GROUPE DE TRAVAIL «ARTICLE 29» SUR LA PROTECTION DES DONNÉES

693/14/FR
WP 213

Avis 03/2014 sur la notification des violations de données à caractère personnel

Adopté le 25 mars 2014

Résumé

Dans le présent avis, le groupe de travail «Article 29» fournit des orientations aux responsables du traitement afin de les aider à décider s'il convient de notifier aux personnes concernées les éventuelles «violations de données à caractère personnel». Bien que le présent avis porte sur l'obligation actuellement imposée aux fournisseurs de communications électroniques au titre de la directive 2002/58/CE, il contient des exemples issus de nombreux secteurs, dans le contexte du projet de règlement sur la protection des données, et présente une série de bonnes pratiques à l'intention de tous les responsables du traitement.

La directive 2002/58/CE exige qu'une notification soit adressée à l'autorité compétente pour tous les cas de violation de données, mais le présent avis analyse les violations de données à caractère personnel qui nécessitent une notification aux personnes concernées et décrit ce que les responsables du traitement auraient pu faire lors de la mise en œuvre de leur système afin d'éviter la violation de données à caractère personnel en premier lieu, ou au moins les mesures qui auraient pu être prises au départ pour que le responsable du traitement ne soit pas tenu de notifier les personnes concernées.

L'avis répond également à certaines questions essentielles relatives aux violations de données à caractère personnel et à l'application de la directive 2002/58/CE.

1. Introduction

Au sens de l'article 2, point i), de la directive 2002/58/CE, on entend par violation de données à caractère personnel «une violation de la sécurité entraînant accidentellement ou de manière illicite la destruction, la perte, l'altération, la divulgation ou l'accès non autorisés de données à caractère personnel transmises, stockées ou traitées d'une autre manière en relation avec la fourniture de services de communications électroniques accessibles au public dans la Communauté».

La directive 2002/58/CE (et la proposition de règlement européen sur la protection des données) exige la notification des violations de données à caractère personnel à l'autorité nationale compétente. Les détails des informations à fournir dans cette notification sont disponibles à l'annexe I du règlement (UE) nº 611/2013.

Quand la violation de données à caractère personnel est susceptible de porter atteinte aux données à caractère personnel ou à la vie privée d'une personne concernée[1], le responsable du traitement des données notifie également la violation à la personne concernée sans retard injustifié[2].

La directive 2002/58/CE, de même que le règlement (UE) nº 611/2013, prévoient une exemption de l'exigence de notification aux personnes concernées si les données ont été rendues incompréhensibles. Si le fournisseur a prouvé, à la satisfaction de l'autorité compétente, qu'il a mis en œuvre les mesures de protection technologiques appropriées pour rendre les données incompréhensibles à toute personne qui n'est pas autorisée à y avoir accès[3], et que ces mesures ont été appliquées aux données concernées par ladite violation de sécurité, la notification d'une violation de données à caractère personnel à la personne concernée n'est pas nécessaire[4].

La raison d'être de cette exemption de notification aux particuliers est que les mesures appropriées peuvent réduire à un niveau négligeable les risques résiduels pour la vie privée des personnes concernées. Une violation de la confidentialité de données à caractère personnel qui ont été cryptées à l'aide d'un algorithme de pointe constitue tout de même une violation de données à caractère personnel, et celle-ci doit être notifiée à l'autorité. Néanmoins, si la confidentialité de la clé de cryptage est intacte, les données sont en principe incompréhensibles à toute personne qui n'est pas autorisée à y avoir accès, et la violation n'est donc pas susceptible de porter atteinte à la personne concernée et ne nécessite dès lors pas de lui être notifiée.

[1] Dans le présent avis, l'expression «personne concernée» est employée au sens de la directive 95/46/CE. Dans le contexte de la directive 2002/58/CE, elle correspond à «abonné ou particulier».

[2] La directive 2002/58/CE et le règlement (UE) nº 611/2013 disposent que la notification à l'autorité doit être effectuée au plus tard vingt-quatre heures après le constat de la violation de données à caractère personnel, si possible, avec possibilité de porter ce délai à trois jours dans certains cas. La notification à l'abonné ou au particulier doit se faire sans retard injustifié (au sens de l'article 2, paragraphe 2, du règlement (UE) nº 611/2013) après le constat de la violation de données à caractère personnel. La notification à la personne concernée est indépendante de la notification à l'autorité nationale compétente.

[3] Article 4, paragraphe 3, de la directive 2002/58/CE; article 4, paragraphe 1, du règlement (UE) nº 611/2013; article 32, paragraphe 3, du règlement général sur la protection des données, version consolidée non officielle après le vote en commission LIBE, fournie par le rapporteur.

[4] Il convient de noter que, si la clé est compromise ultérieurement, toutes les violations antérieures qui n'ont pas été notifiées au motif que la confidentialité de la clé était intacte devront alors être notifiées.

Toutefois, même si les données sont cryptées, une perte ou une altération peuvent avoir des conséquences négatives pour les personnes concernées quand le responsable du traitement des données ne dispose pas de sauvegardes adéquates. Dans ce cas, la notification aux personnes concernées devrait quand même être imposée, même si des mesures de protection par cryptage sont appliquées.

Par conséquent, il importe que les responsables du traitement soient proactifs et prennent les mesures préalables nécessaires. L'article 17 de la directive 95/46/CE, de même que l'article 4, paragraphe 1, et l'article 4, paragraphe 1 *bis*, de la directive 2002/58/CE, prévoient que les responsables du traitement doivent mettre en œuvre les mesures techniques et d'organisation appropriées afin d'«assurer un niveau de sécurité approprié au regard des risques» présentés par le traitement. À cette fin, il convient de disposer d'un cadre approprié de gestion des risques, qui présente les éléments minimaux devant caractériser une telle approche et qui fournisse également une série de commandes techniques et d'organisation appropriées, que le responsable du traitement peut définir, en se concentrant plus particulièrement sur les commandes qui rendent les données incompréhensibles si nécessaire. Les entreprises doivent également définir au préalable des mesures appropriées visant à faire face aux violations de données à caractère personnel et à garantir une réaction rapide et efficace dans de tels cas.

Si les dispositions de l'article 17 ont été dûment respectées, les mesures nécessaires ont été prises avant le traitement des données et les risques liés à une violation de données à caractère personnel auront été pris en considération et réduits au préalable. Dans ces conditions, les risques de violation de données à caractère personnel sont plus rares et les conséquences pour les personnes concernées sont susceptibles d'être moindres. Étant donné que la notification aux personnes concernées n'est pas requise quand la violation ne porte pas atteinte à leurs données à caractère personnel ou à leur vie privée, ou quand des mesures de protection technologique appropriées ont été appliquées aux données concernées par la violation, la meilleure manière d'éviter de devoir avertir les personnes concernées consiste à intégrer des garanties appropriées de la vie privée dans les projets où des données à caractère personnel sont traitées.

Les notifications aux personnes concernées devraient être effectuées sans retard injustifié[5] et elles sont indépendantes des notifications de violations de données à caractère personnel à l'autorité nationale compétente. Le responsable du traitement des données devrait garder à l'esprit que l'un des principaux avantages de la notification, qui ne constitue pas pour autant un critère déterminant en ce qui concerne la nécessité d'avertir les personnes concernées, consiste à fournir à ces dernières les informations nécessaires pour limiter les conséquences négatives découlant des circonstances de la violation. Lorsque le responsable du traitement a un doute sur l'existence d'éventuelles conséquences négatives pour les données à caractère personnel ou la vie privée des personnes concernées, il devrait, par mesure de précaution, effectuer la notification. En outre, il convient de tenir compte de la possibilité qu'ont les autorités compétentes de demander la notification aux particuliers après examen complémentaire de la notification.

[5] La directive 2002/58/CE et le règlement (UE) nº 611/2013 disposent que la notification à l'autorité doit être effectuée au plus tard vingt-quatre heures après le constat de la violation de données à caractère personnel, si possible, avec possibilité porter ce délai à trois jours dans certains cas. La notification à l'abonné ou au particulier doit se faire sans retard injustifié après le constat de la violation de données à caractère personnel.

Le présent avis propose une **liste non exhaustive de cas dans lesquels les personnes concernées devraient être averties**[6]. Nous examinons chaque violation de données à caractère personnel au regard des trois critères de sécurité classiques: l'expression «violation de la disponibilité» correspondra donc à la destruction ou à la perte, accidentelles ou illicites, de données à caractère personnel, «violation de l'intégrité» correspondra à l'altération de données à caractère personnel, et «violation de la confidentialité» correspondra à la divulgation ou à l'accès non autorisés de données à caractère personnel. Dans ce cadre, l'avis fournit des **orientations générales** pour les cas qui ne nécessitent pas de notification. Enfin, il **évoque les principales questions** que les responsables du traitement peuvent se poser lorsqu'ils déterminent s'il convient ou non d'avertir les personnes concernées.

[6] Étant donné que la proposition de règlement sur la protection des données prévoit une généralisation de l'obligation de notification à tous les secteurs et que plusieurs États membres ont déjà mis en place une obligation de notification légale, les exemples cités dans le présent avis ne se limitent pas au secteur des communications électroniques.

2. Violations qui peuvent avoir des conséquences négatives pour les personnes concernées

Les violations doivent être notifiées sans retard injustifié aux personnes concernées quand elles sont de nature à porter atteinte aux données à caractère personnel ou à la vie privée. La présente section contient des exemples de violations qui répondent à ces critères. Elle donne également des exemples de mesures techniques qui, si elles avaient été prises avant l'incident, auraient permis d'éviter la notification aux personnes concernées.

Cas 1. *Quatre ordinateurs portables ont été volés dans un établissement de soins pour enfants; ils contenaient des données sensibles en matière de santé et de sécurité sociale, ainsi que d'autres données à caractère personnel concernant 2 050 enfants.*

Cette violation de données à caractère personnel concerne la confidentialité ainsi que (si le responsable du traitement ne disposait d'aucune sauvegarde des données) la disponibilité et l'intégrité des données.

Conséquences et effets néfastes potentiels de la violation de la confidentialité

- La première conséquence est une violation du secret médical: la base de données contient des informations médicales à caractère personnel sur les enfants, auxquelles peuvent avoir accès des personnes qui n'y ont pas été autorisées.
- La publication de ces données peut avoir des retombées sur l'environnement scolaire ou familial de l'enfant (des données sur une agression, des maladies de longue durée, des troubles mentaux, les difficultés financières ou sociales de la famille, etc.).
- Elle peut affecter émotionnellement les enfants et les parents.
- Ces données peuvent être utilisées pour faire chanter les parents ou les enfants (en fonction de leur âge).
- Les parents d'enfants gravement malades peuvent être la cible de personnes qui veulent profiter de leur faiblesse (charlatans, sectes, etc.).

Conséquences et effets néfastes potentiels de la violation de la disponibilité

- Elle peut troubler la continuité du traitement des enfants, entraînant l'aggravation de la maladie ou une rechute.
- Elle peut entraîner un empoisonnement accidentel en raison d'une allergie à un médicament ou de médicaments incompatibles, ce qui peut causer plusieurs problèmes de santé, voire le décès.
- Elle peut entraîner un retard excessif dans les remboursements ou l'assistance financière accordés aux personnes concernées, ce qui aurait des retombées financières pour les familles concernées.

Conséquences et effets néfastes potentiels de la violation de l'intégrité

- Les données perdues peuvent affecter l'intégrité des dossiers médicaux et perturber le déroulement du traitement des enfants. À titre d'exemple, s'il n'existe qu'une ancienne sauvegarde des dossiers médicaux, toutes les modifications apportées aux données sur les ordinateurs volés seront perdues, entraînant la corruption de l'intégrité des données. L'utilisation de dossiers médicaux qui ne sont pas à jour peut nuire à la continuité du traitement des enfants, entraînant l'aggravation de la maladie ou une rechute.

Dans un tel cas, en raison des effets néfastes potentiels, une notification devrait être effectuée, mais il importe également de tenir compte de l'âge et de la maturité des personnes concernées. Il peut être nécessaire, en l'espèce, d'avertir un parent ou un tuteur légal qui sera prêt à jouer un rôle actif dans les soins médicaux de l'enfant, en plus de la notification aux enfants eux-mêmes, si nécessaire ou requis par la loi en vigueur.

Ainsi, les parents avertis seront en mesure de signaler une anomalie dans la continuité du traitement, de tester les allergies connues par l'établissement ou de demander de nouveaux examens médicaux afin de garantir que leurs enfants recevront le traitement adéquat. Ils peuvent également choisir d'informer directement d'autres personnes de l'état des enfants afin de contrôler certaines des conséquences sur l'environnement de ces derniers.

Exemples de garanties appropriées qui auraient pu permettre de réduire les risques si elles avaient été mises en œuvre au préalable

- La violation de la disponibilité et de l'intégrité aurait pu être évitée, ou bien ses conséquences et effets néfastes auraient pu être atténués si une sauvegarde à jour et suffisamment sécurisée avait été disponible.

- Les conséquences et effets néfastes potentiels de la violation de la confidentialité auraient pu être atténués si les données avaient été protégées à l'aide d'un produit de cryptage approprié, doté d'une clé secrète suffisamment résistante.

Si ces garanties avaient été mises en place et étaient demeurées sûres (à savoir, si la clé était restée secrète et si la sauvegarde était restée disponible), la notification aux personnes concernées n'aurait en principe pas été nécessaire. Cela devrait être démontré à la satisfaction de l'autorité compétente.

Cas 2. *L'exploitation d'une vulnérabilité dans une application web a permis la consultation non autorisée de données à caractère personnel liées aux clients d'un courtier en assurance-vie. Les dossiers des personnes concernées contenaient leur nom et leur adresse ainsi que des questionnaires médicaux complétés. Sept cents personnes sont concernées.*

Conséquences et effets néfastes potentiels de la violation de la confidentialité

- Les données publiées sur l'internet par l'attaquant peuvent avoir des conséquences sur la capacité des personnes concernées à trouver un emploi (par exemple, les réponses à des questions sur des problèmes de santé, une grossesse, etc.).
- Elle peut affecter l'environnement de travail ou familial des personnes concernées.

- Elle peut également avoir des retombées émotionnelles si les personnes concernées dissimulent leur état après diagnostic.
- Elle peut conduire à un vol d'identité.
- Les données (comme le fait d'être client ou de payer pour certains services) peuvent être utilisées à des fins d'hameçonnage.

Étant donné que cet incident est susceptible de porter atteinte aux personnes concernées, la violation devrait leur être notifiée.

Exemples de garanties appropriées qui auraient pu permettre de réduire les risques si elles avaient été mises en œuvre au préalable

- Un contrôle permanent des vulnérabilités potentielles des technologies utilisées, incluant au moins une analyse régulière des vulnérabilités du site web et une mise à jour des logiciels (y compris des logiciels de sécurité), aurait permis soit d'éviter la violation soit de réduire son incidence.

  Même si les attaques jour zéro exploitant des vulnérabilités de sécurité sont difficiles à éviter, des stratégies adéquates et efficaces permettant d'empêcher de manière proactive l'exploitation des vulnérabilités de sécurité, notamment un examen du code, peuvent réduire la marge de risque à un niveau acceptable. En outre, une bonne politique de gestion des incidents de sécurité peut également réduire les conséquences d'une violation en limitant l'ampleur et la durée de ses effets négatifs.

- Comme dans le cas précédent, les conséquences et effets néfastes potentiels de la violation de la confidentialité auraient pu être atténués si les données avaient été protégées à l'aide d'un produit de cryptage approprié, doté d'une clé secrète suffisamment résistante. Cette méthode peut se révéler particulièrement efficace pour la protection contre le vol du disque ou des circonstances similaires.

- Enfin, différentes technologies d'amélioration de la confidentialité auraient pu être utilisées par la compagnie d'assurances, afin de réduire au minimum les données ou les possibilités d'identifier les personnes concernées. À titre d'exemple, la compagnie aurait pu envoyer un numéro d'identification aléatoire par la poste pour permettre à ses clients de remplir le questionnaire médical en ligne. Cette technique permet d'éviter les questions concernant le nom, l'adresse, la date de naissance ou le numéro de téléphone dans le questionnaire en ligne.

Cas 3. *Un employé d'un fournisseur de services internet a donné à un tiers l'identifiant et le mot de passe d'un compte disposant de droits d'accès globaux à la base de données Clients. Le tiers peut, en utilisant ce compte, accéder à toutes les informations sur les clients sans aucune restriction. La base de données contient le nom, l'adresse, l'adresse électronique, les numéros de téléphone, les données d'accès et d'autres données permettant l'identification (nom de l'utilisateur, mots de passe hachés, identifiant des clients), ainsi que des données de paiement (numéro de compte, informations relatives à la carte de crédit, etc.). Même si les données de paiement étaient cryptées à l'aide d'un algorithme de pointe, le compte maître compromis était autorisé à y accéder, et donc le tiers y a également eu accès. La société possède plus de 100 000 clients.*

Conséquences et effets néfastes potentiels de la violation de la confidentialité

- L'utilisation abusive des données de paiement (en particulier des informations relatives aux cartes de crédit) aurait des conséquences financières pour les clients.
- Étant donné que les mots de passe étaient simplement hachés, le tiers peut facilement déduire le texte en clair correspondant. L'accès au compte d'un client donné serait possible même après la fermeture du compte faisant l'objet de la violation.
- Le tiers pourrait facilement utiliser l'adresse électronique et le mot de passe de certaines des personnes concernées pour accéder aux comptes correspondant à d'autres services en ligne, car beaucoup de personnes utilisent le même mot de passe pour plusieurs services en ligne différents.

Conséquences et effets néfastes potentiels de la violation de l'intégrité

- Le tiers a bénéficié d'un accès total à la base de données; il est possible qu'il ait modifié, effacé ou ajouté certaines données du compte.
    - Si le courrier électronique ou l'hébergement web faisaient partie des services fournis par le fournisseur de services internet, le tiers aurait pu consulter, modifier ou effacer ce contenu, modifier la configuration DNS ou clôturer le compte de la personne concernée.

Bien que les données financières aient été cryptées, le tiers a eu accès aux données décryptées grâce à l'interface utilisateur, et l'exemption de notification ne s'applique donc pas.

Si les fichiers de journalisation sécurisés sont fiables (c'est-à-dire s'ils ne sont pas compromis) et qu'ils indiquent que le compte n'a pas accédé à la base de données Clients, la notification à la personne concernée ne devrait alors pas être obligatoire.

Dans toute autre éventualité, étant donné que cet incident est susceptible de porter atteinte à la personne concernée et que l'exemption ne s'applique pas, la violation devrait être notifiée aux clients concernés.

Dès lors que des mots de passe sont compromis, le responsable du traitement devrait obliger les personnes concernées à créer un nouveau mot de passe, en mode sécurisé, afin de garantir que tous les nouveaux mots de passe soient utilisés par des utilisateurs légitimes, et non par des tiers qui ont obtenu les données d'identification. Dans la pratique, cela peut correspondre à la procédure sécurisée de renouvellement d'un mot de passe perdu et des informations justifiant le renouvellement du mot de passe devraient être incluses. Dans la notification adressée à l'utilisateur, il convient également de recommander à ce dernier de ne pas réutiliser l'ancien mot de passe ou un mot de passe similaire et de changer les mots de passe compromis pour tous les comptes où le même mot de passe était utilisé.

Exemples de garanties appropriées qui auraient pu permettre de réduire les risques si elles avaient été mises en œuvre au préalable

- Il convient d'attribuer à chaque personne son propre compte et l'accès aux données à caractère personnel devrait être exclusivement autorisé en appliquant les principes du besoin d'en connaître et de moindre privilège. Cela s'applique également aux vendeurs, au personnel d'entretien de sociétés tierces et à d'autres personnes qui ont besoin d'un accès temporaire à la base de données: ces personnes devraient uniquement avoir accès à la fonctionnalité ou aux données dont elles ont besoin aux fins de l'exécution des tâches qui leur sont dévolues, pour une durée qui se limite à ce qui est strictement nécessaire. L'utilisation des comptes disposant d'un «accès global» à la base de données devrait être limitée et des méthodes de traçage et de restriction de l'utilisation de ce type de comptes devraient être appliquées. La mise en place de ce type de garanties aurait permis soit d'éviter la violation soit d'en limiter l'incidence.
- Si les mots de passe avaient été stockés de manière sécurisée (par exemple, par salage ou à l'aide d'une fonction de hachage à clé cryptographique), les préjudices secondaires pour les particuliers auraient été fortement réduits. Cependant, il est possible que les particuliers choisissant des mots de passe à faible niveau de sécurité courent toujours un risque, notamment lorsqu'ils utilisent ces mêmes données d'accès pour plusieurs services en ligne. Ce risque aurait pu être atténué en suggérant à ces utilisateurs de choisir un mot de passe plus solide.

Cas 4. *Une enveloppe contenant des bordereaux de carte de crédit a été jetée par erreur dans une poubelle au lieu d'être détruite de manière sécurisée. La poubelle a été vidée dans une plus grande poubelle, située en dehors des locaux, en vue de la collecte des déchets. Un individu a sorti l'enveloppe de la deuxième poubelle et a ensuite distribué les bordereaux de carte de crédit dans un lotissement des environs. Les données comprenaient la totalité des informations relatives aux cartes[7] et le nom des titulaires. Dans certains cas, la signature du titulaire était également disponible. 800 personnes concernées ont été affectées.*

Conséquences et effets néfastes potentiels de la violation de la confidentialité

- La violation pourrait avoir des conséquences financières pour les personnes concernées si les informations relatives à leur carte sont toujours valables et font l'objet d'une utilisation abusive[8].

Étant donné que cet incident est susceptible de porter atteinte aux personnes concernées, la violation devrait leur être notifiée. Dans ce cas, si aucun autre enregistrement n'a été conservé, il peut sembler difficile d'avertir individuellement chaque personne concernée, car il est possible que l'on ne sache pas quels bordereaux de carte de crédit se trouvaient spécifiquement dans l'enveloppe. Le magasin devrait alerter le gestionnaire des transactions de paiement par carte afin qu'il puisse détecter d'éventuelles opérations frauduleuses. Une autre orientation pratique proposée dans le règlement (UE) nº 611/2013[9] prévoit que, si le fournisseur, «malgré les efforts raisonnables déployés, n'est pas en mesure d'identifier dans le

[7] Même si la bonne pratique consiste à procéder à une troncature des données des cartes de paiement sur le reçu imprimé du client, cette fonctionnalité n'est pas disponible sur tous les terminaux de point de vente et les données peuvent être imprimées dans leur totalité sur les copies des reçus du commerçant.

[8] Étant donné qu'il est toujours possible d'utiliser les informations de la carte de crédit sans le code de sécurité CVV (ou équivalents), même des violations qui ne concernent pas les CVV doivent être notifiées.

[9] Bien que ce règlement ne s'applique pas dans ce contexte.

délai fixé au paragraphe 3 toutes les personnes susceptibles d'être lésées par la violation de données à caractère personnel, il peut, dans le même délai, informer ces personnes par des avis dans de grands médias nationaux ou régionaux dans les États membres concernés». Par conséquent, dans le cas d'un magasin disposant d'une base de clientèle principalement locale, une notification dans un journal régional peut être considérée comme suffisante. En outre, il pourrait être utile d'avertir les sociétés de carte de crédit de la violation afin qu'elles protègent leurs clients.

Si l'enveloppe avait été retrouvée dans l'une des poubelles par le responsable du traitement et que l'enveloppe ou autre était restée fermée, il est peu probable que la violation ait porté préjudice aux abonnés; dès lors, elle n'avait pas à être notifiée aux personnes concernées.

Exemples de garanties appropriées qui auraient pu permettre de réduire les risques si elles avaient été mises en œuvre au préalable

- Informer les employés des conséquences potentielles de ces violations, et utiliser un destructeur[10] de documents de bureau approprié ou un service de destruction d'archives pour détruire les bordereaux de carte de crédit (et tous documents similaires en papier contenant des données à caractère personnel) avant de les jeter réduiraient grandement le risque de telles violations.
- Il convient également d'utiliser un terminal de point de vente (TPV) qui ne fait pas apparaître la totalité des informations liées aux cartes de crédit.

Cas 5. *L'ordinateur portable crypté d'un conseiller financier a été volé dans le coffre d'une voiture. Toutes les informations figurant dans les analyses financières – par exemple, les hypothèques, les salaires, les demandes de prêt – relatives à 1 000 personnes ont été affectées. La clé de cryptage, la phrase de sécurité, n'est pas compromise, mais aucune sauvegarde n'est disponible.*

Conséquences et effets néfastes potentiels de la violation de la confidentialité

- En fonction de la nature exacte des données qui ont été violées, une utilisation abusive des données peut avoir différentes retombées pour les personnes concernées. Toutefois, étant donné que l'ensemble du disque de l'ordinateur portable bénéficiait d'un cryptage (de pointe) fondé sur une phrase de sécurité forte qui n'a pas été compromise, aucune divulgation non autorisée n'est survenue.

Conséquences et effets néfastes potentiels

- L'indisponibilité des données implique que les personnes concernées devront communiquer une nouvelle fois les informations nécessaires. Cette situation induit un léger préjudice pour les personnes concernées, sous la forme d'une perte de temps et de désagréments.

[10] Par exemple, un destructeur de classe 2 au niveau P-4 ou supérieur dans la classification DIN 66399 pour les documents en papier.

- Dans certains cas, elle peut également entraîner le non-respect de délais de soumission ou de candidature, ce qui peut avoir plusieurs conséquences secondaires pour les personnes concernées en fonction du contexte: amende, perte de revenu ou de bénéfices anticipés, occasion manquée, résiliation d'un contrat d'achat, etc.

Étant donné que les données ont été perdues et que les effets de la violation de la disponibilité n'ont pas été atténués, la violation des données à caractère personnel est susceptible de porter préjudice aux personnes concernées. Par conséquent, la violation devrait être notifiée aux personnes concernées. La notification expliquera que des informations devront être communiquées à nouveau au conseiller financier, mais elle préviendra également les personnes concernées des éventuelles conséquences et préjudices divers qu'elles pourraient subir en raison de la violation.

Exemple de garanties appropriées qui auraient pu permettre de réduire les risques si elles avaient été mises en œuvre au préalable

- Une solution de sauvegarde efficace et sécurisée aurait permis de restaurer les données. Si une sauvegarde à jour des données avait été disponible, aucune violation de la disponibilité ne serait survenue et la notification n'aurait pas été nécessaire.

Cas 6. *Un opérateur de réseau de téléphonie mobile fournit à ses abonnés une interface en ligne leur permettant, en s'identifiant, de se connecter à leur compte et de consulter les dernières factures et les activités récentes sur leur compte. Un accès illicite à la base de données où sont stockés les mots de passe du site web a été découvert. Le tiers a eu accès aux données d'authentification des utilisateurs (nom d'utilisateur et mots de passe hachés en MD5 sans salage).*

Conséquences et effets néfastes potentiels de la violation de la confidentialité

- Le tiers peut déduire le mot de passe et donc accéder au compte de tous les clients puisqu'il possède également les noms d'utilisateur.
- Étant donné que de nombreuses personnes utilisent la même combinaison de nom d'utilisateur et de mot de passe pour beaucoup de comptes en ligne, le tiers est susceptible d'être en mesure d'accéder à d'autres comptes de certaines des personnes concernées, y compris, dans certains cas, à des comptes de messagerie électronique.

Étant donné que les mots de passe étaient simplement hachés, ils ne peuvent pas être considérés comme incompréhensibles au sens de l'article 4, paragraphe 2, du règlement (UE) nº 611/2013[11] de la Commission. Par conséquent, l'exemption de notification aux personnes concernées ne s'applique pas.

[11] L'article 4, paragraphe 2, dispose que:
Les données sont considérées comme incompréhensibles si:

Comme ce cas est susceptible de porter préjudice aux personnes concernées et que l'exemption ne s'applique pas, il faut notifier la violation aux clients concernés, en leur recommandant clairement de changer le mot de passe de tous les comptes qui utilisent le même mot de passe compromis. En tout état de cause, tous les utilisateurs devraient être forcés de changer leur mot de passe, en utilisant une méthode sécurisée, lorsqu'ils tentent d'accéder au service.

Exemple de garanties appropriées qui auraient pu permettre de réduire les risques si elles avaient été mises en œuvre au préalable

- Si les mots de passe avaient été stockés de manière sécurisée (hachés avec une clé cryptographique salée, avec une fonction de hachage de pointe et une clé ou un salage), les préjudices pour les particuliers auraient alors été grandement réduits. Cependant, il est possible que les particuliers choisissant des mots de passe à faible niveau de sécurité courent toujours un risque, notamment lorsqu'ils utilisent ces mêmes données d'accès pour plusieurs services en ligne.

Cas 7. *Un fournisseur de services internet propose une interface permettant aux abonnés de consulter les informations liées à leur compte, l'historique de leur utilisation de l'internet, y compris le volume mensuel et les domaines fréquemment visités. En raison d'une erreur dans le code du site web, les identifiants d'accès de l'utilisateur ne sont plus validés et les données sont accessibles en falsifiant la valeur d'identification soumise dans les paramètres de l'URL. Il est possible d'avoir accès aux informations liées aux comptes de tous les clients en parcourant la liste des numéros d'identification des abonnés.*

Conséquences et effets néfastes potentiels de la violation de la confidentialité

- Les données peuvent être utilisées pour envoyer des messages indésirables aux personnes concernées, par courriel ou par téléphone.
- Il est possible que les données permettent de dresser un profil de l'abonné et révèlent des détails sur son comportement qui pourraient entraîner la divulgation d'informations sensibles. La violation peut affecter l'environnement de travail ou familial des personnes concernées.

Elle est susceptible de porter préjudice au particulier et devrait par conséquent être notifiée aux clients.

Exemple de garanties appropriées qui auraient pu permettre de réduire les risques si elles avaient été mises en œuvre au préalable:

a) elles ont été cryptées en mode sécurisé à l'aide d'un algorithme normalisé et la clé utilisée pour les décrypter n'a été compromise dans aucune violation de sécurité et a été générée de façon à ne pouvoir être trouvée, par aucun moyen technologique existant, par quelqu'un qui n'est pas autorisé à l'utiliser; ou

b) elles ont été remplacées par leur valeur hachée, calculée à l'aide d'une fonction de hachage normalisée à clé cryptographique, et la clé utilisée pour les hacher n'a été compromise dans aucune violation de sécurité et a été générée de façon à ne pouvoir être trouvée, par aucun moyen technologique existant, par quelqu'un qui n'est pas autorisé à l'utiliser.

- Le contrôle des éventuelles vulnérabilités des technologies utilisées, tel que décrit dans le cas 2, ainsi que des tests sur une plate-forme de préproduction avant le déploiement et un examen du code auraient pu permettre d'éviter la violation.

3. Scénarios possibles dans lesquels la notification aux personnes concernées n’est pas nécessaire

Même s’il convient d’évaluer au cas par cas les conséquences d’une violation de données à caractère personnel, afin de prendre dûment en considération tous les éléments dans l’analyse des effets néfastes probables pour les particuliers, en guise d’orientation générale et pour compléter les exemptions décrites dans la section précédente, le responsable du traitement peut également considérer que la notification aux personnes concernées n’est pas nécessaire dans certains cas spécifiques.

Il peut s’agir des cas suivants:

- Une violation de données à caractère personnel qui ne porte que sur la confidentialité, lorsque des données ont été cryptées en mode sécurisé à l’aide d’un algorithme de pointe, et que la clé utilisée pour les décrypter n’a été compromise dans aucune violation de sécurité et a été générée de façon à ne pouvoir être trouvée, par aucun moyen technologique existant, par quelqu’un qui n’est pas autorisé à l’utiliser. En effet, de telles mesures rendent les données incompréhensibles à toute personne qui n’est pas autorisée à y avoir accès.

- Les données, tels les mots de passe, ont été hachées et salées en mode sécurisé. La valeur hachée a été calculée à l’aide d’une fonction de hachage à clé cryptographique de pointe, la clé utilisée pour hacher les données n’a été compromise dans aucune violation de sécurité et a été générée de façon à ne pouvoir être trouvée, par aucun moyen technologique existant, par quelqu’un qui n’est pas autorisé à l’utiliser.

4. Questions/réponses

Dans quels cas la notification aux particuliers n'est-elle pas nécessaire?

- Quand la violation de sécurité ne constitue pas une violation de données à caractère personnel (voir question suivante).
- Quand la violation de données à caractère personnel n'est pas susceptible de porter atteinte aux données à caractère personnel ou à la vie privée de la personne concernée selon les résultats d'une évaluation de la gravité, à la satisfaction de l'autorité compétente.
- Quand le fournisseur a démontré, à la satisfaction de l'autorité compétente, qu'il a mis en œuvre des mesures de protection technologique appropriées et que ces mesures ont été appliquées aux données concernées par la violation de sécurité. À titre d'exemple, si une violation de données à caractère personnel (qui ne porte que sur la confidentialité) concerne uniquement soit des données cryptées à l'aide d'un algorithme de pointe, soit des données hachées salées/cryptées avec une clé à l'aide d'une fonction de hachage de pointe, et que toutes les clés et tous les sels secrets concernés ne sont pas compromis.
- La notification des violations de données, telle que décrite dans le présent avis, constitue une bonne pratique pour tous les responsables du traitement des données, même si la notification n'est pas obligatoire.

Quand une violation de sécurité devient-elle une violation de données à caractère personnel?

Une violation de sécurité constitue une violation de données à caractère personnel quand les données violées sont des données à caractère personnel, telles que définies à l'article 2, point a), de la directive 95/46/CE: *on entend par «données personnelles»: toute information concernant une personne physique identifiée ou identifiable (personne concernée); est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale.*

L'avis 4/2007 explique qu'il s'agit de données liées à une personne: «une personne peut être identifiée soit directement par un nom soit indirectement par un numéro de téléphone, de voiture, de sécurité sociale, de passeport ou par un croisement de critères significatifs, permettant de la reconnaître à l'intérieur d'un petit groupe par exemple (âge, fonction occupée, adresse, etc.)». L'avis 4/2007 fournit des orientations supplémentaires sur ce point.

Doit-on prendre en considération les conséquences secondaires probables?

Oui, les violations de données devraient être notifiées aux personnes concernées si la violation est susceptible de porter atteinte aux données à caractère personnel ou à la vie privée des personnes concernées.
Dès lors, l'ensemble des conséquences et effets néfastes potentiels pour les personnes concernées devraient être pris en considération.

Exemple 1: *Le site web d'une entreprise de divertissement musical est piraté et la base de données des utilisateurs est volée et publiée sur l'internet. Les données à caractère personnel divulguées contiennent les noms/prénoms, les préférences musicales ainsi que les noms d'utilisateur et mots de passe des utilisateurs enregistrés sur le site web de l'entreprise. Neuf mille utilisateurs sont concernés.*

Dans le cas de cette violation, le préjudice direct pour les particuliers peut sembler relativement limité dans la plupart des cas (à savoir la divulgation d'informations sur les préférences musicales) et l'on peut se demander s'il convient d'avertir les personnes concernées. Cependant, étant donné que les mots de passe ont été compromis, ils devront être renouvelés par le responsable du traitement des données. Au cours de ce processus, il sera nécessaire d'informer les utilisateurs des raisons pour lesquelles les mots de passe sont renouvelés. En outre, étant donné que de nombreux utilisateurs emploient le même mot de passe pour plusieurs comptes[12], il est également probable que la violation implique, à titre de préjudice secondaire, une violation de la confidentialité concernant un autre compte. La personne concernée pourra réduire au minimum ces préjudices secondaires en modifiant les mots de passe de tous ses autres comptes. Par conséquent, la notification devrait également inclure des informations relatives aux préjudices probables pour les autres comptes, et recommander d'utiliser des mots de passe différents pour chaque site web et de renouveler les mots de passe de tous les comptes qui utilisaient le mot de passe compromis.

Exemple 2: *Des preuves dans le cadre d'une affaire criminelle concernant un particulier ont été envoyées à un avocat sur un CD, par courrier avec accusé de réception, mais le CD a été perdu par les services postaux.*

La violation directe est une violation de la disponibilité. Elle peut avoir une incidence négligeable ou très élevée pour le(s) particulier(s) concerné(s) en fonction de la possibilité de prendre les mesures appropriées en temps voulu.
Mais un deuxième préjudice est susceptible de survenir si le CD est envoyé sans protection adéquate et qu'un tiers accède aux données. En effet, ce tiers peut les lire, les envoyer à des journalistes, etc. Ce préjudice indirect peut avoir des conséquences très importantes pour le(s) particulier(s).

Dans le cas d'espèce, si le CD peut être renvoyé en temps voulu, l'incidence de la violation directe sur le particulier sera négligeable et n'impliquera pas de notification au particulier, alors que le préjudice indirect potentiel peut être très grave et impliquera nécessairement d'avertir le particulier.

Si une seule personne est concernée, est-il nécessaire de l'avertir?

Oui, la directive 2002/58/CE ne fixe pas de nombre minimal de personnes concernées par une violation de données pour entamer le processus de notification. L'article 3, paragraphe 1, de la directive sur les télécommunications dispose que: «*Lorsque la violation de données à caractère personnel est de nature à affecter négativement les données à caractère personnel ou la vie privée d'un abonné ou d'un particulier, le fournisseur avertit également sans retard indu l'abonné ou le particulier concerné de la violation.*»

[12] Selon des études récentes, 55 % à 80 % des internautes emploient le même mot de passe pour différents comptes.

Par conséquent, le responsable du traitement devrait effectuer la notification, en fonction des effets néfastes probables, indépendamment du nombre de personnes concernées.

Comment procéder quand des données sont susceptibles d'être publiques?

Il convient de tenir compte de deux éléments:

1. Le terme «public» peut impliquer différents niveaux de disponibilité: les données peuvent être librement accessibles sur l'internet, disponibles publiquement dans le cadre d'un service soumis à abonnement, disponibles publiquement hors ligne sur demande, etc.
   À titre d'exemple, en France, les listes électorales sont affichées sur les murs de la mairie pendant les élections; tout électeur ou parti politique peut les obtenir, mais la publication en ligne de ces listes n'est pas autorisée par la loi.
   Par conséquent, l'envoi accidentel de la version électronique des listes au mauvais électeur ou la perte d'un exemplaire sur papier de la liste ne constituerait pas une violation de la confidentialité, contrairement à une publication de la liste sur l'internet, qui devrait quant à elle être notifiée.

2. Certaines données peuvent être publiques pour certaines personnes concernées, mais pas pour d'autres.
   Par exemple, une liste de numéros de téléphone associés à un nom de famille peut contenir à la fois des numéros de téléphone figurant dans les annuaires téléphoniques publics et des numéros sur liste rouge.

En résumé, quand le niveau de disponibilité ou de publicité des données est modifié par la violation, celle-ci doit alors être considérée comme une violation de la confidentialité et être notifiée (si la violation est susceptible de porter préjudice aux personnes concernées).

Comment procéder à la notification quand les informations de contact des particuliers concernés sont insuffisantes ou inconnues?

Dans certains cas, même s'il entretient une relation contractuelle directe avec l'utilisateur final, le fournisseur ne dispose pas d'informations suffisantes pour assurer une notification en bonne et due forme. Dans ce cas, même si l'on tient compte de la possibilité d'effectuer la notification grâce à des avis publiés dans les médias, l'obligation de poursuivre les notifications individuelles en déployant tous les efforts raisonnables subsiste[13].

L'obligation de continuer à déployer des efforts raisonnables, même si elle incombe au fournisseur, en mettant en place tous les mécanismes raisonnables afin de garantir que tous les particuliers affectés soient informés de la violation, n'exclut toutefois pas la possibilité de

[13] Selon l'article 3, paragraphe 7, du règlement (UE) nº 611/2013, si le fournisseur, «malgré les efforts raisonnables déployés, n'est pas en mesure d'identifier toutes les personnes susceptibles d'être lésées par la violation de données à caractère personnel, il informera ces personnes dans le délai applicable, par des avis dans de grands médias nationaux ou régionaux dans les États membres concernés». Dans le même esprit, le même paragraphe prévoit que le fournisseur continue à déployer tous les efforts raisonnables pour identifier ces personnes et les informer dès que possible.

demander l’aide d’autres fournisseurs ou responsables du traitement qui possèdent les informations de contact. Par conséquent, si l’on reprend le cas 4, le responsable du traitement qui ne possède pas les coordonnées des titulaires des cartes pourrait signaler le problème à l’agent de paiement intermédiaire qui peut facilement contacter les personnes en question. D’autres cas peuvent nécessiter la collaboration des autorités compétentes, qui devraient être informées, en tout état de cause, du fait que le fournisseur ne peut garantir de notifications individuelles.

Est-il nécessaire d'avertir les personnes qui n’ont pas été affectées par la violation?

Non, pour autant que l’on puisse déterminer avec certitude quelles personnes ont été affectées par la violation de données. Par exemple, si l’on peut démontrer qu’une partie des personnes n’ont pas été affectées par l’incident de sécurité, il n'est pas nécessaire d'avertir ces personnes. Cependant, le responsable du traitement des données doit prendre en considération tous les effets néfastes probables lorsqu’il prend cette décision. Selon la nature de la violation, certaines personnes peuvent aussi s'inquiéter de ne pas recevoir de notification.