des personnes concernées, de sorte qu'aucune notification à l'autorité de contrôle ou aux personnes concernées n'était nécessaire. Toutefois, cette violation de données doit également être documentée conformément à l'article 33, paragraphe 5.

Actions nécessaires fondées sur les risques recensés		
Documentation interne	Notification à l'autorité de contrôle	Communication aux personnes concernées
✓	X	X

[32] Voir les lignes directrices WP 250, p. 23.

6.4 CAS N° 16: erreur de courrier postal

Un groupe d'assurance propose des assurances automobiles. Pour ce faire, elle envoie par courrier postal des polices régulièrement ajustées. Outre le nom et l'adresse du preneur d'assurance, la lettre contient le numéro d'immatriculation du véhicule sans chiffres masqués, les taux d'assurance de l'année d'assurance en cours et de la suivante, le kilométrage annuel approximatif et la date de naissance du preneur d'assurance. Les données concernant la santé conformément à l'article 9 du RGPD, les données de paiement (données bancaires), les données économiques et financières ne sont pas incluses.

Les lettres sont mises sous enveloppe par des machines automatiques. En raison d'une erreur mécanique, deux lettres destinées à des preneurs d'assurance différents sont insérées dans une seule enveloppe et envoyées à un preneur d'assurance par courrier postal. Le preneur d'assurance ouvre la lettre à son domicile et examine la lettre qui lui était bien destinée ainsi que la lettre d'un autre preneur d'assurance qu'il n'était pas censé recevoir.

6.4.1 CAS N° 16 — Mesures préalables et évaluation des risques

119. La lettre indûment remise contient le nom, l'adresse, la date de naissance, le numéro d'immatriculation du véhicule non masqué et la classification du taux d'assurance de l'année en cours et de l'année suivante. Les effets sur la personne concernée doivent être considérés comme moyens, étant donné que les informations qui ne sont pas accessibles au public, telles que la date de naissance ou les numéros d'immatriculation non masqués du véhicule, et les informations relatives à l'augmentation des tarifs d'assurance sont communiquées au destinataire non autorisé. La probabilité d'une utilisation abusive de ces données est estimée entre faible et moyenne. Toutefois, alors que de nombreux destinataires jetteront probablement la lettre indûment reçue à la poubelle, dans certains cas, il n'est pas totalement exclu que la lettre soit postée sur les réseaux sociaux ou que le preneur d'assurance soit contacté.

6.4.2 CAS N° 16 — Atténuation et obligations

120. Le responsable du traitement devrait faire restituer le document original à ses propres frais. Le mauvais destinataire doit également être informé qu'il ne peut pas effectuer un usage abusif des informations lues.

121. Il ne sera probablement jamais possible d'éviter complètement une erreur de distribution postale dans un courrier de masse utilisant des machines entièrement automatisées. Toutefois, en cas d'augmentation de la fréquence, il est nécessaire de vérifier si les machines automatiques sont réglées et entretenues correctement ou si un autre problème systémique entraîne une telle violation.

Actions nécessaires fondées sur les risques recensés		
Documentation interne	Notification à l'autorité de contrôle	Communication aux personnes concernées
✓	✓	X

6.5 Mesures organisationnelles et techniques visant à prévenir/atténuer les effets des erreurs de courrier

122. Une combinaison des mesures mentionnées ci-dessous — appliquées en fonction des caractéristiques uniques du cas d'espèce — devrait contribuer à réduire la probabilité qu'une violation similaire se reproduise.

123. Mesures recommandées:

(*La liste des mesures suivantes n'est en aucun cas exclusive ni exhaustive. L'objectif est plutôt de fournir des idées de prévention et des solutions possibles. Chaque activité de traitement étant différente, le responsable du traitement devrait décider quelles mesures sont les plus adaptées à la situation donnée.*)

- Fixer des normes précises — sans possibilité d'interprétation — pour l'envoi de lettres/courriels.
- Prévoir une formation adéquate du personnel sur la manière d'envoyer des lettres/courriels.
- Lorsqu'ils envoient des courriels à plusieurs destinataires, ils sont répertoriés dans le champ «cci» par défaut.
- Une confirmation supplémentaire est requise lors de l'envoi de courriers électroniques à plusieurs destinataires, et ceux-ci ne figurent pas dans le champ «cci».
- Appliquer le principe des quatre yeux.
- Privilégier l'adressage automatique plutôt que manuel, avec des données extraites d'une base de données disponible et actualisée; le système d'adressage automatique devrait être régulièrement réexaminé afin de détecter les erreurs cachées et les paramètres incorrects.
- Appliquer le délai de temporisation (par exemple, le message peut être supprimé/édité dans un certain délai après avoir cliqué sur envoi).
- Désactiver la saisie semi-automatique lors de la saisie d'adresses électroniques.
- Organiser des sessions de sensibilisation aux erreurs les plus courantes conduisant à une violation de données à caractère personnel.
- Des sessions de formation et des manuels sur la manière de gérer les incidents conduisant à des violations de données à caractère personnel et sur les personnes à informer (faire intervenir le DPD).

7 AUTRES CAS — INGÉNIERIE SOCIALE

7.1 CAS N° 17: usurpation d'identité

Le centre de contact d'une entreprise de télécommunications reçoit un appel téléphonique d'une personne qui se présente comme client. Le «client» exige de l'entreprise qu'elle modifie l'adresse électronique à laquelle les informations relatives à la facturation doivent être envoyées à partir de ce moment-là. Le travailleur du centre de contact valide l'identité du client en demandant certaines données à caractère personnel, telles que définies par les procédures de l'entreprise. L'appelant indique correctement le numéro fiscal et l'adresse postale demandés (parce qu'il a eu accès à ces éléments). Après la validation, l'opérateur procède à la modification demandée et, à partir de ce moment-là, les informations relatives à la facturation sont envoyées à la nouvelle adresse électronique. La procédure ne prévoit aucune notification à l'ancienne adresse électronique. Le mois suivant, le client légitime contacte l'entreprise pour savoir pourquoi il ne reçoit pas de facturation à son adresse électronique et nie tout appel de sa part demandant le changement d'adresse électronique. La société se rend compte plus tard que les informations ont été envoyées à un utilisateur illégitime et annule le changement.

7.1.1 Cas n° 17 — Évaluation des risques, atténuation des risques et obligations

124. Ce cas illustre l'importance des mesures antérieures. La violation, du point de vue du risque, présente un niveau de risque élevé[33], étant donné que les données relatives à la facturation peuvent fournir des informations sur la vie privée de la personne concernée (par exemple, habitudes, contacts) et pourraient entraîner des dommages matériels (par exemple, harcèlement, risque pour l'intégrité physique). Les données à caractère personnel obtenues au cours de cette attaque peuvent également être utilisées pour faciliter la prise de contrôle des comptes dans cette organisation ou pour exploiter d'autres mesures d'authentification dans d'autres organisations. Compte tenu de ces risques, la mesure d'authentification «appropriée» devrait mettre la barre haut, en fonction des données à caractère personnel qui peuvent être traitées à la suite de l'authentification.

125. En conséquence, tant une notification à l'autorité de contrôle qu'une communication à la personne concernée sont nécessaires de la part du responsable du traitement.

126. Il est clair que le processus de validation préalable du client doit être affiné à la lumière de ce cas. Les méthodes d'authentification utilisées n'étaient pas suffisantes. La partie malveillante a pu prétendre être l'utilisateur visé en utilisant des informations accessibles au public et des informations auxquelles elle avait accès d'une autre façon.

127. L'utilisation de ce type d'authentification statique fondée sur la connaissance (lorsque la réponse ne change pas et que l'information n'est pas «secrète» comme ce serait le cas avec un mot de passe) n'est pas recommandée.

128. L'organisation devrait plutôt utiliser une forme d'authentification qui donnerait lieu à un degré élevé de confiance dans le fait que l'utilisateur authentifié est la personne visée, et personne d'autre. L'introduction d'une méthode d'authentification multifactorielle résoudrait le problème, par exemple vérifier la demande de changement, en envoyant une demande de confirmation à l'ancien contact; ou en ajoutant des questions supplémentaires et en demandant des informations qui n'apparaissent que sur les factures précédentes. C'est au responsable du traitement qu'il appartient de décider des mesures à mettre en place, car c'est lui qui connaît le mieux les détails et les exigences de son fonctionnement interne.

Actions nécessaires fondées sur les risques recensés		
Documentation interne	Notification à l'autorité de contrôle	Communication aux personnes concernées
✓	✓	✓

[33] Pour des orientations sur les traitements «*susceptibles d'engendrer un risque élevé*», voir la note de bas de page 10 ci-dessus.

7.2 CAS N° 18: exfiltration par courriel

Une chaîne d'hypermarchés a détecté, 3 mois après sa configuration, que certains comptes de messagerie électronique avaient été modifiés et que des règles avaient été créées pour que chaque courriel contenant certaines expressions (par exemple «facture», «paiement», «virement bancaire», «authentification carte de crédit», «coordonnées bancaires») soit transféré dans un dossier inutilisé et également transmis à une adresse électronique externe. En outre, à cette époque, une attaque d'ingénierie sociale avait déjà été commise, à savoir que l'auteur de l'attaque, qui se faisait passer pour un fournisseur, avait fait modifier les coordonnées bancaires du fournisseur pour qu'elles correspondent à ses propres données à lui. Enfin, à ce moment-là, plusieurs fausses factures, incluant le nouveau compte bancaire, avaient été envoyées. Le système de suivi de la plateforme de messagerie électronique a fini par émettre une alerte concernant les dossiers. La société n'a pas été en mesure de détecter comment l'auteur de l'attaque avait pu accéder aux comptes de messagerie électronique, mais elle a supposé que l'origine devait être un courriel infecté ayant donné accès au groupe d'utilisateurs en charge des paiements.

En raison de la transmission de courriels par mots clés, l'auteur de l'attaque a reçu des informations sur 99 employés: nom et salaire d'un mois donné pour 89 personnes concernées; nom, état civil, nombre d'enfants, salaire, heures de travail et autres informations sur le salaire perçu par 10 salariés dont le contrat a pris fin. Le responsable du traitement n'a informé que les 10 salariés appartenant à ce dernier groupe.

7.2.1 Cas n° 18 — Évaluation des risques, atténuation des risques et obligations

129. Même si l'auteur de l'attaque ne visait probablement pas à collecter des données à caractère personnel, puisque la violation pourrait entraîner à la fois un préjudice matériel (par exemple, une perte financière) et un préjudice moral (par exemple, vol ou usurpation d'identité), ou que les données peuvent être utilisées pour faciliter d'autres attaques (par exemple, l'hameçonnage), la violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques. Par conséquent, la violation devrait être communiquée à l'ensemble des 99 salariés et pas seulement aux 10 salariés dont les informations sur les salaires ont été divulguées.

130. Après avoir pris connaissance de la violation, le responsable du traitement a imposé un changement de mot de passe pour les comptes compromis, a bloqué l'envoi de courriels vers le compte de messagerie de l'auteur de l'attaque, a informé le prestataire de services du courriel utilisé par l'auteur de l'attaque concernant ses actions, a supprimé les règles fixées par l'auteur de l'attaque et a affiné les alertes du système de surveillance afin qu'une alerte soit lancée dès qu'une règle automatique est créée. À défaut, le responsable du traitement pourrait supprimer le droit des utilisateurs de fixer des règles de transfert automatique, ce qui nécessiterait que l'équipe du service informatique ne le fasse que sur demande, ou il pourrait mettre en place une politique selon laquelle les utilisateurs devraient vérifier et rendre compte des règles établies sur leurs comptes une fois par semaine ou plus souvent, dans les domaines traitant des données financières.

131. Le fait qu'une violation puisse se produire et ne pas être détectée pendant si longtemps et que, sur une plus longue durée, l'ingénierie sociale ait pu être utilisée pour modifier davantage de données, a mis en évidence des problèmes importants dans le système de sécurité informatique du responsable du traitement. Il convient d'y remédier sans délai, par exemple en mettant l'accent sur les examens de l'automatisation et les contrôles des changements, la détection des incidents et les mesures de réaction. Les responsables du traitement des données sensibles, des informations financières, etc. ont une plus grande responsabilité pour ce qui est de garantir une sécurité adéquate des données.

Actions nécessaires fondées sur les risques recensés		
Documentation interne	Notification à l'autorité de contrôle	Communication aux personnes concernées
✓	✓	✓