Lignes directrices 01/2021

sur les exemples de notification des violations de données personnelles

Adopté 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 la consultation publique

Table des matières

LE CONSEIL EUROPÉEN DE LA PROTECTION DES DONNÉES

Vu l'article 70 (1e) du règlement 2016/679/UE 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 " GDPR "),

Vu l'accord EEE, et notamment son annexe XI et son protocole 37, tels que modifiés par la décision du Comité mixte de l'EEE n° 154/2018 du 6 juillet 2018[1] ,

Vu l'article 12 et l'article 22 de son règlement intérieur,

Vu la communication de la Commission au Parlement européen et au Conseil intitulée "La protection des données, pilier de la responsabilisation des citoyens, et l'approche de l'UE en matière de transition numérique - deux ans d'application du règlement général sur la protection des données"[2] ,

A ADOPTÉ LES LIGNES DIRECTRICES SUIVANTES

1 INTRODUCTION

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

2. Le groupe de travail "Article 29" a déjà produit une orientation *générale* sur la notification des violations de données en octobre 2017, en analysant les sections pertinentes du GDPR (Guidelines on Personal data breach notification under Regulation 2016/679, WP 250) (ci-après "Guidelines WP250")[3] . Toutefois, en raison de sa nature et de son calendrier, ces lignes directrices n'ont pas abordé toutes les questions pratiques de manière suffisamment détaillée. Par conséquent, le besoin s'est fait sentir d'une orientation *orientée vers la pratique, basée sur des cas*, qui utilise les expériences acquises par les AS depuis que le GDPR est applicable.

3. Ce document est destiné à compléter les lignes directrices WP 250 et il reflète les expériences communes des AS de l'EEE depuis que le GDPR est devenu applicable. Son objectif est d'aider les responsables du traitement des données à décider de la manière de traiter les violations de données et des facteurs à prendre en compte lors de l'évaluation des risques.

4. Dans le cadre de toute tentative de traitement d'une violation, le responsable du traitement et le sous-traitant doivent d'abord être en mesure de la reconnaître. Le GDPR définit une "violation de données à caractère personnel" à l'article 4, paragraphe 12, comme "une violation de la sécurité conduisant à la perte de données".

---

[1] Les références aux "États membres" faites dans le présent document doivent être comprises comme des références aux "États membres de l'EEE".

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

[3] G29 WP250 rev.1, 6 février 2018, Lignes directrices sur la notification des violations de données personnelles en vertu du règlement 2016/679 - approuvées par l'EDPB, https://ec.europa.eu/newsroom/article29/item-

detail.cfm?item_id=612052.

la destruction, la perte, l'altération, la divulgation non autorisée ou l'accès accidentel ou illicite de données à caractère personnel transmises, stockées ou traitées d'une autre manière".

5. Dans son avis 03/2014 sur la notification des violations[4] et dans ses lignes directrices WP 250, le WP29 a expliqué que les violations peuvent être classées selon les trois principes de sécurité de l'information bien connus suivants :

- "Violation de la confidentialité" - lorsqu'il y a une divulgation ou un accès non autorisé ou accidentel à des données à caractère personnel.
- "Violation de l'intégrité" - lorsqu'il y a une altération non autorisée ou accidentelle de données à caractère personnel.
- "Violation de la disponibilité" - lorsqu'il y a une perte accidentelle ou non autorisée de l'accès à des données à caractère personnel, ou leur destruction.[5]

6. Une violation peut potentiellement avoir une série d'effets négatifs importants sur les personnes, qui peuvent se traduire par des dommages physiques, matériels ou immatériels. Le GDPR explique que cela peut inclure la perte de contrôle sur leurs données personnelles, la limitation de leurs droits, la discrimination, l'usurpation d'identité ou la fraude, la perte financière, l'inversion non autorisée de la pseudonymisation, l'atteinte à la réputation et la perte de confidentialité des données personnelles protégées par le secret professionnel. Il peut également s'agir de tout autre désavantage économique ou social important pour ces personnes. L'une des obligations les plus importantes du responsable du traitement des données 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 GDPR exige du responsable du traitement qu'il :

- documenter toute violation de données à caractère personnel, comprenant les faits relatifs à la violation de données à caractère personnel, ses effets et les mesures correctives prises[6] ;
- notifier la violation des données personnelles à l'autorité de contrôle, à moins que la violation des données ne soit pas susceptible d'entraîner un risque pour les droits et libertés des personnes physiques[7] ;
- communiquer la violation des données personnelles à la personne concernée lorsque la violation des données personnelles est susceptible d'entraîner un risque élevé pour les droits et libertés des personnes physiques[8] .

8. Les violations de données sont des problèmes en soi, mais elles peuvent aussi être les symptômes d'un régime de sécurité des données vulnérable, voire obsolète, et indiquer des faiblesses du système auxquelles il faut remédier. En règle générale, il est toujours préférable de prévenir les violations de données en se préparant à l'avance, car 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 profonde du problème, afin de déterminer si les vulnérabilités qui ont donné lieu à l'incident sont toujours présentes, et donc toujours exploitables. Dans de nombreux cas, le responsable du traitement est en mesure d'identifier que l'incident est susceptible d'entraîner un risque et doit donc être

---

[4] G29 WP213, 25 mars 2014, Avis 03/2014 sur la notification des violations de données personnelles, 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 faut tenir compte du fait qu'une violation de données peut concerner soit une catégorie, soit plusieurs catégories simultanément ou combinées.

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

[7] Article 33(1) du GDPR.

[8] Article 34(1) du GDPR.

notifiée. Dans d'autres cas, il n'est pas nécessaire de reporter la notification jusqu'à ce que le risque et l'impact de la violation aient été pleinement évalués, puisque l'évaluation complète du risque peut avoir lieu parallèlement à la notification et que les informations ainsi obtenues peuvent être fournies à l'AS par étapes sans retard excessif[9] .

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

10. Si un contrôleur estime lui-même que le risque est improbable, mais qu'il s'avère que le risque se matérialise, l'autorité de surveillance compétente peut utiliser ses pouvoirs correctifs et peut décider de sanctions.

11. Chaque responsable de traitement et chaque sous-traitant doit avoir des plans et des procédures en place pour gérer d'éventuelles violations de données. Les organisations doivent avoir des lignes hiérarchiques claires et des personnes responsables de certains aspects du processus de récupération.

12. Il est également essentiel de former et de sensibiliser le personnel du responsable du traitement et du sous-traitant aux questions de protection des données, en mettant l'accent 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.) est également essentielle pour les responsables du traitement et les sous-traitants. Cette formation doit être répétée régulièrement, en fonction du type d'activité de traitement et de la taille du responsable du traitement, en tenant compte des dernières tendances et 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 alimente le "Manuel de gestion des violations de données à caractère personnel" du responsable du traitement et du sous-traitant, qui vise à établir les faits pour chaque facette du traitement à chaque étape importante de l'opération. Un tel manuel, préparé à l'avance, constituerait une source d'information beaucoup plus rapide pour permettre aux responsables du traitement et aux sous-traitants d'atténuer les risques et de respecter les obligations sans retard excessif. Ainsi, en cas de violation de données personnelles, les membres de l'organisation sauront quoi faire et l'incident sera probablement traité plus rapidement que s'il n'y avait pas de mesures d'atténuation ou de plan en place.

14. Bien que les cas présentés ci-dessous soient fictifs, ils sont basés sur des cas typiques tirés de l'expérience collective de l'AS en matière de notifications de violations de données. Les analyses proposées se rapportent explicitement aux cas examinés, mais dans le but d'aider les contrôleurs de données 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, nécessitant ainsi des mesures différentes ou supplémentaires. Les présentes lignes directrices structurent les cas en fonction de certaines catégories de violations (par exemple, les attaques par ransomware). Certaines mesures d'atténuation sont requises dans chaque cas lorsqu'il s'agit d'une certaine catégorie de violations. Ces mesures ne sont pas nécessairement répétées dans chaque analyse de cas appartenant à la même catégorie de violations. Pour les cas appartenant à la même catégorie, seules les différences sont exposées. Par conséquent, le lecteur doit lire tous les cas relatifs à la catégorie de violation concernée pour identifier et distinguer toutes les mesures correctes à prendre.

15. La documentation interne d'une violation est une obligation indépendante des risques liés à la violation, et doit être effectuée dans tous les cas. Les cas présentés ci-dessous tentent d'apporter un éclairage sur la

nécessité ou non de notifier la violation à l'AS et de la communiquer aux personnes concernées.

[9] Article 33(4) du GDPR.

2 RANSOMWARE

16. Une des causes fréquentes de notification de violation de données est une attaque par ransomware subie par le responsable du traitement des données. Dans ce cas, un code malveillant crypte les données personnelles, puis l'attaquant demande au responsable du traitement une rançon en échange du code de décryptage. Ce type d'attaque peut généralement être classé comme une violation de la disponibilité, mais il arrive souvent qu'une violation de la confidentialité se produise également.

2.1 CAS n° 01 : Ransomware avec sauvegarde appropriée et sans exfiltration de

Les systèmes informatiques d'une petite entreprise de fabrication ont été exposés à une attaque de ransomware, et les données stockées dans ces systèmes ont été cryptées. Le responsable du traitement des données a utilisé le chiffrement au repos, de sorte que toutes les données auxquelles le ransomware a eu accès ont été stockées sous forme chiffrée à l'aide d'un algorithme de chiffrement de pointe. La clé de déchiffrement n'a pas été compromise dans l'attaque, c'est-à-dire que l'attaquant ne pouvait ni y accéder ni l'utiliser indirectement. En conséquence, l'attaquant n'a eu accès qu'à des données personnelles cryptées. En particulier, ni le système de messagerie de l'entreprise, ni les systèmes clients utilisés pour y accéder n'ont été affectés. L'entreprise fait appel à l'expertise d'une société de cybersécurité externe pour enquêter sur l'incident. Des journaux retraçant tous les flux de données quittant l'entreprise (y compris les courriels sortants) sont disponibles. Après avoir analysé les journaux 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'incident n'a fait que chiffrer les données, sans les exfiltrer. Les journaux ne montrent aucun flux de données sortant pendant la période de l'attaque. Les données personnelles affectées par la violation concernent des clients et des employés de l'entreprise, quelques dizaines de personnes en tout. Une sauvegarde était facilement disponible, et les données ont été restaurées quelques heures après l'attaque. La violation n'a pas eu de conséquences sur le fonctionnement quotidien du responsable du traitement. Il n'y a eu aucun retard dans le paiement des employés ou le traitement des demandes des clients.

17. Dans ce cas, les éléments suivants ont été tirés de la définition d'une "violation de données à caractère personnel" : une violation de la sécurité a entraîné une modification illégale et un accès non autorisé aux données à caractère personnel stockées.

2.1.1 CAS N° 01 - Mesures préalables et évaluation du risque

18. Comme pour tous les risques posés par des acteurs externes, la probabilité qu'une attaque par ransomware réussisse peut être considérablement réduite en renforçant la sécurité de l'environnement de contrôle des données. La majorité de ces violations peuvent être évitées en s'assurant que des mesures de sécurité organisationnelles, physiques et technologiques appropriées ont été prises. Parmi ces mesures, citons la gestion adéquate des correctifs et l'utilisation d'un système de détection anti-malware approprié. Le fait de disposer d'une sauvegarde appropriée et distincte contribuera à atténuer les conséquences d'une attaque réussie si elle se produit. En outre, un programme d'éducation, de formation et de sensibilisation des employés à la sécurité (SETA) permettra de prévenir et de reconnaître ce type d'attaque. (Parmi ces mesures, une bonne gestion des correctifs, qui garantit que les systèmes sont à jour et que toutes les vulnérabilités connues des systèmes déployés sont corrigées, est l'une des plus importantes, car la plupart des attaques par ransomware exploitent des vulnérabilités bien connues.

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

20. Dans cet exemple, l'attaquant a eu accès à des données personnelles et la confidentialité du texte chiffré contenant des données personnelles sous forme cryptée a été compromise. Toutefois, les données qui auraient pu être exfiltrées ne peuvent pas être lues ou utilisées par l'auteur de l'attaque, du moins pour le moment. La technique de cryptage utilisée par le responsable du traitement est conforme à l'état de l'art. La clé de décryptage n'a pas été compromise et ne pouvait vraisemblablement pas non plus être déterminée par d'autres moyens. En conséquence, les risques pour la confidentialité des

les droits et libertés des personnes physiques sont réduits au minimum, sauf progrès cryptanalytique rendant les données cryptées intelligibles dans le futur.

21. Le responsable du traitement doit prendre en considération le risque que la violation fait courir aux personnes concernées[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 n'est pas compromise[11] . Dans cet exemple, les effets négatifs de la violation ont été atténués assez rapidement après qu'elle se soit produite. Le fait de disposer d'un régime de sauvegarde approprié[12] rend les effets de la violation moins graves et, en l'espèce, le responsable du traitement a pu en faire un usage efficace.

22. En ce qui concerne la gravité des conséquences pour les personnes concernées, seules des conséquences mineures ont pu être identifiées puisque les données affectées ont été restaurées en quelques heures, que la violation n'a pas eu de conséquences sur le fonctionnement quotidien du responsable du traitement et qu'elle n'a pas eu d'effet significatif sur les personnes concernées (par exemple, les paiements des employés ou le traitement des demandes des clients).

2.1.2 CAS n° 01 - Atténuation et obligations

23. Sans sauvegarde, le responsable du traitement ne peut prendre que peu de mesures pour remédier à la perte de données à caractère personnel, et les données doivent être collectées à nouveau. Dans ce cas particulier, cependant, les effets de l'attaque ont pu être contenus efficacement en réinitialisant tous les systèmes compromis à un état propre connu pour être exempt de code malveillant, en corrigeant les vulnérabilités et en restaurant les données affectées peu après l'attaque. En l'absence de sauvegarde, les données sont perdues et la gravité peut augmenter car les risques ou les impacts sur les personnes peuvent également le faire.

24. L'opportunité d'une restauration efficace des données à partir de la sauvegarde facilement disponible est une variable clé dans l'analyse de la violation. La détermination d'un délai approprié pour restaurer les données compromises dépend des circonstances uniques de la violation en question. Le GDPR stipule qu'une violation de données personnelles doit être notifiée sans retard excessif et, si possible, au plus tard après 72 heures. Par conséquent, on pourrait déterminer que le dépassement du délai de 72 heures est déconseillé dans tous les cas, mais lorsqu'il s'agit de cas de niveau de risque élevé, même le respect de ce délai peut être considéré comme insatisfaisant.

25. Dans le cas présent, à la suite d'une analyse d'impact détaillée et d'un processus de réponse aux incidents, le responsable du traitement a déterminé que la violation n'était pas susceptible d'entraîner un risque pour les droits et libertés des personnes physiques, et qu'il n'était donc pas nécessaire de communiquer avec les personnes concernées.

---

[10] Pour des orientations sur les opérations de traitement "*susceptibles d'entraîner un risque élevé*", voir le groupe de travail A29 "Lignes directrices sur l'analyse d'impact sur la protection des données (DPIA) et la détermination du fait que le traitement est "susceptible d'entraîner un risque élevé" aux fins du règlement 2016/679", WP248 rev. 01, - approuvé par l'EDPB, https://ec.europa.eu/newsroom/article29/items/611236, p. 9.

[11] Techniquement, le cryptage des données implique un "accès" aux données originales et, dans le cas d'un ransomware, la suppression de l'original - le code du ransomware doit accéder aux données pour les crypter et supprimer les données originales. Un attaquant peut prendre une copie de l'original avant de le supprimer, mais les données personnelles ne seront pas toujours extraites. Au fur et à mesure que l'enquête d'un responsable du traitement des données progresse, de nouvelles informations peuvent être mises en lumière pour faire évoluer

cette évaluation. L'accès qui entraîne la destruction, la perte, l'altération ou la divulgation non autorisée de données à caractère personnel, ou un risque pour la sécurité d'une personne concernée, même sans interprétation des données, peut être aussi grave que l'accès avec interprétation des données à caractère personnel.

[12] Les procédures de sauvegarde doivent être structurées, cohérentes et reproductibles. Des exemples de procédures de sauvegarde sont la méthode 3-2-1 et la méthode grand-père-père-fils. Toute méthode doit toujours être testée pour vérifier son efficacité en matière de couverture et lorsque des données doivent être restaurées. Les tests doivent également être répétés à intervalles réguliers et surtout lorsque des changements interviennent dans l'opération de traitement ou dans ses circonstances, afin de garantir l'intégrité du système.

l'AS. Cependant, comme toutes les violations de données, elle doit être documentée conformément à l'article 33 (5). L'organisation peut également avoir besoin (ou être tenue ultérieurement par l'autorité de surveillance) de mettre à jour et de corriger ses mesures et procédures organisationnelles et techniques de traitement de la sécurité des données à caractère personnel et d'atténuation des risques. Dans le cadre de cette mise à jour et de ces mesures correctives, l'organisation doit mener une enquête approfondie sur la violation et identifier les causes et les méthodes utilisées par l'auteur de l'infraction afin de prévenir tout événement similaire à l'avenir.

Actions nécessaires en fonction des risques identifiés		
Documentation interne	Notification à l'AS	Communication aux personnes concernées
	X	X

2.2 CAS n° 02 : Ransomware sans sauvegarde appropriée de

L'un des ordinateurs utilisés par une entreprise agricole a été exposé à une attaque de ransomware et ses données ont été cryptées par l'attaquant. L'entreprise fait appel à l'expertise d'une société de cybersécurité externe pour surveiller son réseau. Des journaux retraçant tous les flux de données quittant l'entreprise (y compris les courriels sortants) sont disponibles. Après avoir analysé les journaux et les données collectées par les autres systèmes de détection, l'enquête interne menée avec l'aide de la société de cybersécurité a déterminé que l'auteur de l'attaque n'a fait que crypter les données, sans les exfiltrer. Les journaux ne montrent aucun flux de données sortant pendant la durée de l'attaque. Les données personnelles affectées par la violation concernent les employés et les clients de l'entreprise, soit quelques dizaines de personnes au total. Aucune catégorie particulière de données n'a été touchée. Aucune sauvegarde n'était disponible sous forme électronique. La plupart des données ont été restaurées à partir de sauvegardes papier. La restauration 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 du risque

26. Le responsable du traitement des données devrait avoir adopté les mêmes mesures préalables que celles mentionnées dans la partie 2.1. et dans la section
2.9. La principale différence avec le cas précédent est l'absence de sauvegarde électronique et l'absence de cryptage au repos. Cela conduit à des différences critiques dans les étapes suivantes.

27. Lors de l'évaluation des risques, le responsable du traitement doit étudier la méthode d'infiltration et identifier le type de code malveillant pour comprendre les conséquences possibles de l'attaque. Dans cet exemple, le ransomware a crypté les données personnelles sans les exfiltrer. Par conséquent, il apparaît que les risques pour les droits et libertés des personnes concernées résultent de l'absence de disponibilité des données personnelles, et que la confidentialité des données personnelles n'est pas compromise. Un examen approfondi des journaux du pare-feu et de ses implications est essentiel pour déterminer le risque. Le responsable du traitement des données doit présenter les conclusions factuelles de ces enquêtes sur demande.

28. Le responsable du traitement des données doit garder à l'esprit que si l'attaque est plus sophistiquée, le logiciel malveillant a la possibilité de modifier les fichiers journaux et de supprimer la trace. Ainsi, étant donné que les journaux ne sont pas transmis ou répliqués sur un serveur central de journaux, même après une enquête approfondie qui a permis de déterminer que les données à caractère personnel n'ont pas été exfiltrées par l'attaquant, le responsable du traitement ne peut pas affirmer que l'absence d'entrée dans le journal prouve l'absence d'exfiltration.

29. Le responsable du traitement des données doit évaluer les risques de cette violation[13] si les données ont

été consultées par l'attaquant. Au cours de l'évaluation des risques, le responsable du traitement des données doit également prendre en considération la nature, la sensibilité, le degré de confidentialité et le niveau de sécurité des données.

[13] Pour des orientations sur les opérations de traitement "*susceptibles d'entraîner un risque élevé*", voir la note de bas de page 10 ci-dessus.

le volume et le contexte des données personnelles concernées par la violation. Dans ce cas, aucune catégorie spéciale de données personnelles n'est affectée, et la quantité de données violées et le nombre de personnes concernées sont faibles.

30. La collecte d'informations exactes 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 de la base de données, cela aurait évidemment été un facteur d'augmentation du risque. En cas d'incertitude quant aux spécificités de l'accès illégitime, il convient d'envisager le pire scénario et d'évaluer le risque en conséquence.

31. L'absence d'une base de données de sauvegarde peut être considérée comme un facteur d'accroissement du risque en fonction de la gravité des conséquences pour les personnes concernées résultant du manque de disponibilité des données.

2.2.2 CAS n° 02 - Atténuation et obligations

32. Sans sauvegarde, le responsable du traitement ne peut prendre que peu de mesures pour remédier à la perte de données à caractère personnel, et les données doivent être collectées à nouveau, à moins qu'une autre source ne soit disponible (par exemple, des courriers électroniques de confirmation de commande). Sans sauvegarde, les données peuvent être perdues et la gravité dépendra de l'impact sur les personnes.

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

34. L'information des personnes concernées par la violation peut également dépendre de la durée pendant laquelle les données à caractère personnel sont indisponibles et des difficultés que cela pourrait entraîner dans le fonctionnement du responsable du traitement (par exemple, des retards dans le transfert des paiements des employés). Étant donné que ces retards dans les paiements et les livraisons peuvent entraîner des pertes financières pour les personnes dont les données ont été compromises, on pourrait également affirmer que la violation est susceptible d'entraîner un risque élevé. En outre, il pourrait être impossible d'éviter d'informer les personnes concernées si leur contribution est nécessaire pour restaurer les données cryptées.

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

Actions nécessaires en fonction des risques identifiés		
Documentation interne	Notification à l'AS	Communication aux personnes concernées
		X

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

2.3 CAS n° 03 : Ransomware 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 ransomware et une partie importante de ses données a été chiffrée par l'attaquant. L'entreprise fait appel à l'expertise d'une société externe de cybersécurité pour surveiller son réseau. Des journaux retraçant tous les flux de données quittant l'entreprise (y compris les e-mails sortants) sont disponibles. Après avoir analysé les journaux et les données collectées par les autres systèmes de détection, l'enquête interne menée avec l'aide de la société de cybersécurité a permis de déterminer que l'auteur de l'attaque n'a fait que crypter les données sans les exfiltrer. Les journaux ne montrent aucun flux de données vers l'extérieur pendant la durée de l'attaque. Les données personnelles affectées par la violation concernent les employés et les patients, ce qui représente des milliers d'individus. Des sauvegardes étaient disponibles sous forme électronique. La plupart des données ont été restaurées mais cette opération a duré 2 jours ouvrables et a entraîné des retards importants dans le traitement des patients avec des opérations annulées / reportées, ainsi qu'une baisse du niveau de service en raison de l'indisponibilité des systèmes.

2.3.1 CAS n° 03 - Mesures préalables et évaluation du risque

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

37. La quantité de données violées et le nombre de personnes concernées sont élevés, car les hôpitaux traitent généralement de grandes quantités de données. L'indisponibilité des données a un impact important sur une grande partie des personnes concernées. En outre, il existe un risque résiduel de haute gravité pour la confidentialité des données des patients.

38. Le type de violation, la nature, la sensibilité et le volume des données personnelles concernées par la violation sont importants. Même s'il existait une sauvegarde des données et qu'elles ont pu être restaurées en quelques jours, un risque élevé existe toujours en raison de la gravité des conséquences pour les personnes concernées résultant du manque de disponibilité des données au moment de l'attaque et les jours suivants.

2.3.2 CAS n° 03 - Atténuation et obligations

39. Une notification à l'AS est jugée nécessaire, car des catégories spéciales de données personnelles sont concernées et la restauration des données pourrait prendre beaucoup de temps, ce qui entraînerait des retards importants dans les soins aux patients. L'information des personnes concernées par la violation est nécessaire en raison de l'impact sur les patients, même après la restauration des données cryptées. Alors que les données relatives à tous les patients traités à l'hôpital au cours des dernières années ont été cryptées, seuls les patients qui devaient être traités à l'hôpital pendant la période d'indisponibilité du système informatique ont été touchés. Le responsable du traitement doit communiquer la violation des données à ces patients directement. La communication directe aux autres patients, dont certains n'ont peut-être pas été traités à l'hôpital depuis plus de vingt ans, peut ne pas être nécessaire en raison de l'exception prévue à l'article 34, paragraphe 3, point c). Dans ce cas, il convient de prévoir une communication publique[16] ou une mesure similaire permettant d'informer les personnes concernées de manière tout aussi efficace. En l'espèce, l'hôpital devrait rendre publics l'attaque par ransomware et ses effets.

[15] Pour des orientations sur les opérations de traitement "*susceptibles d'entraîner un risque élevé*", voir la note de bas de page 10 ci-dessus.

[16] Le considérant 86 du GDPR explique que "*Ces communications aux personnes concernées devraient être effectuées dès que cela est raisonnablement possible et en étroite coopération avec l'autorité de contrôle, en respectant les orientations fournies par celle-ci ou par d'autres autorités compétentes telles que les autorités chargées de faire respecter la loi. Par exemple, la nécessité d'atténuer un risque de dommage immédiat exigerait une communication rapide avec les personnes concernées, tandis que la nécessité de mettre en œuvre des mesures appropriées contre des violations de données personnelles continues ou similaires peut justifier un délai de communication plus long*".

40. Ce cas sert d'exemple pour une attaque par ransomware présentant un risque élevé pour les droits et libertés des personnes concernées. Il doit être documenté conformément à l'article 33 (5), notifié à l'AS conformément à l'article 33 (1) et communiqué aux personnes concernées conformément à l'article 34 (1). L'organisation doit également mettre à jour et remédier à ses mesures et procédures organisationnelles et techniques de traitement de la sécurité des données personnelles et d'atténuation des risques.

Actions nécessaires en fonction des risques identifiés		
Documentation interne	Notification à l'AS	Communication aux personnes concernées

2.4 CAS n° 04 : Ransomware sans sauvegarde et avec exfiltration

Le serveur d'une société de transport public a été exposé à une attaque par ransomware et ses données ont été cryptées par l'attaquant. Selon les conclusions de l'enquête interne, l'auteur de l'attaque a non seulement crypté les données, mais il les a également exfiltrées. Le type de données violées était les données personnelles des clients et des employés, ainsi que des plusieurs milliers de personnes utilisant les services de l'entreprise (par exemple, l'achat de billets en ligne). Au-delà des données d'identité de base, des numéros de cartes d'identité et des données financières telles que des détails de cartes de crédit sont concernés par la violation. Une base de données de sauvegarde existait, mais elle a également été chiffrée par l'attaquant.

2.4.1 CAS N° 04 - Mesures préalables et évaluation du risque

41. Le responsable du traitement des données devrait avoir adopté les mêmes mesures préalables que celles mentionnées dans la partie 2.1. et dans la section
2.5. Bien qu'une sauvegarde ait été mise en place, elle a également été affectée par l'attaque. Cette disposition soulève à elle seule des questions sur la qualité des mesures de sécurité informatique antérieures du responsable du traitement et devrait être examinée de plus près au cours de l'enquête, car dans un régime de sauvegarde bien conçu, plusieurs sauvegardes doivent être stockées en toute sécurité sans accès au système principal, sinon elles pourraient être compromises dans la même attaque. En outre, les attaques par ransomware peuvent rester non découvertes pendant des jours, en chiffrant lentement des données rarement utilisées. Cela peut rendre les sauvegardes multiples inutiles, c'est pourquoi les sauvegardes doivent également être effectuées périodiquement et être isolées. Cela augmenterait la probabilité de récupération, mais avec une perte accrue de données.

42. Cette violation concerne non seulement la disponibilité des données, mais aussi leur confidentialité, puisque l'attaquant peut avoir modifié et/ou copié des données du serveur. Par conséquent, le type de violation entraîne un risque élevé[17] .

43. La nature, la sensibilité et le volume des données personnelles augmentent encore les risques, car le nombre de personnes concernées est élevé, tout comme la quantité globale de données personnelles touchées. Au-delà des données d'identité de base, les documents d'identité et les données financières telles que les détails des cartes 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 - pour une usurpation d'identité ou une fraude.

44. En raison d'une logique de serveur défectueuse ou de contrôles organisationnels, les fichiers de sauvegarde ont été affectés par le ransomware, empêchant la restauration des données et augmentant le risque.

[17] Pour des orientations sur les opérations de traitement "*susceptibles d'entraîner un risque élevé*", voir la note de bas de page 10 ci-dessus.

45. Cette violation des données présente un risque élevé pour les droits et libertés des personnes, car elle pourrait vraisemblablement entraîner des dommages matériels (par exemple, une perte financière, puisque les données relatives aux cartes de crédit ont été affectées) et immatériels (par exemple, une usurpation d'identité ou une fraude, puisque les données relatives aux cartes d'identité ont été affectées).

2.4.2 CAS N° 04 - Atténuation et obligations

46. La communication aux personnes concernées est essentielle, afin qu'elles puissent prendre les mesures nécessaires pour éviter tout dommage matériel (par exemple, bloquer leurs cartes de crédit).

47. Outre la documentation de la violation conformément à l'article 33, paragraphe 5, une notification à l'AS 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). Cette communication peut se faire sur une base individuelle, mais pour les personnes dont les coordonnées ne sont pas disponibles, le responsable du traitement doit le faire publiquement, à condition que cette communication ne soit pas susceptible d'entraîner des conséquences négatives supplémentaires pour les personnes concernées, par exemple par le biais 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 les références exactes des dispositions pertinentes du GDPR. L'organisation peut également être amenée à mettre à jour et à remédier à ses mesures et procédures organisationnelles et techniques de traitement de la sécurité des données personnelles et d'atténuation des risques.

Actions nécessaires en fonction des risques identifiés		
Documentation interne	Notification à l'AS	Communication aux personnes concernées

2.5 Mesures organisationnelles et techniques pour prévenir / atténuer les impacts des attaques par ransomware.

48. Le fait qu'une attaque par ransomware ait pu avoir lieu est généralement le signe d'une ou plusieurs vulnérabilités dans le système du responsable du traitement. Cela vaut également pour les cas de ransomware dans lesquels les données à caractère personnel ont été cryptées, mais n'ont pas été exfiltrées. Indépendamment de l'issue et des conséquences de l'attaque, on ne soulignera jamais assez l'importance d'une évaluation globale du système de sécurité des données - avec un accent particulier sur la sécurité informatique. Les faiblesses et les failles de sécurité identifiées doivent être documentées et traitées sans délai.

49. Mesures conseillées :

(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, c'est au responsable du traitement qu'il appartient de décider des mesures les plus adaptées à la situation donnée).

- Maintenir à jour le micrologiciel, le système d'exploitation et les logiciels d'application sur les serveurs, les machines clientes, les composants actifs du réseau et toute autre machine sur le même réseau local (y compris les dispositifs Wi-Fi). S'assurer que des mesures de sécurité informatique appropriées sont en place, s'assurer de leur efficacité et les maintenir régulièrement à jour lorsque le traitement ou les circonstances changent ou évoluent. Il s'agit notamment de tenir des journaux détaillés indiquant quels correctifs sont appliqués et à quel moment.
- Concevoir et organiser les systèmes de traitement et l'infrastructure pour segmenter ou isoler les systèmes de données et les réseaux afin d'éviter la propagation des logiciels malveillants au sein de

l'organisation et vers les systèmes externes.

- L'existence d'une procédure de sauvegarde actualisée, sécurisée et testée. Les supports de sauvegarde à moyen et long terme doivent être séparés du stockage des données opérationnelles et hors de portée des tiers, même en cas d'attaque réussie (comme la sauvegarde incrémentielle quotidienne et la sauvegarde complète hebdomadaire).
- Avoir/obtenir un logiciel anti-malware approprié, à jour, efficace et intégré.

- Disposer d'un pare-feu et d'un système de détection et de prévention des intrusions appropriés, à jour, efficaces et intégrés. Diriger le trafic réseau à travers le pare-feu/détection d'intrusion, même en cas de travail à domicile ou mobile (par exemple en utilisant des connexions VPN aux mécanismes de sécurité de l'organisation lors de l'accès à l'internet).
- Former les employés aux méthodes de reconnaissance et de prévention des attaques informatiques. Le responsable du traitement doit fournir les moyens d'établir si les courriels et les messages obtenus par d'autres moyens de communication sont authentiques et dignes de confiance. Les employés doivent être formés à reconnaître quand une telle attaque s'est produite, à savoir comment retirer le point d'extrémité du réseau et à leur obligation de le signaler immédiatement au responsable de la sécurité.
- Insistez sur la nécessité d'identifier le type de code malveillant pour connaître les conséquences de l'attaque et être en mesure de trouver les bonnes mesures pour atténuer le risque. Si une attaque par ransomware a réussi et qu'aucune sauvegarde n'est disponible, des outils tels que ceux du projet "no more ransom" (nomoreransom.org) peuvent être utilisés pour récupérer les données. Toutefois, si une sauvegarde sûre est disponible, il est conseillé de restaurer les données à partir de celle-ci.
- Transmission ou réplication de tous les journaux vers un serveur central de journaux (incluant éventuellement la signature ou l'horodatage cryptographique des entrées de journaux).
- Cryptage fort et authentification multi-factorielle, en particulier pour l'accès administratif aux systèmes informatiques, gestion appropriée des clés et des mots de passe.
- Tests de vulnérabilité et de pénétration sur une base régulière.
- Créez une équipe de réponse aux incidents de sécurité informatique (CSIRT) ou une équipe de réponse aux urgences informatiques (CERT) au sein de l'organisation, ou rejoignez une CSIRT/CERT collective. Créez un plan d'intervention en cas d'incident, un plan de reprise après sinistre et un plan de continuité des activités, et veillez à ce qu'ils soient testés de manière approfondie.
- Lors de l'évaluation des contre-mesures - l'analyse des risques doit être revue, testée et mise à jour.

3 EXFILTRATION DE DONNÉES ATTAQUES

50. Les attaques qui exploitent les vulnérabilités des services offerts par le responsable du traitement à des tiers sur l'internet, par exemple par le biais d'attaques par injection (par exemple, injection SQL, traversée de chemins), de compromission de sites web et de méthodes similaires, peuvent ressembler à des attaques par ransomware dans la mesure où le risque émane de l'action d'un tiers non autorisé, mais ces attaques visent généralement à copier, exfiltrer et utiliser abusivement des données à caractère personnel à des fins malveillantes. Il s'agit donc principalement d'atteintes à la confidentialité et, éventuellement, à l'intégrité des données. Dans le même temps, si le responsable du traitement est conscient des caractéristiques de ce type de violation, il dispose de nombreuses mesures qui peuvent réduire considérablement le risque de réussite d'une attaque.

3.1 CAS n° 05 : Exfiltration de données de candidatures 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 web. Ce code malveillant rendait accessibles à une ou plusieurs personnes non autorisées les informations personnelles soumises par le biais de formulaires de demande d'emploi en ligne et stockées sur le serveur web. 213 formulaires de ce type sont susceptibles d'être affectés, mais après analyse des données concernées, il a été déterminé qu'aucune catégorie spéciale de données n'a été touchée par la violation. La boîte à outils malveillante installée possédait des fonctionnalités qui permettaient à l'attaquant de supprimer tout historique d'exfiltration et permettaient également de surveiller le traitement sur le serveur et de capturer des données personnelles. La boîte à outils a été découverte un mois seulement après son installation.

3.1.1 CAS n° 05 - Mesures préalables et évaluation du risque

51. La sécurité de l'environnement du responsable du traitement des données est extrêmement importante, car la majorité de ces violations peuvent être évitées en veillant à ce que tous les systèmes soient constamment mis à jour, que les données sensibles soient cryptées et que

les applications sont développées selon des normes de sécurité élevées, telles que l'authentification forte, les mesures contre les attaques par force brute, l'échappement ou l'assainissement des entrées utilisateur[18] , etc. Des audits de sécurité informatique, des évaluations de vulnérabilité et des tests de pénétration périodiques sont également nécessaires pour détecter à l'avance ce type de vulnérabilités et les corriger. Dans ce cas particulier, des outils de surveillance de l'intégrité des fichiers dans l'environnement de production auraient pu aider à détecter l'injection de code. (Une liste de mesures recommandées se trouve à la section 3.7).

52. Le responsable du traitement doit 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 cela soit rapide et efficace, le responsable du traitement doit disposer d'un plan de réponse aux incidents qui précise les mesures rapides et nécessaires pour prendre le contrôle de l'incident. Dans ce cas particulier, le type de violation a été un facteur d'augmentation du risque, car non seulement la confidentialité des données a été restreinte, mais l'infiltré avait également les moyens d'établir des changements dans le système, de sorte que l'intégrité des données a également été remise en question.

53. La nature, la sensibilité et le volume des données personnelles concernées par la violation doivent 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 une quantité considérable d'informations sur les personnes provenant des formulaires en ligne, et ces données pourraient être utilisées à mauvais escient de plusieurs façons (ciblage par des actions de marketing non sollicitées, 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. Les enseignements tirés de la violation doivent être utilisés pour mettre à jour l'infrastructure informatique. Le responsable du traitement des données doit remettre tous les systèmes informatiques concernés dans un état propre connu, remédier à la vulnérabilité et mettre en œuvre de nouvelles mesures de sécurité pour éviter des violations de données similaires à l'avenir, par exemple des contrôles d'intégrité des fichiers et des audits de sécurité. Si les 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 où elles se trouvaient avant la violation. Il peut être nécessaire d'appliquer des sauvegardes complètes, des modifications incrémentielles, puis éventuellement de réexécuter le traitement depuis la dernière sauvegarde incrémentielle - ce qui suppose que le responsable du traitement soit en mesure de reproduire les modifications apportées depuis la dernière sauvegarde. Cela peut nécessiter que le contrôleur dispose d'un système conçu pour conserver les fichiers d'entrée quotidiens au cas où ils devraient être traités à nouveau, ce qui requiert une méthode de stockage robuste et une politique de conservation appropriée.

55. À la lumière de ce qui précède, étant donné que la violation est susceptible d'entraîner un risque élevé pour les droits et libertés des personnes physiques, les personnes concernées doivent absolument en être informées (article 34, paragraphe 1), ce qui signifie bien sûr que la ou les AS concernées doivent également être impliquées sous la forme d'une notification de violation de données. La documentation de la violation est obligatoire conformément à l'article 33, paragraphe 5, du GDPR et facilite l'évaluation de la situation.

Actions nécessaires en fonction des risques identifiés		
Documentation interne	Notification à l'AS	Communication aux personnes concernées

[18] L'échappement ou la désinfection des entrées utilisateur est une forme de validation des entrées, qui garantit que seules des données correctement formatées sont saisies dans un système d'information.

[19] Pour des orientations sur les opérations de traitement "*susceptibles d'entraîner un risque élevé*", voir la note de bas de page 10 ci-dessus.

3.2 CAS n° 06 : Exfiltration du mot de passe haché d'un site web

Une vulnérabilité d'injection SQL a été exploitée pour accéder à la base de données du serveur d'un site web de cuisine. Les utilisateurs étaient uniquement autorisés à choisir des pseudonymes arbitraires comme noms d'utilisateur. L'utilisation d'adresses électroniques à cette fin était déconseillée. Les mots de passe stockés dans la base de données étaient hachés avec un algorithme fort et le sel n'a pas été compromis. Données affectées : mots de passe hachés de 1 200 utilisateurs. Par mesure de sécurité, le responsable du traitement a informé les personnes concernées de la violation par courrier électronique 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 du risque

56. Dans ce cas particulier, la confidentialité des données est compromise, mais les mots de passe de la base de données ont été hachés à l'aide d'une méthode actualisée, ce qui diminue le risque lié à la nature, à la sensibilité et au volume des données personnelles. Ce cas ne présente aucun risque pour les droits et libertés des personnes concernées.

57. En outre, aucune information de contact (par exemple, des adresses e-mail ou des numéros de téléphone) des personnes concernées n'a été compromise, ce qui signifie qu'il n'y a pas de risque significatif pour les personnes concernées d'être visées par des tentatives de fraude (par exemple, recevoir des e-mails de phishing ou des SMS et des appels téléphoniques frauduleux). Aucune catégorie spéciale de données personnelles n'a été impliquée.

58. Certains noms d'utilisateur pourraient être considérés comme des données à caractère personnel, mais le sujet du site web ne permet pas de connotations négatives. Il convient toutefois de noter que l'évaluation des risques peut changer[20] , si le type de site web et les données auxquelles on accède 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 cryptage de pointe pourrait atténuer les effets négatifs de la violation. En veillant à ce qu'un nombre limité de tentatives de connexion soit autorisé, on empêchera les attaques de connexion par force brute de réussir, ce qui réduira considérablement les risques imposés par des attaquants connaissant 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, puisque les personnes concernées sont également en mesure de prendre les mesures nécessaires pour éviter que la violation ne cause d'autres dommages, par exemple en changeant 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 des données doit corriger la vulnérabilité et mettre en œuvre de nouvelles mesures de sécurité afin d'éviter des violations de données similaires à l'avenir, comme par exemple des audits de sécurité systématiques du site web.

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

62. De même, il est fortement conseillé de communiquer aux personnes concernées une violation impliquant des mots de passe, même si les mots de passe ont été stockés en utilisant un hachage salé avec un algorithme conforme à l'état de l'art. Il est préférable d'utiliser des méthodes d'authentification qui évitent de traiter les mots de passe du côté du serveur. Les personnes concernées devraient avoir le choix de prendre les mesures appropriées concernant leurs propres mots de passe.

Actions nécessaires en fonction des risques

identifiés		
Documentation interne	Notification à l'AS	Communication aux personnes concernées
	X	X

[20] Pour des orientations sur les opérations de traitement "*susceptibles d'entraîner un risque élevé*", voir la note de bas de page 10 ci-dessus.

3.3 CAS n° 07 : attaque par bourrage de crÃ©dits sur un site web bancaire

Une banque a subi une cyber-attaque contre l'un de ses sites de banque en ligne. L'attaque visait à énumérer tous les identifiants de connexion possibles en utilisant un mot de passe trivial fixe. Les mots de passe sont composés de 8 chiffres. En raison d'une 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'attaquant, même si le mot de passe utilisé n'était pas correct ou si le compte bancaire n'était plus actif. Environ 100 000 personnes concernées ont été touchées. Sur ce nombre, l'attaquant a réussi à se connecter à environ 2 000 comptes qui utilisaient le mot de passe trivial qu'il a essayé d'utiliser. Après coup, le responsable du traitement a été en mesure d'identifier toutes les tentatives de connexion illégitimes. Le responsable du traitement a pu confirmer que, selon les contrôles antifraude, aucune transaction n'a été effectuée par ces comptes pendant l'attaque. La banque était consciente de la violation de données car son centre d'opérations de sécurité a détecté un nombre élevé de demandes de connexion dirigées vers le site web. En réponse, le responsable du traitement a désactivé la possibilité de se connecter au site web et a forcé la réinitialisation du mot de passe des comptes compromis. Le responsable du traitement n'a communiqué la violation qu'aux utilisateurs dont les comptes ont été 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 du risque

63. Il est important de mentionner que les responsables du traitement des données à caractère hautement personnel[21] ont une plus grande responsabilité en termes de sécurité des données, par exemple en disposant d'un centre d'opérations de sécurité et d'autres mesures de prévention, de détection et de réponse aux incidents. Le non-respect de ces normes plus strictes entraînera certainement des mesures plus graves lors de l'enquête de l'autorité de surveillance.

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

65. Le fait qu'une violation ait pu se produire dans un environnement aussi sensible met en évidence des failles importantes dans la sécurité des données du système du responsable du traitement, et peut être un indicateur du moment où l'examen et la mise à jour des mesures concernées sont "nécessaires" conformément aux articles 24, paragraphe 1, 25, paragraphe 1, et 32, paragraphe 1, du GDPR. Les données violées permettent l'identification unique des personnes concernées et contiennent d'autres informations à leur sujet (notamment le sexe, la date et le lieu de naissance), en outre, elles peuvent être utilisées par l'attaquant pour deviner les mots de passe des clients ou pour mener une campagne de spear phishing dirigée vers les clients de la banque.

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

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 la violation, il a également corrigé la vulnérabilité du site web et pris d'autres mesures pour prévenir de futures violations de données similaires, telles que

[21] Telles que les informations des personnes concernées relatives aux méthodes de paiement telles que les numéros de carte, les comptes bancaires, le paiement en ligne, les salaires, les relevés bancaires, les études économiques ou toute autre information susceptible de révéler des informations économiques relatives aux personnes concernées.

[22] Pour des orientations sur les opérations de traitement "*susceptibles d'entraîner un risque élevé*", voir la note de bas de page 10 ci-dessus.

comme l'ajout d'une authentification à deux facteurs sur le site web concerné et le passage à une authentification forte du client.

68. La documentation de la violation conformément à l'article 33, paragraphe 5, du GDPR et la notification de l'AS à ce sujet ne sont pas facultatives dans ce scénario. En outre, le responsable du traitement doit notifier les 100 000 personnes concernées (y compris les personnes dont les comptes n'ont pas été compromis) conformément à l'article 34 du GDPR.

Actions nécessaires en fonction des risques identifiés		
Documentation interne	Notification à l'AS	Communication aux personnes concernées

3.4 Mesures organisationnelles et techniques pour prévenir / atténuer les impacts des attaques de pirates informatiques.

69. Comme dans le cas des attaques par ransomware, quels que soient le résultat et les conséquences de l'attaque, la réévaluation de la sécurité informatique est obligatoire pour les contrôleurs dans des cas similaires.

70. Mesures conseillées :[23]

(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, c'est au responsable du traitement qu'il appartient de décider des mesures les plus adaptées à la situation donnée*).

- Cryptage et gestion des clés à la pointe de la technologie, en particulier lorsque des mots de passe, des données sensibles ou financières sont traités. Le hachage et le salage cryptographiques des informations secrètes (mots de passe) sont toujours préférables au cryptage des mots de passe. L'utilisation de méthodes d'authentification évitant le traitement des mots de passe du côté du serveur est préférable.
- Maintenir le système à jour (logiciels et micrologiciels). S'assurer que toutes les mesures de sécurité informatique sont en place, s'assurer de leur efficacité et les tenir 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 GDPR, le responsable du traitement doit tenir un registre de toutes les mises à jour effectuées, y compris le moment où elles ont été appliquées.
- Utilisation de méthodes d'authentification forte comme l'authentification à deux facteurs et les serveurs d'authentification, complétée par une politique de mot de passe actualisée.
- Les normes de développement sécurisé comprennent le filtrage des entrées utilisateur (en utilisant la liste blanche dans la mesure du possible), l'échappement des entrées utilisateur et les mesures de prévention de la force brute (telles que la limitation du nombre maximal de tentatives). Les "Web Application Firewalls" peuvent contribuer à l'utilisation efficace de cette technique.
- Mise en place d'une politique solide de gestion des privilèges des utilisateurs et du contrôle d'accès.
- Utilisation de systèmes de pare-feu, de détection des intrusions et d'autres systèmes de défense du périmètre appropriés, à jour, efficaces et intégrés.
- Audits systématiques de la sécurité informatique et évaluation des vulnérabilités (tests de pénétration).
- Examens et tests réguliers pour s'assurer que les sauvegardes peuvent être utilisées pour restaurer toute donnée dont l'intégrité ou la disponibilité a été affectée.
- Pas d'ID 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 RISQUE HUMAIN INTERNE SOURCE

71. Le rôle de l'erreur humaine dans les violations de données à caractère personnel doit être souligné, en raison de son aspect courant. Étant donné que ces types de violations peuvent être aussi bien intentionnels qu'involontaires, il est très difficile pour les responsables du traitement des données 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 d'aborder ces facteurs humains et a adopté la résolution visant à traiter le rôle de l'erreur humaine dans les violations de données personnelles en octobre 2019[24] . Cette résolution souligne que des mesures de sauvegarde appropriées doivent être prises pour prévenir les erreurs humaines et fournit une liste non exhaustive de ces mesures de sauvegarde et approches.

4.1 CAS n° 08 : Exfiltration de données professionnelles par un employé de

Pendant sa période de préavis, le salarié d'une entreprise copie des données commerciales de la base de données de l'entreprise. Le salarié n'est autorisé à accéder à ces données que pour remplir ses tâches professionnelles. Quelques mois plus tard, après avoir quitté son emploi, il utilise les données ainsi obtenues (données de contact de base) pour alimenter un nouveau traitement de données dont il est le responsable afin de contacter les clients de l'entreprise pour les attirer dans sa nouvelle activité.

4.1.1 CAS n° 08 - Mesures préalables et évaluation du risque

72. Dans ce cas particulier, aucune mesure préalable n'a été prise pour empêcher l'employé de copier les coordonnées de la clientèle de l'entreprise, puisqu'il avait besoin - et avait - un accès légitime à ces informations pour ses tâches professionnelles. Étant donné que la plupart des emplois dans le domaine des relations avec la clientèle exigent que l'employé accède d'une manière ou d'une autre à des données à caractère personnel, ces violations de données peuvent être les plus difficiles à prévenir. La limitation de la portée de l'accès peut restreindre le travail que l'employé concerné est en mesure d'accomplir. Toutefois, des politiques d'accès bien conçues et un contrôle constant peuvent contribuer à prévenir de telles violations.

73. Comme d'habitude, lors de l'évaluation des risques, il convient de prendre en considération 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, puisque la base de données est généralement laissée intacte, son contenu étant "simplement" copié pour une utilisation ultérieure. La quantité de données concernées est généralement faible ou moyenne. Dans ce cas particulier, aucune catégorie spéciale de données à caractère personnel n'a été affectée, l'employé avait seulement besoin des coordonnées de clients pour pouvoir les contacter après avoir quitté l'entreprise. Par conséquent, les données concernées ne sont pas sensibles.

74. Bien que le seul objectif de l'ex-employé qui a malicieusement copié les données puisse se limiter à obtenir les coordonnées de la clientèle de l'entreprise 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, puisqu'il n'a aucune garantie quant aux intentions de l'employé. Ainsi, alors que les conséquences de la violation pourraient se limiter à l'exposition de l'ex-employé à des pratiques d'auto-marketing injustifiées, un abus plus grave des données volées n'est pas exclu, en fonction de la finalité du traitement mis en place par l'ex-employé[25] .

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

[25] Pour des orientations sur les opérations de traitement "*susceptibles d'entraîner un risque élevé*", voir la note de bas de page 10 ci-dessus.

4.1.2 CAS N° 08 - Atténuation et obligations

75. L'atténuation des effets négatifs de la violation dans le cas ci-dessus est difficile. Il peut être nécessaire d'engager une action en justice immédiate pour empêcher l'ancien employé d'abuser des données et de les diffuser plus avant. Dans un deuxième temps, l'objectif devrait être d'éviter que des situations similaires ne se reproduisent. Le responsable du traitement peut essayer d'ordonner à l'ex-employé de cesser d'utiliser les données, mais le succès de cette action est au mieux douteux. Des mesures techniques appropriées, telles que l'impossibilité de copier ou de télécharger des données sur des dispositifs amovibles, peuvent être utiles.

76. Il n'existe pas de solution unique pour ce type de cas, mais une approche systématique peut contribuer à les prévenir. Par exemple, l'entreprise peut envisager - lorsque c'est possible - de retirer certaines formes d'accès aux employés qui ont signalé leur intention de démissionner ou de mettre en place des journaux d'accès afin que les accès indésirables puissent être enregistrés et signalés. Le contrat signé avec les employés doit comporter des clauses interdisant de telles actions.

77. Dans l'ensemble, comme la violation en question n'entraînera pas un risque élevé pour les droits et libertés des personnes physiques, une notification à l'AS suffira. Toutefois, l'information des personnes concernées peut également être bénéfique pour le responsable du traitement des données, car il est préférable qu'elles soient informées de la fuite de données par l'entreprise plutôt que par l'ex-employé qui tente de les contacter. Documentation relative à la violation des données conformément à l'article 33
(5) est une obligation légale.

Actions nécessaires en fonction des risques identifiés		
Documentation interne	Notification à l'AS	Communication aux personnes concernées
		X

4.2 CAS n° 09 : Transmission accidentelle de données à un tiers de confiance

Un agent d'assurance a constaté que - grâce au paramétrage défectueux d'un fichier Excel reçu par e-mail - il a pu accéder à des informations relatives à une vingtaine de clients n'appartenant pas à son périmètre. Il est tenu au secret professionnel et était le seul destinataire de l'e-mail. L'accord entre le responsable du traitement des données et l'agent d'assurance oblige l'agent à signaler au responsable du traitement des données une violation de données personnelles sans délai excessif. Par conséquent, l'agent a immédiatement signalé l'erreur au responsable du traitement, qui a corrigé le fichier et l'a envoyé à nouveau, en demandant à l'agent de supprimer le premier message. Conformément à l'accord 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 uniquement des données de contact et des 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 des données n'a identifié aucune caractéristique particulière de la part des personnes ou du responsable du traitement des données susceptible d'affecter le niveau d'impact de la violation.

4.2.1 CAS N° 09 - Mesures préalables et évaluation du risque

78. Dans ce cas, la violation ne découle pas d'une action intentionnelle d'un employé, mais d'une erreur humaine involontaire causée par l'inattention. Ces types de violation peuvent être évités ou leur fréquence peut être réduite a) en appliquant des programmes de formation, d'éducation et de sensibilisation permettant aux employés de mieux comprendre l'importance de la protection des données personnelles, b) en réduisant l'échange de fichiers par courrier électronique et en utilisant plutôt des systèmes dédiés au traitement des données des clients, par exemple, c) en vérifiant deux fois les fichiers avant de les envoyer, d) en séparant la création et l'envoi des fichiers.

79. Cette violation de données ne concerne que la confidentialité des données, dont l'intégrité et l'accessibilité restent intactes. La violation des données ne concerne que deux douzaines de clients, la quantité de données affectées peut donc être considérée comme faible. En outre, les données personnelles concernées ne contiennent pas de données sensibles. Le fait que le responsable du traitement des données ait immédiatement contacté le contrôleur des données après avoir eu connaissance de la violation des données peut être considéré comme un facteur d'atténuation du risque. (La possibilité que des données aient été envoyées 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 des données, celle-ci n'aura probablement aucune incidence sur les droits et libertés des personnes concernées.

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

4.2.2 CAS n° 09 - Atténuation et obligations

81. En outre, d'autres circonstances atténuant le risque entrent 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 l'inclusion éventuelle d'étapes supplémentaires dans le contrôle des documents impliquant des données à caractère personnel permettront probablement d'éviter des cas similaires à l'avenir.

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

Actions nécessaires en fonction des risques

identifiés		
Documentation interne	Notification à l'AS	Communication aux personnes concernées
	X	X

4.3 Mesures organisationnelles et techniques pour prévenir / atténuer les impacts des sources internes de risques humains

83. Une combinaison des mesures mentionnées ci-dessous - appliquées en fonction des caractéristiques uniques du cas - devrait permettre de réduire le risque qu'une violation similaire se reproduise.

84. Mesures conseillées :

(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, c'est au responsable du traitement qu'il appartient de décider des mesures les plus adaptées à la situation donnée.*)

- Mise en œuvre périodique de programmes de formation, d'éducation et de sensibilisation des employés sur leurs obligations en matière de confidentialité et de sécurité, ainsi que sur la détection et le signalement des menaces pour la sécurité des données personnelles[26] . Développer un programme de sensibilisation pour rappeler aux employés les erreurs les plus courantes menant à des violations de données personnelles et comment les éviter.
- Mise en place de pratiques, procédures et systèmes solides et efficaces en matière de protection des données et de la vie privée[27] .
- Évaluation des pratiques, procédures et systèmes de protection de la vie privée afin d'en assurer l'efficacité continue[28] .
- Élaborer des politiques de contrôle d'accès appropriées et obliger les utilisateurs à respecter les règles.
- Mettre en œuvre des techniques pour forcer l'authentification de l'utilisateur lors de l'accès à des données personnelles sensibles.
- Désactiver le compte de l'utilisateur lié à l'entreprise dès que la personne quitte l'entreprise.
- Vérification des flux de données inhabituels entre le serveur de fichiers et les postes de travail des employés.
- Configuration de la sécurité de l'interface E/S dans le BIOS ou par l'utilisation d'un logiciel contrôlant l'utilisation des interfaces de l'ordinateur (verrouillage ou déverrouillage, par exemple USB/CD/DVD, etc.).
- Examiner la politique d'accès des employés (par exemple, consigner l'accès aux données sensibles et exiger de l'utilisateur qu'il saisisse une raison professionnelle, afin que celle-ci soit disponible pour les audits).
- Désactiver les services de cloud ouverts.
- Interdire et empêcher l'accès à des services de courrier ouverts connus.
- Désactiver la fonction d'impression d'écran dans le système d'exploitation.
- Appliquer une politique de bureau propre.
- Verrouillage automatique de tous les ordinateurs après un certain temps d'inactivité.
- Utilisez des mécanismes (par exemple, un jeton (sans fil) pour se connecter/ouvrir des comptes verrouillés) pour un changement rapide d'utilisateur dans les environnements partagés.
- Utilisation de systèmes dédiés à la gestion des données personnelles qui appliquent des mécanismes de contrôle d'accès appropriés et qui empêchent les erreurs humaines, comme l'envoi de communications à la mauvaise personne. L'utilisation de feuilles de calcul et d'autres documents de bureau ne constitue pas un moyen approprié pour gérer les données des clients.

5 APPAREILS PERDUS OU VOLÉS ET DOCUMENTS PAPIER

85. Un type de cas fréquent est la perte ou le vol d'appareils portables. Dans ces cas, le responsable du traitement doit prendre en considération les circonstances du traitement, telles que le type de données stockées sur l'appareil, ainsi que les actifs de soutien, et les mesures prises avant la violation pour assurer un niveau de sécurité approprié. Tous ces éléments ont une incidence sur les impacts potentiels de la violation des données. L'évaluation des risques peut être difficile, car le dispositif n'est plus disponible.

[26] Section 2) le paragraphe (i) de la résolution pour aborder le rôle de l'erreur humaine dans les violations de données personnelles.

[27] Section 2) le paragraphe (ii) de la résolution pour aborder le rôle de l'erreur humaine dans les violations de données personnelles.

[28] Section 2) paragraphe (iii) de la résolution pour aborder le rôle de l'erreur humaine dans les violations de données personnelles.

86. Ces types de violations peuvent toujours être classés comme des violations de la confidentialité. Cependant, s'il n'y a pas de sauvegarde de la base de données volée, le type de violation peut également être une violation de la disponibilité et une violation de l'intégrité.

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

5.1 CAS n° 10 : Matériel volé stockant des données personnelles cryptées

Lors d'un cambriolage dans une garderie pour enfants, deux tablettes ont été volées. Les tablettes contenaient une application qui contenait des données personnelles sur les enfants fréquentant la garderie. Nom, date de naissance, données personnelles sur l'éducation des enfants étaient concernés. Les tablettes cryptées, qui étaient éteintes au moment de l'effraction, et l'application étaient toutes deux protégées par un mot de passe fort. Les données de sauvegarde étaient effectivement et facilement accessibles au responsable du traitement. Après avoir été informée de l'effraction, la garderie a ordonné à distance l'effacement des tablettes peu après la découverte de l'effraction.

5.1.1 CAS n° 10 - Mesures préalables et évaluation du risque

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

89. Après avoir pris connaissance d'une violation, le responsable du traitement des données doit évaluer la source du risque, les systèmes soutenant le traitement des données, le type de données à caractère personnel concernées et les impacts potentiels de la violation des données sur les personnes concernées. La violation des données décrite ci-dessus aurait pu porter atteinte à la confidentialité, à la disponibilité et à l'intégrité des données concernées, mais grâce aux mesures appropriées prises par le responsable du traitement avant et après la violation des données, aucun de ces problèmes ne s'est produit.

5.1.2 CAS n° 10 - Atténuation et obligations

90. La confidentialité des données personnelles sur les appareils n'a pas été compromise en raison de la forte protection par mot de passe des tablettes et des applications. Les tablettes étaient configurées de manière à ce que la définition d'un mot de passe entraîne également le cryptage des données sur l'appareil. Cette protection a été renforcée par l'action du contrôleur qui a tenté d'effacer à distance toutes les données des appareils volés.

91. Grâce aux mesures prises, la confidentialité des données a également été préservée. En outre, la sauvegarde a permis de garantir la disponibilité continue des données personnelles, ce qui a empêché tout impact négatif potentiel.

92. En raison de ces faits, la violation de données décrite ci-dessus n'était pas susceptible d'entraîner un risque pour les droits et libertés des personnes concernées, de sorte qu'aucune notification à l'AS ou aux personnes concernées n'était nécessaire. Toutefois, cette violation des données doit également être documentée conformément à l'article 33, paragraphe 5.

Actions nécessaires en fonction des risques identifiés		
Documentation interne	Notification à l'AS	Communication aux personnes concernées
	X	X

5.2 CAS n° 11 : Matériel volé stockant des données personnelles non cryptées

L'ordinateur portable électronique d'un employé d'une société prestataire de services a été volé. L'ordinateur portable volé contenait les noms, prénoms, sexe, adresses et dates 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 personnelles étaient également concernées. L'accès au disque dur de l'ordinateur portable n'était protégé par aucun mot de passe. Les données personnelles ont pu être restaurées à partir des sauvegardes quotidiennes disponibles.

5.2.1 CAS n° 11 - Mesures préalables et évaluation du risque

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

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 en l'espèce car il ne possédait aucune protection par mot de passe ou cryptage. L'absence de mesures de sécurité de base accroît le niveau de risque pour les personnes concernées. En outre, l'identification des personnes concernées est également problématique, ce qui accroît également la gravité de la violation. Le nombre considérable de personnes concernées accroît le risque, néanmoins, aucune catégorie spéciale de données à caractère personnel n'était concernée par la violation des données.

96. Au cours de l'évaluation des risques[29] , le responsable du traitement doit prendre en considération les conséquences et les effets négatifs potentiels de la violation de la confidentialité. À la suite de la violation, les personnes concernées peuvent être victimes d'une usurpation d'identité sur la base des données disponibles sur l'appareil volé ; le risque est donc considéré comme élevé.

5.2.2 CAS n° 11 - Atténuation et obligations

97. L'activation du cryptage des appareils et l'utilisation d'un mot de passe fort pour protéger la base de données stockée auraient pu empêcher la violation des données d'entraîner un risque pour les droits et libertés des personnes concernées.

98. En raison de ces circonstances, la notification de l'AS est requise, la notification des personnes concernées est également nécessaire.

Actions nécessaires en fonction des risques identifiés		
Documentation interne	Notification à l'AS	Communication aux personnes concernées

5.3 CAS n° 12 : Vol de dossiers papier contenant des données sensibles

Un registre papier a été volé dans un centre de désintoxication pour toxicomanes. Ce carnet contenait des données de base sur l'identité et la santé des patients admis dans l'établissement de désintoxication. Les données étaient uniquement stockées sur papier et aucune sauvegarde n'était disponible pour les médecins traitant les patients. Le livre n'était pas stocké dans un tiroir ou une pièce fermée à clé, le responsable du traitement des données n'avait ni régime de contrôle d'accès ni aucune autre mesure de sauvegarde pour la documentation papier.

[29] Pour des orientations sur les opérations de traitement "*susceptibles d'entraîner un risque élevé*", voir la note de bas de page 10 ci-dessus.

5.3.1 CAS n° 12 - Mesures préalables et évaluation du risque

99. Aucune mesure de sécurité préalable n'a été prise par le responsable du traitement des données, de sorte que les données à caractère personnel stockées dans ce livre étaient facilement accessibles à la personne qui les trouvait. En outre, la nature des données personnelles stockées dans le livre fait de l'absence de données de sauvegarde un facteur de risque très grave.

100. Ce cas sert d'exemple pour une violation de données à haut risque. En raison de l'absence de mesures de sécurité appropriées, des données sensibles relatives à la santé, conformément à l'article 9, paragraphe 1, du GDPR, ont été perdues. Étant donné qu'il s'agissait dans ce cas d'une catégorie particulière de données à caractère personnel, les risques potentiels pour les personnes concernées étaient 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 personnelles 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 personnelle du patient. La violation de la disponibilité peut également perturber la continuité du traitement des patients. La modification/suppression de certaines parties du contenu du livre n'étant pas exclue, l'intégrité des données personnelles est également compromise.

5.3.2 CAS n° 12 - Atténuation et obligations

102. Lors de l'évaluation des mesures de sauvegarde, il convient également de prendre en compte le type de bien supporté. Le registre des patients étant un document physique, sa sauvegarde aurait dû être organisée différemment de celle d'un dispositif électronique. La pseudonymisation des noms des patients, le stockage du carnet dans des locaux protégés et dans un tiroir ou une pièce verrouillés, ainsi qu'un contrôle d'accès approprié avec authentification lors de l'accès au carnet auraient pu empêcher la violation des données.

103. La violation des données décrite ci-dessus peut avoir de graves conséquences pour les personnes concernées ; la notification de l'AS et la communication de la violation aux personnes concernées sont donc obligatoires.

Actions nécessaires en fonction des risques identifiés		
Documentation interne	Notification à l'AS	Communication aux personnes concernées

5.4 Mesures organisationnelles et techniques pour prévenir/atténuer les impacts 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 permettre de réduire le risque qu'une violation similaire se reproduise.

105. Mesures conseillées :

(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, c'est au responsable du traitement qu'il appartient de décider des mesures les plus adaptées à la situation donnée.*)

- Activez le cryptage de l'appareil (tel que Bitlocker, Veracrypt ou DM-Crypt).
- Utilisez un code d'accès/mot de passe sur tous les appareils. Cryptez tous les appareils électroniques mobiles d'une manière qui nécessite la saisie d'un mot de passe complexe pour le décryptage.
- Utilisez l'authentification multifactorielle.
- Activez les fonctionnalités des appareils très mobiles qui permettent de les localiser en cas de perte ou d'égarement.

[30] Pour des orientations sur les opérations de traitement "*susceptibles d'entraîner un risque élevé*", voir la note de bas de page 10 ci-dessus.

- Utilisez le logiciel/application MDM (Mobile Devices Management) et la localisation. Utilisez des filtres anti-reflets. Fermez tous les appareils non surveillés.
- Si cela est possible et adapté au traitement des données en question, sauvegarder les données personnelles non pas sur un appareil mobile, mais sur un serveur dorsal central.
- Si le poste de travail est connecté au réseau local de l'entreprise, effectuez une sauvegarde automatique à partir des dossiers de travail s'il est inévitable que des données personnelles y soient stockées.
- Utilisez un VPN sécurisé (par exemple, qui nécessite une clé d'authentification de second facteur distincte pour l'établissement d'une connexion sécurisée) pour connecter les appareils mobiles aux serveurs dorsaux.
- Fournissez des verrous physiques aux employés afin de leur permettre de sécuriser physiquement les appareils mobiles qu'ils utilisent lorsqu'ils restent sans surveillance.
- Une réglementation appropriée de l'utilisation des appareils en dehors de l'entreprise.
- Une réglementation appropriée de l'utilisation des appareils au sein de l'entreprise.
- Utilisez le logiciel/application MDM (Mobile Devices Management) et activez la fonction d'effacement à distance.
- Utilisez une gestion centralisée des appareils avec un minimum de droits d'installation de logiciels pour les utilisateurs finaux.
- Installez des contrôles d'accès physiques.
- Évitez de stocker des informations sensibles sur des appareils mobiles ou des disques durs. S'il est nécessaire d'accéder au système interne de l'entreprise, des canaux sécurisés doivent être utilisés, comme indiqué précédemment.

6 MISPOSTAL

106. Dans ce cas également, la source du risque est une erreur humaine interne, mais ici aucune action malveillante n'a conduit à la violation. Elle est le résultat d'une inattention. Le responsable du traitement ne peut pas faire grand-chose après coup. La prévention est donc encore plus importante dans ce cas que dans les autres types de violation.

6.1 CAS n° 13 : erreur de courrier postal

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

6.1.1 CAS n° 13 - Mesures préalables et évaluation du risque

107. Les factures contenaient les données personnelles requises pour une livraison réussie (nom, adresse, ainsi que l'article acheté et son prix). Il est important d'identifier comment l'erreur humaine a pu se produire en premier lieu, et si d'une manière ou d'une autre, elle aurait pu être évitée. Dans le cas particulier décrit, le risque est faible, étant donné qu'aucune catégorie spéciale de données à caractère personnel ou d'autres données dont l'utilisation abusive pourrait entraîner des effets négatifs substantiels n'étaient concernées, 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 doit prévoir le renvoi gratuit des articles et des factures qui les accompagnent, et il doit également demander aux mauvais destinataires de détruire/supprimer toutes les copies éventuelles des factures contenant les données personnelles de l'autre personne.

109. Même si la violation elle-même ne présente pas un risque élevé pour les droits et libertés des personnes concernées, et que la communication aux personnes concernées n'est donc pas obligatoire en vertu de l'article 34 du GDPR, la communication de la violation aux personnes concernées ne peut être évitée, car leur coopération est nécessaire pour atténuer le risque.

Actions nécessaires en fonction des risques identifiés		
Documentation interne	Notification à l'AS	Communication aux personnes concernées
	X	X

6.2 CAS n° 14 : données personnelles hautement confidentielles envoyées par courrier par erreur

Le service de l'emploi d'une administration publique a envoyé un message électronique - concernant des formations à venir - aux personnes enregistrées 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 cet e-mail. Le nombre de personnes concernées s'élève à plus de 60000. Par la suite, le bureau a 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 du risque

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 concernées est considérable, et l'utilisation de leur numéro de sécurité sociale, ainsi que d'autres données personnelles plus fondamentales, augmente encore le risque, qui peut être considéré comme élevé[31] . La distribution 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 précédemment, les moyens de limiter efficacement les risques d'une violation similaire sont limités. Bien que le responsable du traitement ait demandé la suppression du message, il ne peut pas obliger les destinataires à le faire et, par conséquent, il ne peut pas non plus être certain qu'ils se conforment à cette demande.

113. L'exécution des trois actions indiquées ci-dessous devrait être évidente dans un cas comme celui-ci.

Actions nécessaires en fonction des risques identifiés		
Documentation interne	Notification à l'AS	Communication aux personnes concernées

6.3 CAS n° 15 : données personnelles envoyées par courrier par erreur

Une liste de participants à un cours d'anglais juridique qui se déroule dans un hôtel pendant 5 jours est envoyée par erreur à 15 anciens participants au cours au lieu de l'hôtel. La liste contient les noms, adresses e-mail et préférences alimentaires des 15 participants. Seuls deux participants ont indiqué leurs préférences alimentaires, précisant qu'ils sont intolérants au lactose. Aucun des participants n'a une identité protégée. Le responsable du traitement découvre l'erreur immédiatement après l'envoi de la liste, en informe les destinataires et leur demande de supprimer la liste.

6.3.1 CAS n° 15 - Mesures préalables et évaluation du risque

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

[31] Pour des orientations sur les opérations de traitement "*susceptibles d'entraîner un risque élevé*", voir la note de bas de page 10 ci-dessus.

115. Les risques découlant de la nature, de la sensibilité, du volume et du contexte des données à caractère personnel sont faibles. Les données personnelles comprennent des données sensibles sur les préférences alimentaires de deux des participants. Même si l'information selon laquelle une personne est intolérante au lactose est une donnée de santé, le risque que cette donnée soit utilisée de manière préjudiciable doit être considéré comme relativement faible. Si, dans le cas de données relatives à la santé, on suppose généralement que la violation est susceptible d'entraîner un risque élevé pour la personne concernée[32] , dans le même temps, dans ce cas particulier, on ne peut identifier aucun risque que la violation entraîne des dommages physiques, matériels ou immatériels pour la personne concernée en raison de la divulgation non autorisée d'informations relatives à l'intolérance au lactose. Contrairement à d'autres préférences alimentaires, l'intolérance au lactose ne peut normalement pas être liée à des convictions religieuses ou philosophiques. La quantité de données violées 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 s'être rendu compte de l'erreur peut être considéré comme une circonstance atténuante.

117. Si un courrier électronique est envoyé à un destinataire incorrect/non autorisé, il est recommandé que le responsable du traitement des données envoie un courrier électronique de suivi aux destinataires involontaires en leur présentant ses excuses, en leur demandant de supprimer le courrier électronique incriminé et en les informant qu'ils n'ont pas le droit d'utiliser les adresses électroniques qui leur sont identifiées.

118. En raison de ces faits, cette violation des données n'était pas susceptible d'entraîner un risque pour les droits et libertés des personnes concernées, de sorte qu'aucune notification à l'AS ou aux personnes concernées n'était nécessaire. Toutefois, cette violation des données doit également être documentée conformément à l'article 33, paragraphe 5.

Actions nécessaires en fonction des risques identifiés		
Documentation interne	Notification à l'AS	Communication aux personnes concernées
	X	X

6.4 CAS n° 16 : erreur de courrier postal

Un groupe d'assurance propose des assurances automobiles. Pour ce faire, il envoie par courrier postal des polices de cotisation régulièrement adaptées. 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 de santé selon l'article 9 GDPR, les données de paiement (coordonnées bancaires), les données économiques et financières ne sont pas incluses.

Les lettres sont emballées par des machines de mise sous pli automatisées. En raison d'une erreur mécanique, deux lettres destinées à des assurés différents sont insérées dans une enveloppe et envoyées à un assuré par la poste. L'assuré ouvre la lettre chez lui et prend connaissance de sa lettre correctement distribuée ainsi que de la lettre incorrectement distribuée d'un autre assuré.

6.4.1 CAS N° 16 - Mesures préalables et évaluation du risque

119. La lettre remise par erreur 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 sont à considérer comme moyens, car des informations non accessibles au public telles que la date de

[32] Voir les Directives WP 250, p. 23.

les numéros de naissance ou d'immatriculation des véhicules non masqués, ainsi que des détails sur l'augmentation des taux d'assurance sont divulgués au destinataire non autorisé. La probabilité d'une utilisation abusive de ces données est évaluée comme étant faible à moyenne. Toutefois, si de nombreux destinataires jetteront probablement la lettre reçue à tort à la poubelle, il n'est pas totalement exclu, dans certains cas, que la lettre soit publiée sur les réseaux sociaux ou que l'assuré soit contacté.

6.4.2 CAS n° 16 - Atténuation et obligations

120. Le contrôleur doit se faire renvoyer le document original à ses frais. Le mauvais destinataire doit également être informé qu'il ne doit pas faire un mauvais usage des informations lues.

121. Il ne sera probablement jamais possible d'empêcher complètement une erreur de distribution postale dans un envoi de masse utilisant des machines entièrement automatisées. Toutefois, en cas de fréquence accrue, il est nécessaire de vérifier si les machines de mise sous pli sont réglées et entretenues de manière suffisamment correcte, ou si un autre problème systémique est à l'origine d'une telle erreur.

Actions nécessaires en fonction des risques identifiés		
Documentation interne	Notification à l'AS	Communication aux personnes concernées
		X

6.5 Mesures organisationnelles et techniques pour prévenir / atténuer les impacts de mispostal

122. Une combinaison des mesures mentionnées ci-dessous - appliquées en fonction des caractéristiques uniques du cas - devrait permettre de réduire le risque qu'une violation similaire se reproduise.

123. Mesures conseillées :

(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, c'est au responsable du traitement qu'il appartient de décider des mesures les plus adaptées à la situation donnée.*)

- Fixer des normes exactes - sans marge d'interprétation - pour l'envoi de lettres / courriels.
- Formation adéquate du personnel sur la façon d'envoyer des lettres / e-mails.
- Lorsque vous envoyez des messages électroniques à plusieurs destinataires, ceux-ci figurent par défaut dans le champ "bcc".
- Une confirmation supplémentaire est requise lors de l'envoi de messages électroniques à plusieurs destinataires, et ceux-ci ne figurent pas dans le champ "bcc".
- Application du principe des quatre yeux.
- Adressage automatique au lieu d'être manuel, avec des données extraites d'une base de données disponible et à jour ; le système d'adressage automatique doit être régulièrement contrôlé pour vérifier l'absence d'erreurs cachées et de réglages incorrects.
- Application d'un délai pour le message (par exemple, le message peut être supprimé / modifié dans un certain délai après avoir cliqué sur le bouton de pression).
- Désactivation de l'autocomplétion lors de la saisie d'adresses électroniques.
- Sessions de sensibilisation aux erreurs les plus courantes menant à une violation des données personnelles.
- Des sessions de formation et des manuels sur la manière de gérer les incidents conduisant à une violation des données personnelles et sur les personnes à informer (impliquer le DPD).

7 AUTRES CAS - INGÉNIERIE SOCIALE

7.1 CAS n° 17 : Vol d'identité

Le centre de contact d'une société de télécommunications reçoit un appel téléphonique d'une personne qui se fait passer pour un client. Le prétendu client demande à l'entreprise de modifier l'adresse électronique à laquelle les informations de facturation doivent être envoyées à partir de maintenant. L'employé du centre de contact valide l'identité du client en lui demandant certaines données personnelles, telles que définies par les procédures de l'entreprise. L'appelant indique correctement le numéro fiscal et l'adresse postale du client demandé (car il avait accès à ces éléments). Après validation, l'opérateur effectue le changement demandé et, à partir de là, les informations de facturation sont envoyées à la nouvelle adresse électronique. La procédure ne prévoit aucune notification à l'ancien contact électronique. Le mois suivant, le client légitime contacte la société, demandant pourquoi il ne reçoit pas de facturation à son adresse électronique, et nie tout appel de sa part demandant le changement du contact électronique. Plus tard, l'entreprise se rend compte que les informations ont été envoyées à un utilisateur illégitime et annule le changement.

7.1.1 CAS n° 17 - Évaluation et atténuation des risques et obligations

124. Ce cas sert d'exemple sur l'importance des mesures préalables. Du point de vue du risque, la violation présente un niveau de risque élevé33, car les données de facturation peuvent donner des informations sur la vie privée de la personne concernée (par exemple, ses habitudes, ses contacts) et pourraient entraîner des dommages matériels (par exemple, harcèlement, risque pour l'intégrité physique). Les données personnelles obtenues lors de cette attaque peuvent également être utilisées afin de faciliter la prise de contrôle de comptes dans cette organisation ou d'exploiter d'autres mesures d'authentification dans d'autres organisations. Compte tenu de ces risques, la mesure d'authentification "appropriée" doit répondre à une exigence élevée, en fonction des données à caractère personnel qui peuvent être traitées à la suite de l'authentification.

125. Par conséquent, le responsable du traitement doit à la fois adresser une notification à l'autorité de surveillance et une communication à la personne concernée.

126. Le processus antérieur de validation des clients doit manifestement être affiné à la lumière de cette affaire. Les méthodes utilisées pour l'authentification n'étaient pas suffisantes. La partie malveillante a pu se faire passer pour l'utilisateur prévu en utilisant des informations accessibles au public et des informations auxquelles elle avait accès par ailleurs.

127. L'utilisation de ce type d'authentification statique basée sur la connaissance (où la réponse ne change pas, et où l'information n'est pas "secrète" comme ce serait le cas avec un mot de passe) n'est pas recommandée.

128. Au lieu de cela, l'organisation devrait utiliser une forme d'authentification qui permettrait d'obtenir un degré élevé de confiance dans le fait que l'utilisateur authentifié est la personne visée, et non quelqu'un d'autre. L'introduction d'une méthode d'authentification multifactorielle hors bande permettrait de résoudre le problème, par exemple pour vérifier la demande de changement, en envoyant une demande de confirmation à l'ancien contact ; ou en ajoutant des questions supplémentaires et en exigeant des informations uniquement visibles sur les factures précédentes. Il incombe au responsable du traitement 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 en fonction des risques identifiés

Documentation interne	Notification à l'AS	Communication aux personnes concernées

[33] Pour des orientations sur les opérations de traitement "*susceptibles d'entraîner un risque élevé*", voir la note de bas de page 10 ci-dessus.

7.2 CAS n° 18 : Exfiltration d'emails

Une chaîne d'hypermarchés a détecté, trois mois après sa configuration, que certains comptes de messagerie avaient été modifiés et que des règles avaient été créées pour que chaque courriel contenant certaines expressions (par exemple "facture", "paiement", "virement bancaire", "authentification de carte de crédit", "coordonnées bancaires") soit déplacé vers un dossier inutilisé et également transféré vers une adresse électronique externe. De plus, à ce moment-là, une attaque par ingénierie sociale avait déjà été réalisée, c'est-à-dire que l'attaquant, se faisant passer pour un fournisseur, avait modifié les coordonnées bancaires de ce fournisseur pour les remplacer par les siennes. Enfin, à ce moment-là, plusieurs fausses factures avaient été envoyées avec les nouvelles coordonnées bancaires. Le système de surveillance de la plate-forme de messagerie a fini par donner une alerte concernant les dossiers. L'entreprise n'a pas été en mesure de détecter comment l'attaquant a pu accéder aux comptes de messagerie, mais elle suppose qu'un courriel infecté est à l'origine de l'accès au groupe d'utilisateurs en charge des paiements.

En raison de la transmission d'e-mails basée sur des mots-clés, l'attaquant a reçu des informations sur 99 employés : nom et salaire d'un mois particulier concernant 89 personnes concernées ; nom, état civil, nombre d'enfants, salaire, heures de travail et informations résiduelles sur la perception du salaire de 10 employés dont le contrat a pris fin. Le responsable du traitement n'a notifié que les 10 employés appartenant à ce dernier groupe.

7.2.1 CAS n° 18 - Évaluation et atténuation des risques et obligations

129. Même si l'attaquant ne visait probablement pas à collecter des données à caractère personnel, étant donné que la violation pourrait entraîner des dommages matériels (par exemple, une perte financière) et immatériels (par exemple, une usurpation d'identité ou une fraude), ou que les données pourraient être utilisées pour faciliter d'autres attaques (par exemple, le hameçonnage), la violation des données à caractère personnel est susceptible d'entraîner un risque élevé pour les droits et libertés des personnes physiques. Par conséquent, la violation doit être communiquée à l'ensemble des 99 employés et pas seulement aux 10 employés dont les informations salariales 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 d'e-mails au compte de messagerie de l'attaquant, a notifié au fournisseur de services l'e-mail utilisé par l'attaquant concernant ses actions, a supprimé les règles définies par l'attaquant et a affiné les alertes du système de surveillance afin de donner une alerte dès qu'une règle automatique est créée. Le responsable du traitement pourrait également retirer aux utilisateurs le droit de définir des règles de transfert et demander à l'équipe de services informatiques de ne le faire que sur demande. Il pourrait aussi instaurer une politique selon laquelle les utilisateurs devraient vérifier les règles définies sur leurs comptes et en rendre compte une fois par semaine, voire plus souvent dans les domaines traitant des données financières.

131. Le fait qu'une violation ait pu se produire et passer inaperçue pendant si longtemps et le fait que, dans un délai plus long, l'ingénierie sociale aurait pu être utilisée pour modifier davantage de données, ont mis en évidence des problèmes importants dans le système de sécurité informatique du contrôleur. Il convient de s'y attaquer sans tarder, notamment en mettant l'accent sur les examens d'automatisation et les contrôles des changements, ainsi que sur les mesures de détection et de réponse aux incidents. Les contrôleurs qui traitent des données sensibles, des informations financières, etc. ont une plus grande responsabilité en termes de sécurité des données.

Actions nécessaires en fonction des risques

identifiés		
Documentation interne	Notification à l'AS	Communication aux personnes concernées