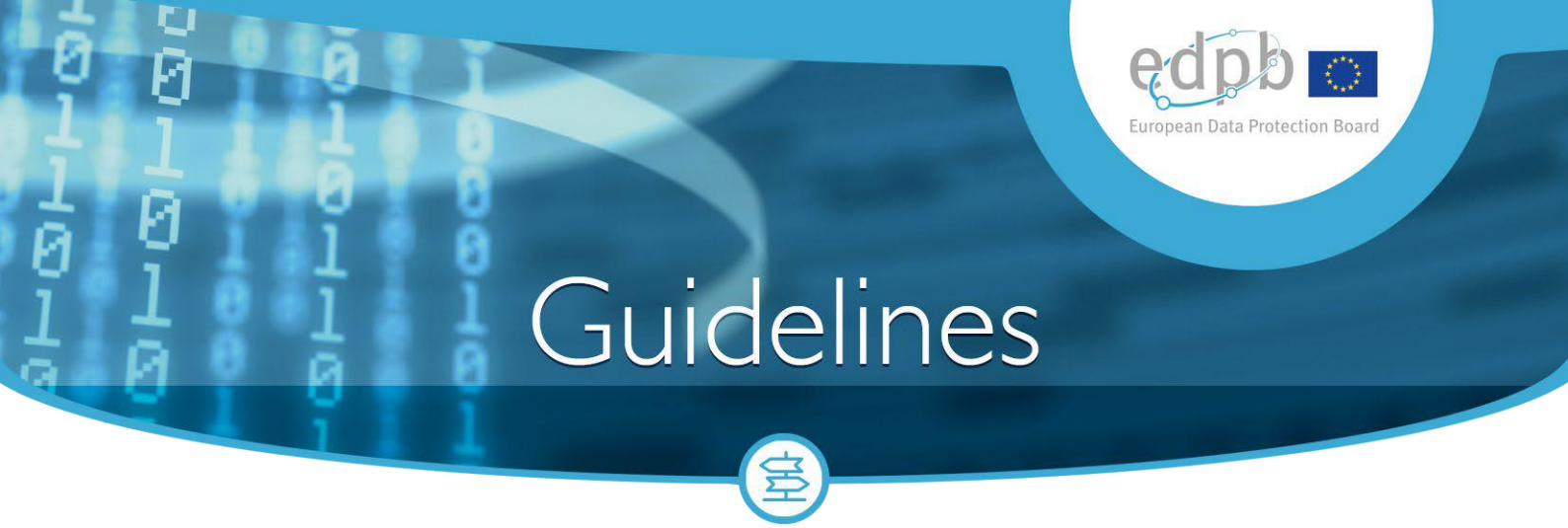


Lignes directrices 9/2022 sur la notification de violations de données à caractère personnel en vertu du RGPD

Version 2.0

Adoptées le 28 mars 2023

Historique des versions

Version 1.0	10 octobre 2022	Adoption des lignes directrices [version actualisée des lignes directrices précédentes WP250 (rév.01) adoptées par le groupe de travail «article 29» et approuvées par le comité européen de la protection des données le 25 mai 2018] pour consultation publique ciblée.
Version 2.0	28 mars 2023	Adoption des lignes directrices à la suite de la consultation publique ciblée portant sur la question de la notification de violations de données pour les responsables du traitement non établis dans l'EEE.

TABLE DES MATIÈRES

Le comité européen de la protection des données,

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

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

vu les articles 12 et 22 de son règlement intérieur,

vu les lignes directrices du groupe de travail «article 29» sur la notification de violations de données à caractère personnel en vertu du règlement (UE) 2016/679, WP250 rév.01,

A ADOPTÉ LES LIGNES DIRECTRICES SUIVANTES

0 PRÉFACE

1. Le 3 octobre 2017, le groupe de travail «article 29» (ci-après le «G29») a adopté ses lignes directrices sur la notification des violations de données à caractère personnel au titre du règlement (UE) 2016/679 (WP250 rév.01)[2], qui ont été approuvées par le comité européen de la protection des données (ci-après le «CEPD») lors de sa première réunion plénière[3]. Le présent document est une version légèrement actualisée de ces lignes directrices. Toute référence faite aux lignes directrices du G29 sur la notification de violations de données à caractère personnel en vertu du règlement (UE) 2016/679 (WP250 rév.01) devrait désormais s'entendre comme faisant référence aux présentes lignes directrices 9/2022 du CEPD.

2. Le CEPD a constaté qu'il était nécessaire de clarifier les exigences en matière de notification concernant les violations de données à caractère personnel dans les établissements de pays tiers. Le point relatif à ce sujet a été révisé et actualisé, le reste du document demeurant inchangé, à l'exception de modifications rédactionnelles. La révision concerne plus particulièrement le point 73 de la section II.C.2 du présent document.

INTRODUCTION

3. Le RGPD a introduit l'exigence que toute violation de données à caractère personnel (ci-après la «violation») soit notifiée à l'autorité de contrôle nationale compétente[4] (ou en cas de violation transfrontalière, à l'autorité chef de file) et, dans certains cas, communiquée aux personnes dont les données à caractère personnel ont été affectées par ladite violation.

4. L'obligation de notifier les violations existait pour certaines organisations, telles que les fournisseurs de services de communications électroniques accessibles au public [comme prévu par la directive

[1] Dans le présent document, on entend par «États membres» les «États membres de l'EEE».
[2] Lignes directrices du G29 sur la notification de violations de données à caractère personnel en vertu du règlement (UE) 2016/679 (WP250 rév.01) (dernière version révisée et adoptée le 6 février 2018), disponibles à l'adresse https:// ec.europa.eu/newsroom/article29/items/612052.
[3] Voir https://edpb.europa.eu/news/news/2018/endorsement-gdpr-wp29-guidelines-edpb_fr.
[4] Voir l'article 4, paragraphe 21, du RGPD.

2009/136/CE et le règlement (UE) nº 611/2013][5]. Certains États membres disposaient par ailleurs déjà de leur propre obligation de notification des violations. Il pouvait s'agir de l'obligation de notifier les violations impliquant certaines catégories de responsables du traitement autres que les fournisseurs de services de communications électroniques accessibles au public (par exemple, en Allemagne et en Italie), ou de l'obligation de notifier toutes les violations portant sur des données à caractère personnel (par exemple, aux Pays-Bas). D'autres États membres pouvaient disposer de codes de bonne pratique pertinents (par exemple, en Irlande[6]). Cependant, si un certain nombre d'autorités européennes chargées de la protection des données ont encouragé les responsables du traitement à notifier les violations, la directive 95/46/CE sur la protection des données[7], que le RGPD a remplacé, ne contenait pas d'obligation spécifique à cet égard. Une telle exigence était donc nouvelle pour de nombreuses organisations. Le RGPD rend cette notification obligatoire pour tous les responsables du traitement à moins qu'une violation soit peu susceptible d'engendrer un risque pour les droits et libertés des individus[8]. Les sous-traitants ont également un rôle important à jouer et doivent notifier toute violation au responsable du traitement[9].

5. Le CEPD considère que cette exigence de notification présente plusieurs avantages. Lors de la notification à l'autorité de contrôle, les responsables du traitement peuvent notamment obtenir des conseils afin de savoir s'il convient d'informer les personnes concernées. En effet, l'autorité de contrôle peut ordonner au responsable du traitement d'informer lesdites personnes de la violation[10]. D'un autre côté, la communication d'une violation aux personnes concernées permet au responsable du traitement de leur fournir des informations sur les risques résultant de la violation et sur les mesures qu'elles peuvent prendre afin de se protéger des conséquences potentielles. Tout plan de réaction à une violation devrait viser à protéger les individus et leurs données à caractère personnel. Aussi la notification des violations devrait-elle être vue comme un outil permettant de renforcer la conformité en matière de protection des données à caractère personnel. Parallèlement, il convient de noter que la non-communication d'une violation aux personnes concernées ou à l'autorité de contrôle pourrait entraîner une sanction pour le responsable du traitement en vertu de l'article 83 du RGPD.

6. Les responsables du traitement et les sous-traitants sont ainsi encouragés à prévoir à l'avance et à mettre en place des processus leur permettant de détecter et d'endiguer rapidement toute violation, d'évaluer les risques pour les personnes concernées[11] et de déterminer ensuite s'il est nécessaire d'informer l'autorité de contrôle compétente et de communiquer, si nécessaire, la violation aux personnes concernées. La notification à l'autorité de contrôle devrait faire partie intégrante de ce plan de réaction aux incidents.

7. Le RGPD contient des dispositions concernant les cas où une violation doit être notifiée, les personnes et entités auxquelles il convient de la notifier ainsi que les informations que devrait comprendre cette notification. Les informations requises pour une telle notification peuvent certes être communiquées

---

[5] Voir http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=celex:32009L0136 et http://eur-lex.europa.eu/legalcontent/FR/TXT/?uri=CELEX%3A32013R0611

[6] Voir https://www.dataprotection.ie/docs/Data_Security_Breach_Code_of_Practice/1082.htm

[7] Voir http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=celex:31995L0046

[8] Les droits consacrés par la charte des droits fondamentaux de l'Union européenne, disponible à l'adresse suivante: http://eurlex.europa.eu/legal-content/FR/TXT/?uri=CELEX:12012P/TXT

[9] Voir l'article 33, paragraphe 2, du RGPD. Ce concept est similaire à celui de l'article 5 du règlement (UE) nº 611/2013, qui dispose qu'un fournisseur auquel il est fait appel pour fournir une partie d'un service de communications électroniques (sans qu'il soit directement lié par contrat avec les abonnés) est tenu d'informer le fournisseur qui l'a engagé en cas de violation de données à caractère personnel.

[10] Voir l'article 34, paragraphe 4, et l'article 58, paragraphe 2, point e), du RGPD.

[11] Ceci peut se faire dans le cadre de l'exigence de suivi et d'examen de l'analyse d'impact relative à la protection des données (AIPD), requise pour les opérations de traitement susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes physiques (article 35, paragraphes 1 et 11).

de façon échelonnée, mais les responsables du traitement devraient réagir à toute violation dans des délais appropriés.

8. Dans son avis 03/2014 sur la notification des violations de données à caractère personnel[12], le G29 a fourni des orientations aux responsables du traitement afin de les aider à décider s'il convient d'informer les personnes concernées en cas de violation. L'avis portait sur l'obligation imposée aux fournisseurs de communications électroniques au titre de la directive 2002/58/CE, fournissait des exemples tirés de nombreux secteurs, dans le contexte du RGPD, encore à l'état de projet à l'époque, et présentait une série de bonnes pratiques à l'intention de tous les responsables du traitement.

9. Les présentes lignes directrices expliquent les obligations établies par le RGPD en matière de notification et de communication des violations ainsi que certaines des mesures que les responsables du traitement et les sous-traitants peuvent adopter en vue de respecter ces obligations. Elles fournissent également des exemples de différents types de violations et des entités et personnes à informer dans différents cas de figure.

I. NOTIFICATION D'UNE VIOLATION DE DONNÉES À CARACTÈRE PERSONNEL EN VERTU DU RGPD

A. Considérations de base concernant la sécurité

10. L'une des exigences du RGPD est que les données à caractère personnel soient traitées de façon à garantir un niveau de sécurité approprié desdites données, et notamment à les protéger contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées[13].

11. Le RGPD exige par conséquent des responsables du traitement et des sous-traitants qu'ils mettent en place des mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque pour les données à caractère personnel traitées. Ils devraient tenir compte de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, que présente le traitement pour les droits et libertés des personnes physiques[14]. Le RGPD exige également que toutes les mesures de protection techniques et organisationnelles appropriées soient mises en œuvre pour établir immédiatement si une violation des données à caractère personnel s'est produite, ce qui déterminera si l'obligation de notification s'applique[15].

12. Aussi l'un des éléments clés de toute politique de sécurité des données est d'être en mesure de prévenir toute violation dans la mesure du possible et, lorsqu'une telle violation se produit malgré tout, d'y réagir dans les meilleurs délais.

B. Qu'est-ce qu'une violation de données à caractère personnel?

1. Définition

13. Avant de pouvoir remédier à une violation, le responsable du traitement doit être capable de la reconnaître. À son article 4, paragraphe 12, le RGPD définit une «violation de données à caractère personnel» comme:

---

[12] Voir l'avis 03/2014 du G29 sur la notification des violations de données à caractère personnel http://ec.europa.eu/justice/data-protection/article29/documentation/opinion-recommendation/files/2014/wp213_en.pdf

[13] Voir l'article 5, paragraphe 1, point f), et l'article 32 du RGPD.

[14] Article 32; voir également le considérant 83 du RGPD.

[15] Voir le considérant 87 du RGPD.

«*une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données*».

14. Ce que l'on entend par «destruction» de données à caractère personnel devrait être assez clair: il s'agit des cas où les données n'existent plus, ou n'existent plus sous une forme utile pour le responsable du traitement. «Dommage» devrait également être relativement clair: il s'agit des cas où les données à caractère personnel ont été altérées, corrompues ou ne sont plus complètes. Pour ce qui est de la «perte» de données à caractère personnel, cela signifie que les données pourraient toujours exister, mais que le responsable du traitement a perdu tout contrôle ou tout accès à ces données, ou encore qu'il ne les a plus en sa possession. Enfin, le traitement non autorisé ou illicite peut inclure la divulgation de données à caractère personnel à des destinataires (ou l'accès à de telles données par ceux-ci) n'étant pas autorisés à les recevoir (ou à y avoir accès), ou toute autre forme de traitement en infraction au RGPD.

Exemple

Il peut, par exemple, y avoir perte de données à caractère personnel lorsqu'un appareil contenant une copie de la base de données client d'un responsable du traitement est perdu ou volé. Un autre exemple de perte serait lorsque la copie unique d'un ensemble de données à caractère personnel a été chiffrée par un rançongiciel, ou par le responsable du traitement à l'aide d'une clé qui n'est plus en sa possession.

15. Il convient avant tout de garder à l'esprit qu'une violation est une forme d'incident de sécurité. Toutefois, comme indiqué à l'article 4, paragraphe 12, le RGPD ne s'applique que lorsqu'il s'agit d'une violation de données à caractère personnel. Une telle violation aura pour conséquence que le responsable du traitement ne sera plus en mesure d'assurer la conformité avec les principes relatifs au traitement de données à caractère personnel tels que définis à l'article 5 du RGPD. Cette nuance met en lumière la différence entre un incident de sécurité et une violation de données à caractère personnel: si toutes les violations de données à caractère personnel constituent des incidents de sécurité, tous les incidents de sécurité ne constituent pas nécessairement des violations de données à caractère personnel[16].

16. Les éventuelles conséquences négatives d'une violation pour les personnes concernées sont envisagées ci-après.

2. Types de violations de données à caractère personnel

17. Dans son avis 03/2014 sur la notification des violations, le G29 expliquait que les violations pouvaient être classées selon trois principes de sécurité de l'information bien connus[17]:

- «**violation de la confidentialité**» – la divulgation ou l'accès non autorisés ou accidentels à des données à caractère personnel;
- «**violation de l'intégrité**» – l'altération non autorisée ou accidentelle de données à caractère personnel;

[16] Il convient de noter qu'un incident de sécurité ne se limite pas à des modèles de menaces où une entité extérieure s'attaque à une organisation, mais qu'il inclut également les incidents de traitement internes qui enfreignent les principes de sécurité.
[17] Voir l'avis 03/2014 du G29.

- «**violation de la disponibilité**» – la destruction ou la perte accidentelles ou non autorisées de l'accès[18] à des données à caractère personnel.

18. Il convient également de noter qu'en fonction des circonstances, une violation peut concerner à la fois la confidentialité, l'intégrité et la disponibilité de données à caractère personnel ou une combinaison de ces éléments.

19. S'il est relativement facile de déterminer si une violation de la confidentialité ou de l'intégrité s'est produite, il peut être moins évident de déterminer l'existence d'une violation de la disponibilité. Une violation sera toujours considérée comme une violation de la disponibilité en cas de perte ou de destruction permanente de données à caractère personnel.

Exemple

Il peut, par exemple, y avoir perte de disponibilité lorsque des données ont été supprimées, soit accidentellement, soit par une personne non autorisée, ou encore, dans le cas de données chiffrées de façon sécurisée, lorsque la clé de déchiffrement a été perdue. Si le responsable du traitement n'est pas en mesure de restaurer l'accès aux données, par exemple au moyen d'une sauvegarde, alors la perte de disponibilité sera considérée comme permanente.

Une perte de disponibilité peut également se produire en cas de perturbation majeure du service normal d'une organisation, par exemple dans le cas d'une panne de courant ou d'une attaque par déni de service rendant les données à caractère personnel indisponibles.

20. La question pourrait se poser de savoir si une perte de disponibilité temporaire des données à caractère personnel doit être considérée comme une violation, et, si tel est le cas, s'il est nécessaire de la notifier. L'article 32 du RGPD sur la «sécurité du traitement» explique que, lors de la mise en œuvre des mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, il convient d'envisager, entre autres, «*des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement*», ainsi que «*des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique*».

21. Par conséquent, un incident de sécurité entraînant l'indisponibilité temporaire de données à caractère personnel est également considéré comme un type de violation, dès lors que la perte de l'accès aux données peut avoir une incidence significative sur les droits et libertés des personnes physiques. Il convient de préciser que l'indisponibilité de données à caractère personnel en raison d'un entretien planifié du système n'est pas considérée comme une «violation de la sécurité» au sens de l'article 4, paragraphe 12, du RGPD.

22. Une violation entraînant une perte de disponibilité temporaire devrait être documentée conformément à l'article 33, paragraphe 5, du RGPD, au même titre qu'une perte ou une destruction permanente de données à caractère personnel (ou tout autre type de violation). Cela aidera le responsable du traitement à démontrer son respect du principe de responsabilité à l'autorité de

[18] Il est bien établi que l'«accès» est une composante fondamentale de la «disponibilité». Voir par exemple NIST SP800-SP80053rev4, qui définit la «disponibilité» comme: «le principe consistant à garantir que les informations sont accessibles et utilisables en temps utile et de manière fiable», disponible à l'adresse suivante: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf. Le CNSSI-4009 mentionne également: «L'accès rapide et fiable aux données et services d'information pour les utilisateurs autorisés». Voir https://rmf.org/wpcontent/uploads/2017/10/CNSSI-4009.pdf. L'ISO/IEC 27000:2016 définit également la disponibilité comme la «propriété d'être accessible et utilisable à la demande par une entité autorisée»: https://www.iso.org/obp/ui/#iso:std:isoiec:27000:ed-4:v1:fr

contrôle, qui pourrait demander à consulter ces registres[19]. Toutefois, en fonction des circonstances de la violation, il peut être nécessaire ou non de la notifier à l'autorité de contrôle et de la communiquer aux personnes concernées. Afin d'en juger, le responsable du traitement devra évaluer la probabilité et la gravité de l'incidence de la perte de disponibilité des données à caractère personnel sur les droits et libertés des personnes physiques. Conformément à l'article 33 du RGPD, le responsable du traitement devra en effet notifier la violation, à moins que celle-ci ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques. Ce point devra évidemment faire l'objet d'une appréciation au cas par cas.

Exemple

Si des données médicales critiques concernant les patients d'un hôpital sont rendues indisponibles, ne serait-ce que temporairement, cela pourrait présenter un risque pour les droits et libertés des personnes concernées; des opérations pourraient par exemple être annulées et des vies mises en danger.

Inversement, si les systèmes d'une entreprise médiatique ne sont pas disponibles pendant plusieurs heures (p. ex. en raison d'une panne de courant), et que l'entreprise en question n'est de ce fait plus en mesure d'envoyer des bulletins d'information à ses abonnés, il est peu probable que cela représente un risque pour les droits et libertés des personnes concernées.

23. Il convient de noter que, bien qu'une perte de disponibilité des systèmes du responsable du traitement puisse être uniquement temporaire et n'avoir aucune incidence sur les personnes physiques, il est important que le responsable du traitement envisage toutes les conséquences potentielles d'une violation, dès lors qu'elle peut encore nécessiter une notification pour d'autres raisons.

Exemple

Une attaque par rançongiciel (logiciel malveillant qui chiffre les données du responsable du traitement jusqu'à ce qu'une rançon soit versée) pourrait entraîner une perte temporaire de disponibilité si les données peuvent être restaurées au moyen d'une sauvegarde. Cependant, une intrusion dans le réseau s'est tout de même produite et sa notification pourrait se révéler nécessaire si l'incident est considéré comme une violation de la confidentialité (c.-à-d. que le pirate a accédé aux données à caractère personnel) et que cela présente un risque pour les droits et libertés des personnes physiques.

3. Les conséquences possibles d'une violation de données à caractère personnel

24. Une violation peut potentiellement avoir, pour les personnes concernées, toute une série de conséquences négatives, susceptibles d'entraîner des dommages physiques, matériels ou un préjudice moral. Le RGPD explique que ces dommages et préjudices peuvent inclure une perte de contrôle sur leurs données à caractère personnel, la limitation de leurs droits, une discrimination, un vol ou une usurpation d'identité, une perte financière, un renversement non autorisé de la procédure de pseudonymisation, une atteinte à la réputation ou une perte de confidentialité de données à caractère personnel protégées par le secret professionnel. Ils peuvent également comprendre tout autre dommage économique ou social important pour les personnes concernées[20].

25. Le RGPD exige donc du responsable du traitement qu'il notifie toute violation à l'autorité de contrôle, à moins qu'elle ne soit pas susceptible d'engendrer le risque que de telles conséquences négatives ne se produisent. Lorsqu'en revanche, ce risque est élevé, le RGPD exige du responsable du traitement qu'il communique la violation aux personnes concernées dans les meilleurs délais[21].

[19] Voir l'article 33, paragraphe 5, du RGPD.
[20] Voir également les considérants 75 et 85 du RGPD.
[21] Voir également le considérant 86 du RGPD.

26. Le considérant 87 du RGPD souligne l'importance d'être en mesure d'identifier une violation, d'évaluer ses risques pour les personnes concernées et de la notifier, le cas échéant:

> «*Il convient de vérifier si toutes les mesures de protection techniques et organisationnelles appropriées ont été mises en œuvre pour établir immédiatement si une violation des données à caractère personnel s'est produite et pour informer rapidement l'autorité de contrôle et la personne concernée. Il convient d'établir que la notification a été faite dans les meilleurs délais, compte tenu en particulier de la nature et de la gravité de la violation des données à caractère personnel et de ses conséquences et effets négatifs pour la personne concernée. Une telle notification peut amener une autorité de contrôle à intervenir conformément à ses missions et à ses pouvoirs fixés par le présent règlement*.»

27. Des orientations complémentaires sur l'évaluation du risque de conséquences négatives pour les personnes concernées sont disponibles au chapitre IV du présent document.

28. Si les responsables du traitement ne notifient pas une violation de données à l'autorité de contrôle, aux personnes concernées ou aux deux, alors que les conditions établies à l'article 33 et/ou 34 du RGPD sont remplies, l'autorité de contrôle sera amenée à effectuer un choix, dans le cadre duquel elle sera tenue d'envisager toutes les mesures correctrices à sa disposition, notamment l'imposition d'une amende administrative appropriée[22], que celle-ci accompagne l'une des mesures correctrices définies par l'article 58, paragraphe 2, du RGPD ou soit imposée comme une sanction indépendante. Si une telle amende administrative est choisie, celle-ci pourra s'élever jusqu'à 10 000 000 EUR ou jusqu'à 2 % du chiffre d'affaires annuel mondial total de l'entreprise conformément à l'article 83, paragraphe 4, point a), du RGPD. Il importe également de garder à l'esprit que dans certains cas, la non-notification d'une violation pourrait trahir une absence de mesures de sécurité ou l'inadéquation des mesures de sécurité existantes. Les lignes directrices du G29 sur les amendes administratives disposent que: «[l]*a survenance de plusieurs violations différentes commises simultanément dans un cas particulier implique que l'autorité de contrôle a la possibilité d'infliger les amendes administratives à un niveau qui rend celles-ci efficaces, proportionnées et dissuasives, dans les limites de la violation la plus grave*». Dans un tel cas, l'autorité de contrôle aura également la possibilité de prononcer des sanctions pour non-notification ou non-communication d'une violation (articles 33 et 34 du RGPD), d'une part, et pour absence de mesures de sécurité (adéquates) (article 32 du RGPD), d'autre part, dès lors qu'il s'agit de deux violations distinctes.

II. ARTICLE 33 – NOTIFICATION À L'AUTORITÉ DE CONTRÔLE

A. Quand procéder à la notification

1. Exigences de l'article 33

29. L'article 33, paragraphe 1, du RGPD dispose ce qui suit:

> «*En cas de violation de données à caractère personnel, le responsable du traitement en notifie la violation en question à l'autorité de contrôle compétente conformément à l'article 55, dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance, à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques. Lorsque la notification à l'autorité de contrôle n'a pas lieu dans les 72 heures, elle est accompagnée des motifs du retard*.»

[22] Pour plus de détails, voir les lignes directrices du G29 sur l'application et la fixation des amendes administratives, disponibles à l'adresse suivante: http://ec.europa.eu/newsroom/just/document.cfm?doc_id=47889

30. Le considérant 87 du RGPD prévoit ce qui suit[23]:

> «*Il convient de vérifier si toutes les mesures de protection techniques et organisationnelles appropriées ont été mises en œuvre pour établir immédiatement si une violation des données à caractère personnel s'est produite et pour informer rapidement l'autorité de contrôle et la personne concernée. Il convient d'établir que la notification a été faite dans les meilleurs délais, compte tenu en particulier de la nature et de la gravité de la violation des données à caractère personnel et de ses conséquences et effets négatifs pour la personne concernée. Une telle notification peut amener une autorité de contrôle à intervenir conformément à ses missions et à ses pouvoirs fixés par le présent règlement*.»

2. Quand un responsable du traitement prend-il «connaissance»?

31. Comme indiqué ci-dessus, en cas de violation, le RGPD exige du responsable du traitement qu'il notifie la violation en question dans les meilleurs délais, et, si possible, 72 heures au plus tard après en avoir pris connaissance. Cette exigence soulève la question de savoir quand un responsable du traitement peut être considéré comme ayant pris «connaissance» d'une violation. Le CEPD considère qu'un responsable du traitement devrait être considéré comme ayant pris «connaissance» lorsqu'il est raisonnablement certain qu'un incident de sécurité s'est produit et que cet incident a compromis des données à caractère personnel.

32. Cependant, comme indiqué précédemment, le RGPD exige du responsable du traitement qu'il mette en œuvre toutes les mesures de protection techniques et organisationnelles appropriées pour établir immédiatement si une violation des données à caractère personnel s'est produite et pour informer rapidement l'autorité de contrôle et les personnes concernées. Il dispose également qu'il convient d'établir que la notification a été faite dans les meilleurs délais, compte tenu en particulier de la nature et de la gravité de la violation et de ses conséquences et effets négatifs pour la personne concernée[24]. Le responsable du traitement se voit ainsi tenu de prendre les mesures nécessaires pour s'assurer de prendre «connaissance» de toute violation dans les meilleurs délais afin de pouvoir réagir de façon appropriée.

33. Le moment exact où un responsable du traitement peut être considéré comme ayant pris «connaissance» d'une violation spécifique dépendra des circonstances de la violation en question. Dans certains cas, il sera relativement clair dès le début qu'une violation s'est produite, tandis que dans d'autres, un certain temps pourrait être nécessaire avant de pouvoir déterminer si des données à caractère personnel ont été compromises. L'accent devrait toutefois être mis sur une intervention et une enquête rapide visant à déterminer s'il y a effectivement eu violation de données à caractère personnel, et, si tel est le cas, à prendre des mesures correctives et à avertir qui de droit, le cas échéant.

Exemples

1. Dans le cas de la perte d'une clé USB contenant des données à caractère personnel chiffrées, il est souvent impossible d'évaluer si des personnes non autorisées ont eu accès auxdites données. Cependant, bien que le responsable du traitement ne soit pas en mesure de déterminer si une violation de la confidentialité s'est produite, un tel cas doit être notifié dès lors qu'il est raisonnablement certain qu'une violation de la disponibilité a eu lieu; le responsable du traitement aurait pris «connaissance» de cette violation lorsqu'il s'est rendu compte de la disparition de la clé USB.

2. Un tiers informe un responsable du traitement qu'il a accidentellement reçu les données à caractère personnel de l'un de ses clients et fournit la preuve de cette divulgation non autorisée. Dès

[23] Le considérant 85 du RGPD est également important à cet égard.

[24] Voir le considérant 87 du RGPD.

lors que le responsable du traitement a reçu des preuves claires attestant d'une violation de la confidentialité, il ne fait aucun doute qu'il en a pris «connaissance».

3. Un responsable du traitement remarque une possible intrusion dans son réseau. Il vérifie son système afin de déterminer si les données à caractère personnel qui y sont conservées ont été compromises et confirme que tel est le cas. Une fois encore, dès lors que le responsable du traitement dispose à présent de preuves claires attestant d'une violation, il ne fait aucun doute qu'il en a pris «connaissance».

4. Un cybercriminel contacte le responsable du traitement après avoir piraté son système afin de lui demander une rançon. Dans ce cas, après avoir vérifié son système en vue de confirmer qu'il a été piraté, le responsable du traitement dispose de preuves claires attestant qu'une violation s'est produite, et il ne fait aucun doute qu'il en a pris connaissance.

34. Après avoir été informé d'une possible violation par un individu, par une organisation médiatique ou par une autre source, ou encore lorsqu'il a lui-même détecté un incident de sécurité, le responsable du traitement peut mener une brève enquête afin de déterminer si une violation s'est effectivement produite. Lors de cette période d'enquête, le responsable du traitement peut ne pas être considéré comme ayant pris «connaissance». Cette période d'enquête initiale devrait cependant débuter aussi rapidement que possible et déterminer avec un degré de certitude raisonnable si une violation s'est produite; une enquête plus détaillée pourra alors suivre.

35. Après avoir pris connaissance d'un incident, le responsable du traitement devra notifier toute violation soumise à l'obligation de notification dans les meilleurs délais, et, si possible, dans les 72 heures. Au cours de cette période, le responsable du traitement devrait évaluer le risque probable pour les personnes, afin de déterminer si l'obligation de notification a été déclenchée, ainsi que la ou les mesures nécessaires pour remédier à la violation. Un responsable du traitement peut cependant déjà disposer d'une évaluation initiale des risques potentiels qui pourraient résulter d'une violation dans le cadre d'une analyse d'impact relative à la protection des données (AIPD)[25] effectuée préalablement aux opérations de traitement concernées. Une AIPD est néanmoins plus générale que les circonstances spécifiques de toute violation réelle. Aussi une évaluation complémentaire tenant compte de ces circonstances devra-t-elle être réalisée en tout état de cause. Pour plus d'informations sur l'évaluation du risque, voir le chapitre IV.

36. Dans la plupart des cas, ces mesures préliminaires devraient être prises peu de temps après l'alerte initiale (c.-à-d. lorsque le responsable du traitement ou le sous-traitant suspecte qu'un incident de sécurité portant sur des données à caractère personnel pourrait avoir eu lieu). À l'exception de certains cas exceptionnels, cette procédure ne devrait pas être plus longue que dans l'exemple ci-dessous.

Exemple

Une personne informe le responsable du traitement qu'elle a reçu un courrier électronique dont l'expéditeur se fait passer pour le responsable du traitement et qui contient des données à caractère personnel concernant son utilisation (réelle) des services du responsable du traitement, ce qui indiquerait que la sécurité de ce dernier a été compromise. Le responsable du traitement procède à une brève enquête et repère une intrusion dans son réseau ainsi que des preuves signalant un accès non autorisé à des données à caractère personnel. Le responsable du traitement sera désormais considéré comme ayant pris «connaissance» de la violation et devra en informer l'autorité de contrôle, à moins que ladite violation ne soit peu susceptible d'engendrer un risque pour les droits et libertés

[25] Voir les lignes directrices WP248 du G29 sur les AIPD à l'adresse suivante: http://ec.europa.eu/newsroom/document.cfm?doc_id=44137

des individus. Le responsable du traitement devra prendre des mesures correctives appropriées afin de remédier à la violation.

37. Le responsable du traitement devrait disposer de procédures internes afin d'être en mesure de détecter une violation et d'y remédier. Par exemple, afin de détecter certaines irrégularités dans le traitement des données, un responsable du traitement ou un sous-traitant peut avoir recours à certaines mesures techniques telles que des analyseurs de flux de données et de journaux, qui permettront de définir des incidents et des alertes en établissant des corrélations entre des données journal[26]. Il est important qu'une fois détectée, une violation soit communiquée au niveau de direction approprié afin qu'il soit possible d'y remédier et, le cas échéant, de la notifier conformément à l'article 33 et, si nécessaire, à l'article 34. De telles mesures et de tels mécanismes de notification devraient être détaillés dans le plan de réaction aux incidents et/ou dans les accords de gouvernance. Ceux-ci aideront le responsable du traitement à planifier et à déterminer efficacement à qui échoit la responsabilité opérationnelle au sein de l'organisation concernant la gestion d'une violation, ainsi que s'il faut, et comment, rapporter une violation de façon appropriée.

38. Le responsable du traitement devrait également disposer d'accords avec tout sous-traitant auquel il a recours, lui-même soumis à l'obligation d'avertir le responsable du traitement en cas de violation (voir plus bas).

39. S'il incombe aux responsables du traitement et aux sous-traitants de mettre en place les mesures appropriées afin d'être en mesure de prévenir une violation, d'y réagir et d'y remédier, certaines mesures pratiques devraient être prises en toutes circonstances.

    - Des informations concernant tous les incidents de sécurité devraient être communiquées à une personne responsable ou aux personnes chargées de remédier aux incidents, d'établir l'existence d'une violation et d'évaluer le risque.
    - Le risque pour les personnes concernées résultant d'une violation devrait ensuite être évalué (risque inexistant, risque, ou risque élevé) et les services concernés de l'organisation devraient être informés.
    - Le cas échéant, il conviendra subséquemment de notifier la violation à l'autorité de contrôle et de la communiquer aux personnes concernées.
    - Parallèlement, le responsable du traitement devrait prendre des mesures pour endiguer la violation et y remédier. La violation devrait être documentée tout au long de son évolution.

40. Il doit donc être clair que le responsable du traitement a l'obligation de réagir à une alerte initiale et de déterminer si une violation a effectivement eu lieu. Cette brève période permet au responsable du traitement de procéder à une enquête et de collecter des preuves et autres informations pertinentes. Une fois que le responsable du traitement a établi, avec un degré de certitude raisonnable, qu'une violation a eu lieu, si les conditions de l'article 33, paragraphe 1, du RGPD sont remplies, il doit alors la notifier à l'autorité de contrôle dans les meilleurs délais et, si possible, dans les 72 heures[27]. Si un responsable du traitement ne réagit pas dans les meilleurs délais et qu'il apparaît de façon évidente qu'une violation a eu lieu, ce manque de réaction pourrait être considéré comme une non-notification en vertu de l'article 33 du RGPD.

41. L'article 32 du RGPD dispose clairement que le responsable du traitement et le sous-traitant doivent mettre en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau

[26] Il convient de noter que les données journal facilitant la vérifiabilité par exemple du stockage, des modifications ou de l'effacement des données peuvent aussi être qualifiées de données à caractère personnel concernant la personne qui a lancé les opérations de traitement respectives.

[27] Voir le règlement (CEE, Euratom) nº 1182/71 portant détermination des règles applicables aux délais, aux dates et aux termes, disponible à l'adresse suivante: http://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:31971R1182

de sécurité adapté des données à caractère personnel: la capacité de détecter une violation, d'y remédier et de la communiquer dans les meilleurs délais devrait être considérée comme un élément essentiel de ces mesures.

3. Responsables conjoints du traitement

42. L'article 26 du RGPD concerne les responsables conjoints du traitement et dispose que ceux-ci devraient définir leurs obligations respectives aux fins d'assurer le respect du RGPD[28]. Ceci impliquera de déterminer quelle partie sera responsable du respect des obligations définies aux articles 33 et 34 du RGPD. Le CEPD recommande que les arrangements contractuels entre les responsables conjoints du traitement comprennent des dispositions déterminant quel responsable du traitement prendra la direction ou sera responsable du respect de l'obligation de notification des violations établie par le RGPD.

4. Obligations du sous-traitant

43. Si le responsable du traitement conserve la responsabilité générale en matière de protection des données à caractère personnel, le rôle du sous-traitant est essentiel afin de permettre au responsable du traitement de respecter ses obligations, notamment en termes de notification des violations. En effet, l'article 28, paragraphe 3, du RGPD précise que le traitement par un sous-traitant est régi par un contrat ou un autre acte juridique. L'article 28, paragraphe 3, point f), dispose que le contrat ou l'autre acte juridique doit prévoir que le sous-traitant «aide le responsable du traitement à garantir le respect des obligations prévues aux articles 32 à 36, compte tenu de la nature du traitement et des informations à la disposition du sous-traitant».

44. L'article 33, paragraphe 2, du RGPD indique clairement que si un responsable du traitement a recours à un sous-traitant et que celui-ci prend connaissance d'une violation des données à caractère personnel qu'il traite au nom du responsable du traitement, il doit la lui notifier «dans les meilleurs délais». Il convient de noter que le sous-traitant ne doit pas évaluer la probabilité qu'un risque découle d'une violation avant de la notifier au responsable du traitement; il appartient au responsable du traitement d'effectuer cette évaluation après avoir pris connaissance de la violation. Le sous-traitant doit simplement établir si une violation s'est produite puis la notifier au responsable du traitement. Le responsable du traitement a recours au sous-traitant pour atteindre ses objectifs; aussi le responsable du traitement doit-il en principe être considéré comme ayant pris «connaissance» une fois que le sous-traitant l'a informé de la violation. L'obligation faite au sous-traitant de notifier la violation au responsable du traitement permet à ce dernier d'y remédier et de déterminer s'il est nécessaire d'avertir l'autorité de contrôle conformément à l'article 33, paragraphe 1, ainsi que les personnes concernées conformément à l'article 34, paragraphe 1. Le responsable du traitement pourrait également analyser lui-même la violation en question, dès lors que le sous-traitant pourrait ne pas connaître tous les éléments pertinents liés à la violation. Il pourrait par exemple ne pas savoir si le responsable du traitement conserve toujours une copie ou une sauvegarde des données à caractère personnel détruites ou perdues par le sous-traitant. Ces éléments pourraient avoir une incidence sur l'obligation de notification du responsable du traitement.

45. Le RGPD ne définit pas de délai spécifique dans lequel le sous-traitant doit alerter le responsable du traitement, si ce n'est qu'il doit le faire «dans les meilleurs délais». Aussi le CEPD recommande-t-il au sous-traitant de notifier rapidement la violation en question au responsable du traitement et de lui fournir des informations complémentaires à ce sujet au fur et à mesure que des détails supplémentaires se font jour. Cette communication est essentielle afin d'aider le responsable du traitement à satisfaire à son obligation de notifier la violation à l'autorité de contrôle dans les 72 heures.

[28] Voir également le considérant 79 du RGPD.

46. Comme expliqué plus haut, le contrat entre le responsable du traitement et le sous-traitant devrait inclure des dispositions précisant la façon de satisfaire aux exigences définies à l'article 33, paragraphe 2, parallèlement à d'autres dispositions du RGPD. Ces dispositions pourraient inclure des exigences de notification rapide par le sous-traitant, ce qui aiderait le responsable du traitement à respecter l'obligation d'informer l'autorité de contrôle dans les 72 heures.

47. Lorsque le sous-traitant propose ses services à plusieurs responsables du traitement affectés par le même incident, le sous-traitant devra communiquer les détails dudit incident à tous les responsables du traitement.

48. Un sous-traitant pourrait effectuer une notification au nom du responsable du traitement si celui-ci lui en a donné l'autorisation et si cela fait partie des dispositions contractuelles entre le responsable du traitement et le sous-traitant. Une telle notification doit être effectuée conformément aux articles 33 et 34 du RGPD. Il est cependant important de noter que le titulaire de l'obligation légale de notification reste le responsable du traitement

B. Fournir des informations à l'autorité de contrôle

1. Informations à fournir

49. Lorsqu'un responsable du traitement notifie une violation à l'autorité de contrôle, l'article 33, paragraphe 3, du RGPD prévoit que la notification doit, à tout le moins:

> *«a) décrire la nature de la violation de données à caractère personnel y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés;*
>
> (b) *communiquer le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues;*
>
> (c) *décrire les conséquences probables de la violation de données à caractère personnel;*
>
> (d) *décrire les mesures prises ou que le responsable du traitement propose de prendre pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives*.»

50. Le RGPD ne définit pas les catégories de personnes concernées ni les enregistrements de données à caractère personnel. Toutefois, le CEPD suggère que les catégories de personnes concernées se réfèrent aux différents types d'individus dont les données à caractère personnel ont été affectées par une violation: en fonction des descripteurs utilisés, cela pourrait inclure, entre autres, les enfants et autres groupes vulnérables, les personnes handicapées, les employés ou les clients. De façon similaire, les catégories d'enregistrements des données à caractère personnel pourraient se référer aux différents types d'enregistrement que le responsable du traitement pourrait traiter, telles que les données concernant la santé, les dossiers de scolarité, les informations relatives à l'assistance sociale, les données financières, les numéros de compte bancaire, les numéros de passeport, etc.

51. Le considérant 85 du RGPD indique clairement que l'obligation de notification a pour finalité de limiter les dommages pour les personnes physiques. Par conséquent, si les types de personnes concernées ou les types de données à caractère personnel témoignent d'un risque de dommages particuliers causés par une violation (p. ex. usurpation d'identité, fraude, perte financière, menace envers le secret professionnel), il est important que la notification indique ces catégories. De cette façon, l'obligation de définir les catégories est liée à l'obligation de décrire les conséquences probables de la violation.

52. L'absence d'informations précises (p. ex. le nombre exact de personnes concernées affectées) ne devrait pas constituer un obstacle à la notification d'une violation dans les meilleurs délais. Le RGPD accepte que des chiffres approximatifs soient communiqués quant au nombre de personnes et

d'enregistrements de données concernés. Il convient de se concentrer davantage sur le fait de remédier aux conséquences négatives de la violation que sur la fourniture de chiffres précis.

53. Aussi, lorsqu'il a été clairement établi qu'une violation s'est produite, mais que sa portée exacte n'est pas encore connue, une notification échelonnée (voir ci-après) est-elle une bonne manière de satisfaire à l'obligation de notification.

54. L'article 33, paragraphe 3, du RGPD dispose que le responsable du traitement doit «à tout le moins» inclure les informations listées dans toute notification, ce qui signifie qu'un responsable du traitement peut, si nécessaire, décider de fournir plus d'informations. Les différents types de violations (confidentialité, intégrité ou disponibilité) peuvent nécessiter la fourniture d'informations complémentaires afin d'expliquer en détail les circonstances de chaque cas.

Exemple

Le responsable du traitement pourrait trouver utile d'inclure le nom de son sous-traitant dans sa notification à l'autorité de contrôle si celui-ci est à l'origine de la violation, notamment si cette dernière a entraîné un incident ayant affecté les enregistrements de données à caractère personnel de nombreux autres responsables du traitement ayant recours au même sous-traitant.

55. En tout état de cause, l'autorité de contrôle peut demander des informations complémentaires dans le cadre de son enquête sur la violation.

2. Notification échelonnée

56. En fonction de la nature de la violation, il peut être nécessaire que le responsable du traitement effectue une enquête complémentaire afin d'établir tous les faits pertinents liés à l'incident. Aussi l'article 33, paragraphe 4, du RGPD dispose-t-il ce qui suit:

«*Si, et dans la mesure où, il n'est pas possible de fournir toutes les informations en même temps, les informations peuvent être communiquées de manière échelonnée sans autre retard indu*.»

57. Cela signifie que le RGPD reconnaît que les responsables du traitement ne disposeront pas toujours de toutes les informations nécessaires concernant une violation dans les 72 heures après en avoir pris connaissance, dès lors que l'ensemble des détails de l'incident peuvent ne pas être systématiquement disponibles au cours de cette période initiale. Il autorise donc une notification échelonnée. Une telle notification interviendra plus probablement dans le cas de violations plus complexes, telles que certains types d'incidents de cybersécurité nécessitant par exemple une enquête approfondie et détaillée afin d'établir pleinement la nature de la violation et la mesure dans laquelle des données à caractère personnel ont été compromises. Dans de nombreux cas, le responsable du traitement devra ainsi poursuivre son enquête et fournir des informations complémentaires à l'autorité de contrôle par la suite. Il y est autorisé à condition de justifier son retard conformément à l'article 33, paragraphe 1, du RGPD. Le CEPD recommande que, si le responsable du traitement ne dispose pas encore de toutes les informations nécessaires, il en informe l'autorité de contrôle dans le cadre de sa notification initiale et précise qu'il fournira des informations plus détaillées par la suite. L'autorité de contrôle devrait déterminer la façon et le moment où des informations complémentaires devraient être fournies. Cela n'empêche toutefois pas le responsable du traitement de fournir des informations complémentaires à tout autre moment s'il prend connaissance d'informations complémentaires pertinentes concernant la violation devant être communiquées à l'autorité de contrôle.

58. L'obligation de notification a pour objectif d'encourager les responsables du traitement à réagir rapidement à une violation, à l'endiguer et, si possible, à récupérer les données à caractère personnel compromises, ainsi qu'à solliciter des conseils auprès de l'autorité de contrôle. La notification à l'autorité de contrôle dans les premières 72 heures peut permettre au responsable du traitement de

s'assurer que sa décision concernant la communication ou non de la violation aux personnes concernées est correcte.

59. L'objectif de cette notification à l'autorité de contrôle n'est cependant pas uniquement d'obtenir des conseils relatifs à la notification éventuelle des personnes concernées. Dans certains cas, il sera évident qu'en raison de la nature de la violation et de la gravité du risque, le responsable du traitement devra informer les personnes concernées dans les meilleurs délais. Par exemple, s'il existe un risque immédiat d'usurpation d'identité, ou si des catégories particulières de données à caractère personnel[29] sont divulguées sur le web, le responsable du traitement devrait réagir dans les meilleurs délais afin d'endiguer la violation et de la communiquer aux personnes concernées (voir chapitre III). Dans des circonstances exceptionnelles, cette communication peut même être effectuée avant la notification à l'autorité de contrôle. De façon plus générale, la notification à l'autorité de contrôle ne peut servir de justification à la non-communication de la violation aux personnes concernées lorsque celle-ci est nécessaire.

60. Il convient également de préciser que si une enquête de suivi met au jour, après la notification initiale, des preuves indiquant que l'incident de sécurité a été endigué et qu'aucune violation n'a effectivement eu lieu, le responsable du traitement peut en informer l'autorité de contrôle. Cette information pourrait alors être ajoutée aux informations déjà fournies à l'autorité de contrôle et l'incident classé comme n'étant pas une violation. Aucune sanction n'est prévue en cas de notification d'un incident qui s'avère, en fin de compte, ne pas constituer une violation.

Exemple

Un responsable du traitement informe l'autorité de contrôle, dans les 72 heures suivant la détection de la violation, de la perte d'une clé USB contenant une copie des données à caractère personnel de certains de ses clients. Il s'avère par la suite que ladite clé USB avait été rangée au mauvais endroit dans les locaux du responsable du traitement et qu'elle a été retrouvée. Le responsable du traitement en informe l'autorité de contrôle et demande à ce que sa notification soit modifiée.

61. Il convient de noter qu'une telle approche échelonnée de la notification existe déjà en vertu des obligations découlant de la directive 2002/58/CE et du règlement nº 611/2013 ainsi que dans le cadre d'autres incidents autodéclarés.

3. Notification tardive

62. L'article 33, paragraphe 1, du RGPD indique clairement que lorsque la notification à l'autorité de contrôle n'a pas lieu dans les 72 heures, elle est accompagnée des motifs du retard. Cette disposition reconnaît, au même titre que le concept de notification échelonnée, qu'un responsable du traitement pourrait ne pas toujours être en mesure de notifier une violation dans ce délai, et qu'une notification tardive pourrait être autorisée.

63. Un tel scénario pourrait par exemple se produire lorsqu'un responsable du traitement constate, sur une courte période, plusieurs violations similaires affectant de façon identique de grandes quantités de personnes concernées. Un responsable du traitement pourrait prendre connaissance d'une violation et, en entreprenant son enquête et avant la notification, détecter d'autres violations similaires dont la cause diffère. En fonction des circonstances, il pourrait falloir un certain temps au responsable du traitement pour établir la portée des violations et pour élaborer une notification constructive comprenant différentes violations très similaires, mais aux causes potentiellement différentes, plutôt que de notifier chaque violation individuellement. La notification à l'autorité de contrôle pourrait par conséquent avoir lieu plus de 72 heures après la prise de connaissance de ces violations par le responsable du traitement.

[29] Voir l'article 9 du RGPD.

64. À proprement parler, chaque violation individuelle est un incident devant être notifié. Toutefois, afin d'éviter que la notification ne soit excessivement fastidieuse, le responsable du traitement pourrait soumettre une notification «groupée» énumérant toutes ces violations, à condition qu'elles concernent un seul type de données à caractère personnel compromises de façon similaire et qu'elles se soient produites sur une période de temps relativement courte. Si une série de violations concernant différents types de données à caractère personnel compromises de façon différente se produisent, la notification devra alors se faire selon la procédure classique, c'est-à-dire que chaque violation devra être notifiée conformément à l'article 33.

65. Si le RGPD autorise dans une certaine mesure les notifications tardives, celles-ci restent exceptionnelles. Il convient de signaler qu'une notification groupée peut également être effectuée pour des violations similaires multiples notifiées dans les 72 heures.

C. Violations transfrontalières et violations dans des établissements de pays tiers

1. Violations transfrontalières

66. En cas de traitement transfrontalier[30] de données à caractère personnel, une violation peut affecter des personnes concernées dans plus d'un État membre. L'article 33, paragraphe 1, du RGPD indique clairement qu'en cas de violation, le responsable du traitement doit la notifier à l'autorité de contrôle compétente conformément à l'article 55 du RGPD[31]. L'article 55, paragraphe 1, du RGPD dispose ce qui suit:

> «*Chaque autorité de contrôle est compétente pour exercer les missions et les pouvoirs dont elle est investie conformément au présent règlement sur le territoire de l'État membre dont elle relève*.»

67. Toutefois, l'article 56, paragraphe 1, du RGPD prévoit ce qui suit:

> «*Sans préjudice de l'article 55, l'autorité de contrôle de l'établissement principal ou de l'établissement unique du responsable du traitement ou du sous-traitant est compétente pour agir en tant qu'autorité de contrôle chef de file concernant le traitement transfrontalier effectué par ce responsable du traitement ou ce sous-traitant, conformément à la procédure prévue à l'article 60*.»

68. Par ailleurs, l'article 56, paragraphe 6, du RGPD énonce ce qui suit:

> «*L'autorité de contrôle chef de file est le seul interlocuteur du responsable du traitement ou du sous-traitant pour le traitement transfrontalier effectué par ce responsable du traitement ou ce sous-traitant*.»

69. Cela signifie qu'en cas de violation dans le cadre d'un traitement transfrontalier nécessitant une notification, le responsable du traitement devra informer l'autorité de contrôle chef de file[32]. Aussi un responsable du traitement doit-il, lors de la rédaction de son plan de réaction à une violation, évaluer quelle autorité de contrôle est l'autorité de contrôle chef de file qu'il devra informer[33]. Cela permettra au responsable du traitement de réagir rapidement à une violation et de respecter ses obligations au titre de l'article 33. Il doit être clair qu'en cas de violation impliquant un traitement transfrontalier, il convient de notifier la violation à l'autorité de contrôle chef de file, qui n'est pas nécessairement celle de l'endroit où les personnes concernées résident ou de l'endroit où la violation a eu lieu. Lorsqu'il

---

[30] Voir l'article 4, paragraphe 23, du RGPD.

[31] Voir également le considérant 122 du RGPD.

[32] Voir les lignes directrices du G29 sur la désignation d'une autorité de contrôle chef de file d'un responsable du traitement ou d'un sous-traitant disponibles à l'adresse suivante: http://ec.europa.eu/newsroom/document.cfm?doc_id=44102

[33] Une liste des coordonnées de toutes les autorités de protection des données nationales est disponible à l'adresse suivante: https://edpb.europa.eu/about-edpb/about-edpb/members_fr

notifie la violation à l'autorité de contrôle chef de file, le responsable du traitement devrait indiquer, le cas échéant, si la violation implique des établissements situés dans d'autres États membres et les États membres dans lesquels des personnes concernées sont susceptibles d'être affectées par la violation. Si le responsable du traitement a des doutes concernant l'identité de l'autorité de contrôle chef de file, il devrait, à tout le moins, informer l'autorité de contrôle locale de l'endroit où la violation s'est produite.

2. Violations dans des établissements de pays tiers

70. L'article 3 du RGPD concerne le champ d'application territorial du RGPD, y compris lorsqu'il s'applique au traitement de données à caractère personnel par un responsable du traitement ou un sous-traitant n'étant pas établi dans l'UE. Plus précisément, l'article 3, paragraphe 2, du RGPD énonce ce qui suit[34]:

> «*Le présent règlement s'applique au traitement des données à caractère personnel relatives à des personnes concernées qui se trouvent sur le territoire de l'Union par un responsable du traitement ou un sous-traitant qui n'est pas établi dans l'Union, lorsque les activités de traitement sont liées:*
>
> (a) *à l'offre de biens ou de services à ces personnes concernées dans l'Union, qu'un paiement soit exigé ou non desdites personnes; ou*
>
> (b) *au suivi du comportement de ces personnes, dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'Union*.»

71. L'article 3, paragraphe 3, du RGPD est également pertinent en la matière et dispose que[35]:

> «[l]*e présent règlement s'applique au traitement de données à caractère personnel par un responsable du traitement qui n'est pas établi dans l'Union mais dans un lieu où le droit d'un État membre s'applique en vertu du droit international public*».

72. Lorsqu'un responsable du traitement qui n'est pas établi dans l'UE est soumis à l'article 3, paragraphe 2, du RGPD ou à l'article 3, paragraphe 3, du RGPD et constate une violation, il est par conséquent toujours tenu de respecter les obligations de notification définies aux articles 33 et 34 du RGPD. L'article 27 du RGPD dispose qu'un responsable du traitement (ou un sous-traitant) doit désigner un représentant dans l'UE lorsque l'article 3, paragraphe 2, du RGPD s'applique.

73. Toutefois, la simple présence d'un représentant dans un État membre ne déclenche pas le système de guichet unique[36]. C'est pour cette raison que la violation devra être notifiée à chaque autorité de contrôle des États membres dans lesquels résident des personnes concernées. De telles notifications relèvent de la responsabilité du responsable du traitement[37].

---

[34] Voir également les considérants 23 et 24 du RGPD.

[35] Voir également le considérant 25.

[36] Voir les lignes directrices du G29 sur la désignation d'une autorité de contrôle chef de file d'un responsable du traitement ou d'un sous-traitant disponibles à l'adresse suivante: http://ec.europa.eu/newsroom/document.cfm?doc_id=44102

[37] Conformément aux lignes directrices 3/2018 relatives au champ d'application territorial du RGPD (article 3), disponibles à l'adresse https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_3_2018_territorial_scope_fr.pdf, le CEPD considère que la fonction d'un représentant dans l'Union n'est pas compatible avec le rôle d'un délégué à la protection des données (ci-après le «DPD») externe, de sorte que la responsabilité d'informer l'autorité de contrôle en cas de violation de données à caractère personnel continue d'incomber au responsable du traitement, conformément à l'article 27, paragraphe 5, du RGPD. Il est toutefois possible d'associer un représentant à la procédure de notification si cela a été explicitement stipulé dans le mandat écrit.

74. De la même façon, lorsqu'un sous-traitant est soumis à l'article 3, paragraphe 2, du RGPD il sera tenu de respecter les obligations incombant aux sous-traitants, et notamment l'obligation de notifier la violation au responsable du traitement conformément à l'article 33, paragraphe 2, du RGPD.

D. Conditions dans lesquelles la notification n'est pas obligatoire

75. L'article 33, paragraphe 1, du RGPD indique clairement qu'une violation qui n'est «pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques» ne doit pas être notifiée à l'autorité de contrôle. Tel pourrait par exemple être le cas lorsque les données à caractère personnel sont déjà disponibles pour le public et qu'une divulgation desdites données n'est pas susceptible d'engendrer un risque pour les personnes concernées. Ceci contraste avec les obligations de notification s'appliquant aux fournisseurs de services de communications électroniques accessibles au public en vertu de la directive 2009/136/CE, qui dispose que toutes les violations pertinentes doivent être notifiées à l'autorité compétente.

76. Dans son avis 03/2014 sur la notification des violations[38], le G29 expliquait qu'une violation de la confidentialité de données à caractère personnel qui ont été chiffrées à l'aide d'un algorithme de pointe constituait tout de même une violation de données à caractère personnel, et que celle-ci devait être notifiée. Néanmoins, si la confidentialité de la clé de chiffrement est intacte – c.-à-d. que la clé 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 –, les données sont en principe incompréhensibles. La violation n'est donc pas susceptible de porter atteinte aux personnes concernées et n'aurait donc pas besoin de leur être communiquée[39]. Toutefois, même lorsque les données sont chiffrées, une perte ou une altération peut avoir des conséquences négatives pour les personnes concernées lorsque le responsable du traitement ne dispose pas de sauvegardes adéquates. Dans ce cas de figure, il convient de communiquer la violation aux personnes concernées, même si les données elles-mêmes ont fait l'objet de mesures de chiffrement adéquates.

77. Le G29 expliquait aussi que le même raisonnement s'appliquait dans les cas où les données à caractère personnel, telles les mots de passe, sont hachées et salées en mode sécurisé, où la valeur hachée a été calculée à l'aide d'une fonction de hachage à clé cryptographique de pointe, où la clé utilisée pour hacher les données n'a été compromise dans aucune violation de sécurité et où celle-ci 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.

78. Par conséquent, si les données à caractère personnel ont été rendues incompréhensibles pour tout tiers non autorisé et si les données en question constituent une copie ou qu'il en existe une sauvegarde, une violation de la confidentialité portant sur des données à caractère personnel correctement chiffrées ne doit pas être notifiée à l'autorité de contrôle. La raison en est qu'une telle violation est peu susceptible d'engendrer un risque pour les droits et libertés des personnes physiques. Cela signifie bien entendu que la personne concernée ne devra pas non plus être informée dès lors que la violation est peu susceptible d'engendrer un risque élevé. Il convient toutefois de garder à l'esprit que si la notification peut ne pas être requise dans un premier temps dans la mesure où il n'existe pas de risque probable pour les droits et libertés des personnes physiques, cet état des choses peut évoluer avec le temps, et le risque devra alors être réévalué. Par exemple, si l'on se rend ultérieurement compte que la clé est compromise ou si l'on découvre une vulnérabilité dans le logiciel de chiffrement, une notification pourrait toujours être nécessaire.

79. Il convient en outre de noter qu'une violation de données chiffrées ne disposant pas d'une sauvegarde constitue une violation de la disponibilité, ce qui pourrait engendrer un risque pour les personnes concernées et donc nécessiter une notification. De la même façon, une violation qui entraîne la perte

[38] Avis 03/2014 du G29 sur la notification des violations, , http://ec.europa.eu/justice/data-protection/article29/documentation/, opinion-recommendation/files/2014/wp213_en.pdf

[39] Voir également l'article 4, paragraphes 1 et 2, du règlement (UE) nº 611/2013.

de données chiffrées disposant d'une sauvegarde peut toujours constituer une violation à notifier en fonction de la période de temps nécessaire pour restaurer les données à partir de la sauvegarde en question et des conséquences de cette perte de disponibilité pour les personnes physiques. Comme indiqué à l'article 32, paragraphe 1, point c), du RGPD, un facteur de sécurité important est en effet l'existence de «*moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique*».

Exemple

Une violation qui ne nécessiterait aucune notification à l'autorité de contrôle serait la perte d'un appareil mobile chiffré de façon sécurisée et utilisé par le responsable du traitement et son personnel. Si la clé de chiffrement reste en la possession du responsable du traitement et que les données à caractère personnel affectées ne constituent pas une copie unique, celles-ci seraient inaccessibles à tout pirate. Cela signifie que la violation est peu susceptible d'engendrer un risque pour les droits et libertés des personnes concernées. Si, par la suite, il devient évident que la clé de chiffrement a été compromise ou que le logiciel ou algorithme de chiffrement est vulnérable, le risque pour les droits et libertés des personnes physiques s'en verra affecté et une notification pourra alors être nécessaire.

80. Cependant, si un responsable du traitement n'informe pas l'autorité de contrôle alors que les données n'ont pas été effectivement chiffrées de façon sécurisée, il se trouvera en situation de non-respect de l'article 33 du RGPD. Ainsi, en choisissant leur logiciel de chiffrement, les responsables du traitement devraient être particulièrement attentifs à la qualité et à la bonne application du chiffrement envisagé, s'assurer de comprendre le niveau de protection qu'il fournit effectivement et évaluer s'il convient aux risques potentiels. Les responsables du traitement devraient également connaître en détail le fonctionnement de leur produit de chiffrement. Par exemple, un appareil pourrait être crypté une fois éteint, mais pas lorsqu'il se trouve en mode veille. Certains produits de chiffrement disposent par ailleurs de «clés par défaut» qui doivent être modifiées par chaque client afin d'être efficaces. Le chiffrement pourrait également être considéré comme adéquat par des experts en sécurité au moment de sa mise en œuvre, mais pourrait être dépassé quelques années plus tard. Il ne serait alors plus certain que les données soient chiffrées de façon suffisante par le produit en question et que celui-ci fournit un niveau de protection approprié.

III. ARTICLE 34 – COMMUNICATION À LA PERSONNE CONCERNÉE

A. Informer les personnes concernées

81. Dans certains cas, en plus de notifier une violation à l'autorité de contrôle, le responsable du traitement est également tenu de la communiquer aux personnes concernées.

Aussi l'article 34, paragraphe 1, du RGPD dispose-t-il ce qui suit:

«[l]*orsqu'une violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique, le responsable du traitement communique la violation de données à caractère personnel à la personne concernée dans les meilleurs délais*».

82. Les responsables du traitement devraient garder à l'esprit que la notification à l'autorité de contrôle est obligatoire, à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques. En outre, lorsqu'une violation est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, ces dernières doivent également être informées. Le seuil à atteindre est par conséquent plus élevé pour la communication aux personnes concernées que pour la notification à l'autorité de contrôle, et toutes les violations ne devront donc pas être communiquées aux personnes concernées, ce qui les protège de notifications excessives et non nécessaires.

83. Le RGPD indique que la communication d'une violation aux personnes concernées devrait se faire «dans les meilleurs délais», c'est-à-dire aussi vite que possible. L'objectif principal de la notification aux personnes concernées est de fournir des informations spécifiques concernant les mesures qu'elles devraient prendre pour se protéger[40]. Comme précisé ci-dessus, en fonction de la nature de la violation et des risques engendrés, une communication rapide aidera les personnes concernées à prendre des mesures pour se protéger contre toute conséquence négative de la violation.

84. L'annexe B des présentes lignes directrices fournit une liste non exhaustive d'exemples de cas où une violation pourrait être susceptible d'engendrer un risque élevé pour les personnes concernées et, partant, de cas où un responsable du traitement devra notifier une violation aux personnes concernées.

B. Informations à fournir

85. Concernant la notification des personnes concernées, l'article 34, paragraphe 2, du RGPD dispose que:

> «[l]*a communication à la personne concernée visée au paragraphe 1 du présent article décrit, en des termes clairs et simples, la nature de la violation de données à caractère personnel et contient au moins les informations et mesures visées à l'article 33, paragraphe 3, points b), c) et d)*».

86. Conformément à cette disposition, le responsable du traitement devrait au moins fournir les informations suivantes:

- une description de la nature de la violation;
- le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact;
- une description des conséquences probables de la violation; et
- une description des mesures prises ou que le responsable du traitement propose de prendre pour remédier à la violation, y compris, le cas échéant, des mesures pour en atténuer les éventuelles conséquences négatives.

87. À titre d'exemple de mesures prises pour remédier à la violation et pour en atténuer les conséquences négatives, un responsable du traitement pourrait indiquer qu'après avoir notifié la violation à l'autorité de contrôle pertinente, il a reçu des conseils sur la gestion de la violation et l'atténuation de ses conséquences. Le responsable du traitement devrait également, le cas échéant, fournir des conseils spécifiques aux personnes affectées concernant la façon de se protéger des éventuelles conséquences négatives de la violation, par exemple en réinitialisant leurs mots de passe si les informations de connexion ont été compromises. Une fois encore, un responsable du traitement peut choisir de fournir des informations complémentaires à celles présentées ici comme nécessaires.

C. Contacter les personnes concernées

88. En principe, la violation devrait être communiquée aux personnes concernées directement, à moins que cela n'exige des efforts disproportionnés. Dans ce cas, il est plutôt procédé à une communication publique ou à une mesure similaire permettant aux personnes concernées d'être informées de manière tout aussi efficace [article 34, paragraphe 3, point c), du RGPD].

89. La communication d'une violation aux personnes concernées devrait se faire au moyen de messages dédiés ne contenant pas d'autres informations, telles que des comptes rendus réguliers, des bulletins d'informations ou des messages standard. La communication de la violation sera ainsi plus claire et transparente.

[40] Voir également le considérant 86 du RGPD.

90. De telles méthodes de communication transparente pourraient être des messages directs (p. ex. e-mail, SMS, message direct), des notifications ou des bannières bien visibles sur le site internet, des communications postales et des annonces bien visibles dans des médias imprimés. Une notification se limitant uniquement à un communiqué de presse ou à un blog d'entreprise ne constituerait pas une méthode efficace de communication d'une violation à une personne. Le CEPD recommande que les responsables du traitement choisissent une méthode qui maximise la probabilité que les informations soient communiquées comme il se doit à toutes les personnes concernées. En fonction des circonstances, cela peut impliquer que le responsable du traitement ait recours à plusieurs méthodes de communication, par opposition à un canal de contact unique.

91. Il pourrait également être nécessaire que les responsables du traitement veillent à ce que la communication soit accessible dans des formats alternatifs appropriés ainsi que dans les langues pertinentes afin que les personnes concernées soient en mesure de comprendre les informations qui leur sont communiquées. Par exemple, la langue utilisée lors des échanges habituels préalables avec une personne concernée sera généralement appropriée pour communiquer une violation à cette même personne. Toutefois, si la violation touche des personnes concernées avec lesquelles le responsable du traitement n'a jamais interagi par le passé, ou en particulier des personnes qui résident dans un État membre ou un pays non membre de l'UE autre que celui où est établi le responsable du traitement, une communication dans la langue locale devrait être appropriée, compte tenu des ressources nécessaires. L'objectif principal est d'aider les personnes concernées à comprendre la nature de la violation ainsi que les mesures qu'elles peuvent mettre en place pour se protéger.

92. Les responsables du traitement sont les mieux placés pour déterminer le canal le plus approprié afin de communiquer une violation aux personnes concernées, en particulier s'ils interagissent fréquemment avec leurs clients. Cependant, un responsable du traitement devrait bien évidemment se montrer prudent dans l'utilisation d'un canal de contact compromis par une violation, dès lors que ce canal pourrait également être utilisé par le pirate pour se faire passer pour le responsable du traitement.

93. Parallèlement, le considérant 86 du RGPD explique ce qui suit:

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

94. Les responsables du traitement pourraient dès lors contacter et consulter l'autorité de contrôle non seulement pour obtenir des conseils sur la façon d'informer les personnes concernées d'une violation conformément à l'article 34, mais également sur les messages adéquats à envoyer aux personnes concernées et sur la façon la plus appropriée de les contacter.

95. Parallèlement, le considérant 88 du RGPD indique que la notification d'une violation devrait «tenir compte des intérêts légitimes des autorités répressives lorsqu'une divulgation prématurée risquerait d'entraver inutilement l'enquête sur les circonstances de la violation des données à caractère personnel». Cela peut signifier que, dans certaines circonstances, lorsque cela se justifie et sur les conseils des autorités répressives, le responsable du traitement peut retarder la communication de la violation aux personnes concernées jusqu'au moment où cette communication n'entraverait plus une telle enquête. Passé ce délai, les personnes concernées devront toutefois toujours être informées dans les meilleurs délais.

96. Dans le cas particulier où le responsable du traitement n'est pas en mesure de communiquer une violation à une personne concernée car il ne dispose pas d'informations suffisantes pour la contacter, il devrait l'informer dès que raisonnablement possible (p. ex. lorsqu'une personne concernée exerce son droit d'accès à ses données à caractère personnel au titre de l'article 15 et fournit au responsable du traitement les informations complémentaires nécessaires afin de la contacter).

D. Conditions dans lesquelles la communication n'est pas obligatoire

97. L'article 34, paragraphe 3, du RGPD définit trois conditions dans lesquelles la communication aux personnes concernées n'est pas nécessaire en cas de violation, à savoir:

- le responsable du traitement a mis en œuvre les mesures techniques et organisationnelles appropriées afin de protéger les données à caractère personnel préalablement à la violation, en particulier les mesures qui rendent les données à caractère personnel incompréhensibles pour toute personne qui n'est pas autorisée à y avoir accès. Cela pourrait par exemple inclure la protection des données à caractère personnel au moyen d'un chiffrement de pointe ou par tokénisation;
- le responsable du traitement a pris, immédiatement après la violation, des mesures qui garantissent que le risque élevé pour les droits et libertés des personnes concernées n'est plus susceptible de se concrétiser. Par exemple, en fonction des circonstances du cas d'espèce, le responsable du traitement peut avoir immédiatement déterminé et pris des mesures contre la personne ayant accédé aux données à caractère personnel avant qu'elle n'ait pu les utiliser. Il convient cependant toujours de tenir compte des conséquences potentielles de toute violation de la confidentialité, toujours en fonction de la nature des données concernées;
- contacter les personnes concernées exigerait des efforts disproportionnés[41], par exemple si leurs coordonnées ont été perdues à la suite de la violation ou ne sont tout simplement pas connues. Par exemple, l'entrepôt d'un bureau de statistiques a été inondé et les documents contenant les données à caractère personnel n'existaient qu'en format papier. Dans un tel cas, le responsable du traitement doit procéder à une communication publique ou prendre une mesure similaire permettant aux personnes concernées d'être informées de manière tout aussi efficace. En cas d'efforts disproportionnés, des dispositions techniques pourraient également être envisagées afin que les informations concernant la violation soient disponibles sur demande, ce qui pourrait se révéler utile pour les personnes éventuellement affectées par la violation, mais que le responsable du traitement n'est pas en mesure de contacter par un autre biais.

98. Conformément au principe de responsabilité, les responsables du traitement devraient être en mesure de démontrer à l'autorité de contrôle qu'ils remplissent l'une ou plusieurs de ces conditions [42]. Il convient de garder à l'esprit que si la notification peut ne pas être requise dans un premier temps dans la mesure où il n'existe pas de risque pour les droits et libertés des personnes physiques, cet état des choses peut évoluer avec le temps, et le risque devra alors être réévalué.

99. Si un responsable du traitement décide de ne pas communiquer une violation aux personnes concernées, l'article 34, paragraphe 4, du RGPD explique que l'autorité de contrôle peut exiger de lui qu'il procède à cette communication si elle considère que la violation est susceptible d'engendrer un risque élevé pour les personnes concernées. Elle peut également au contraire considérer que les conditions visées à l'article 34, paragraphe 3, du RGPD sont remplies et qu'aucune communication aux personnes concernées n'est donc requise. Si l'autorité de contrôle juge que la décision de ne pas

[41] Voir les lignes directrices du G29 sur la transparence, qui aborderont la problématique des efforts disproportionnés, disponible à l'adresse suivante: http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48850

[42] Voir l'article 5, paragraphe 2, du RGPD.

informer les personnes concernées n'est pas fondée, elle peut par ailleurs envisager de recourir aux pouvoirs et sanctions à sa disposition.

IV. ÉVALUATION DE L'EXISTENCE D'UN RISQUE OU D'UN RISQUE ÉLEVÉ

A. Le risque en tant que déclencheur de la notification

100. Bien que le RGPD introduise l'obligation de notifier une violation, celle-ci ne s'impose pas en toutes circonstances:

- la notification à l'autorité de contrôle compétente est obligatoire à moins qu'une violation soit peu susceptible d'engendrer un risque pour les droits et libertés des individus;
- la communication d'une violation aux personnes concernées ne devient nécessaire que lorsque ladite violation est susceptible d'engendrer un risque élevé pour leurs droits et libertés.

101. Cela signifie qu'immédiatement après avoir pris connaissance d'une violation, il est crucial que le responsable du traitement ne cherche pas uniquement à endiguer l'incident, mais qu'il évalue également le risque qui pourrait en résulter. Il y a deux raisons principales à cela: premièrement, si le responsable du traitement connaît la probabilité et la gravité potentielle des conséquences pour les personnes concernées, cela l'aidera à prendre des mesures efficaces pour endiguer et remédier à la violation; deuxièmement, cela l'aidera à déterminer s'il est tenu d'informer l'autorité de contrôle et, le cas échéant, les personnes concernées.

102. Comme expliqué plus haut, la notification d'une violation est obligatoire à moins que cette violation soit peu susceptible d'engendrer un risque pour les droits et libertés des individus, tandis que la communication d'une violation aux personnes concernées ne devient nécessaire que lorsque ladite violation est susceptible d'engendrer un risque *élevé* pour leurs droits et libertés. Un tel risque existe lorsqu'une violation est susceptible d'engendrer des dommages physiques, matériels ou un préjudice moral pour les personnes dont les données ont fait l'objet de la violation. Des exemples de tels dommages sont la discrimination, le vol ou l'usurpation d'identité, la perte financière ou l'atteinte à la réputation. Lorsque la violation implique des données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, la religion ou les convictions philosophiques, l'appartenance syndicale, ou des données génétiques, des données concernant la santé ou des données concernant la vie sexuelle ou des données relatives à des condamnations pénales et à des infractions, ou encore à des mesures de sûreté connexes, de tels dommages sont considérés comme susceptibles de se produire[43].

B. Les facteurs à prendre en compte lors de l'évaluation du risque

103. Les considérants 75 et 76 du RGPD indiquent qu'en général, lors de l'évaluation du risque, il convient de tenir compte à la fois de la probabilité et de la gravité du risque pour les droits et libertés des personnes concernées. Ils disposent en outre que le risque devrait faire l'objet d'une évaluation objective.

104. Il est à noter que l'évaluation du risque présenté par une violation pour les droits et libertés des personnes concernées se fait selon une approche différente de celle adoptée dans le cadre d'une AIPD[44]. L'AIPD envisage en effet autant les risques encourus si le traitement des données est effectué comme prévu que les risques en cas de violation. Dans le cadre de son appréciation d'une éventuelle

[43] Voir les considérants 75 et 85 du RGPD.

[44] Voir les lignes directrices du G29 sur les AIPD à l'adresse suivante: http://ec.europa.eu/newsroom/document.cfm?doc_id=44137

violation, une telle analyse évalue de façon générale la probabilité d'une telle violation ainsi que les dommages qu'elle pourrait engendrer pour les personnes concernées; il s'agit, en d'autres termes, de l'évaluation d'un incident hypothétique. En cas de violation réelle, l'incident s'est déjà produit et l'accent est donc entièrement mis sur le risque présenté par la violation pour les personnes concernées.

Exemple

Une AIPD considère que l'utilisation envisagée d'un logiciel de sécurité donné afin de protéger les données à caractère personnel constitue une mesure appropriée pour assurer un niveau de sécurité adapté au risque que le traitement présenterait pour les personnes concernées sans ledit logiciel. Toutefois, si le logiciel révélait ultérieurement une vulnérabilité, cela changerait sa capacité à limiter le risque pour les données à caractère personnel protégées et il devrait donc être réévalué dans le cadre d'une AIPD continue. Cette vulnérabilité est ensuite exploitée et une violation se produit. Le responsable du traitement devrait évaluer les circonstances spécifiques de la violation, les données concernées et la gravité potentielle des conséquences pour les personnes concernées, ainsi que la probabilité que le risque se concrétise.

105. En évaluant le risque présenté par une violation pour les personnes concernées, le responsable du traitement devrait par conséquent tenir compte des circonstances spécifiques de la violation, y compris la gravité des conséquences potentielles et la probabilité que celles-ci se produisent. Le CEPD recommande donc que l'évaluation tienne compte des critères suivants[45]:

- **Le type de violation**

106. Le type de la violation survenue peut avoir une incidence sur le niveau de risque encouru par les personnes concernées. Par exemple, les conséquences d'une violation de la confidentialité dans le cadre de laquelle des informations médicales ont été divulguées à des parties non autorisées pourraient différer de celles engendrées par une violation dans le cadre de laquelle les informations médicales d'un patient ont été perdues ou ne sont plus disponibles.

- **La nature, le caractère sensible et le volume des données à caractère personnel**

107. De toute évidence, l'un des facteurs clés dans l'évaluation du risque est le type et le caractère sensible des données à caractère personnel qui ont été compromises par la violation. En général, plus les données sont sensibles, plus le risque de dommage sera élevé pour les personnes concernées, mais il convient également de tenir compte des autres données à caractère personnel qui pourraient déjà être disponibles au sujet de la personne concernée. Par exemple, dans des circonstances normales, la divulgation du nom et de l'adresse d'une personne est peu susceptible d'entraîner un préjudice important. Par contre, si le nom et l'adresse d'un parent adoptif sont divulgués à un parent biologique, les conséquences pourraient être considérables à la fois pour le parent adoptif et pour l'enfant.

108. Si, prises individuellement, des violations portant sur des données relatives à la santé, des documents d'identité ou des données financières, telles que des données de carte de crédit, peuvent nuire à la personne concernée, prises ensemble, elles pourraient être utilisées pour une usurpation d'identité. La combinaison de données à caractère personnel est ainsi généralement plus sensible que chaque type de données à caractère personnel pris séparément.

[45] L'article 3, paragraphe 2, du règlement (UE) nº 611/2013 fournit des orientations sur les facteurs qui devraient être pris en compte pour ce qui est de la notification des violations dans le secteur des services de communications électroniques et pouvant être utiles dans le cadre de la notification en vertu du RGPD. Voir http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:173:0002:0008:fr:PDF

109. Si certains types de données à caractère personnel peuvent sembler, au premier abord, relativement inoffensifs, il convient tout de même d'évaluer minutieusement ce que les données pourraient révéler sur la personne concernée. Une liste de clients acceptant des livraisons régulières n'est a priori pas particulièrement sensible, mais ces mêmes données concernant des clients ayant demandé à ce que leurs livraisons soient interrompues lorsqu'ils partent en vacances constitueraient des informations utiles aux yeux de criminels.

110. De la même façon, si une petite quantité de données à caractère personnel hautement sensibles peut avoir d'importantes conséquences pour la personne concernée, un grand nombre de détails peut révéler une quantité d'informations plus grande encore au sujet de cette même personne. Une violation touchant de gros volumes de données à caractère personnel au sujet de très nombreuses personnes peut ainsi avoir des conséquences pour un tout aussi grand nombre de personnes.

- **La facilité d'identification des personnes concernées**

111. Un facteur important à prendre en compte est la facilité avec laquelle une partie ayant accès à des données à caractère personnel compromises peut identifier des individus spécifiques ou associer les données en question à d'autres informations afin d'identifier ces mêmes individus. Dans certaines circonstances, une identification pourrait être possible directement à partir des données à caractère personnel compromises, sans que des recherches spécifiques ne soient nécessaires pour découvrir l'identité de la personne concernée, tandis que dans d'autres, il pourrait être extrêmement difficile d'attribuer des données à caractère personnel à une personne spécifique, bien que cela puisse toujours être possible dans certaines conditions. Une identification peut être directement ou indirectement possible à partir des données compromises, comme elle peut dépendre des circonstances spécifiques de la violation et de la disponibilité publique de renseignements personnels connexes. Cette dernière éventualité serait plus pertinente en cas de violation de la confidentialité ou de la disponibilité.

112. Comme indiqué plus haut, les données à caractère personnel protégées par un niveau de chiffrement approprié seront incompréhensibles pour tout tiers non autorisé sans la clé de déchiffrement. En outre, une pseudonymisation correctement mise en œuvre (définie à l'article 4, paragraphe 5, du RGPD comme «*le traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable*») peut également réduire la probabilité que des personnes physiques soient identifiées en cas de violation. Les techniques de pseudonymisation ne peuvent néanmoins pas être considérées comme suffisantes à elles seules pour rendre les données incompréhensibles.

- **La gravité des conséquences pour les personnes concernées**

113. En fonction de la nature des données à caractère personnel impliquées dans une violation, par exemple des catégories particulières de données, les dommages potentiels pour les personnes concernées peuvent être particulièrement graves, notamment lorsque la violation pourrait entraîner un vol ou une usurpation d'identité, un préjudice physique, une détresse psychologique, une humiliation ou une atteinte à la réputation. Si la violation concerne des données à caractère personnel de personnes vulnérables, celles-ci pourraient être exposées à un plus grand risque de dommages.

114. Le fait que le responsable du traitement ait connaissance ou non de ce que des données à caractère personnel se trouvent en la possession de personnes dont les intentions sont inconnues ou potentiellement malicieuses peut avoir une incidence sur le niveau de risque potentiel. Prenons le cas d'une violation de la confidentialité dans le cadre de laquelle des données à caractère personnel ont été accidentellement divulguées à un tiers, tel que défini à l'article 4, paragraphe 10, ou à un autre destinataire. Une telle situation peut par exemple se produire lorsque des données à caractère personnel sont envoyées par erreur au mauvais service d'une organisation ou à un organisme fournisseur fréquemment sollicité. Le responsable du traitement peut demander au destinataire de lui

renvoyer les données reçues ou de les détruire de façon sécurisée. Dans les deux cas, dès lors que le responsable du traitement entretient une relation continue avec le destinataire et qu'il pourrait avoir connaissance de ses procédures, de ses antécédents et de toute autre information pertinente, ce dernier peut être considéré comme «fiable». En d'autres termes, le responsable du traitement peut disposer d'un certain degré de confiance envers le destinataire, de manière à pouvoir raisonnablement s'attendre à ce que ce dernier ne lise pas les données envoyées par erreur ou n'y accède pas et à ce qu'il satisfasse à sa demande de les lui renvoyer. Quand bien même le destinataire aurait accédé aux données, le responsable du traitement pourrait toujours être convaincu qu'il n'entreprendra aucune autre action par rapport à celles-ci et qu'il les lui renverra rapidement et coopérera pour assurer leur récupération. Dans de tels cas, le responsable du traitement peut tenir compte de ce facteur dans son évaluation du risque présenté par la violation. Si le fait que le destinataire est considéré comme fiable peut neutraliser la gravité des conséquences de la violation, cela ne signifie en effet pas pour autant qu'aucune violation ne s'est produite. La probabilité que ladite violation engendre un risque pour les personnes concernées peut en revanche s'en voir invalidée et il ne serait dès lors plus nécessaire de la notifier à l'autorité de contrôle ou aux personnes concernées. Encore une fois, tout dépendra des circonstances spécifiques de chaque violation. Le responsable du traitement devra cependant toujours conserver les renseignements relatifs à la violation dans le cadre de son obligation générale de tenir des registres des violations (voir le chapitre V ci-après).

115. Il convient également de tenir compte de la permanence des conséquences pour les personnes concernées, celles-ci pouvant être considérées comme plus importantes si elles ont un effet à long terme.

- **Les caractéristiques particulières des personnes concernées**

116. Une violation peut toucher des données à caractère personnel concernant des enfants ou d'autres personnes vulnérables, qui pourraient alors être exposés à un risque plus important. D'autres facteurs spécifiques aux personnes concernées pourraient également affecter la gravité des conséquences de la violation pour les personnes en question.

- **Les caractéristiques particulières du responsable du traitement**

117. La nature et le rôle du responsable du traitement ainsi que de ses activités peuvent affecter le niveau de risque qu'engendre une violation pour les personnes concernées. Par exemple, dès lors qu'une organisation médicale traite des catégories particulières de données à caractère personnel, le risque pour les personnes concernées sera plus important en cas de violation de données à caractère personnel que s'il s'agissait d'une liste de diffusion d'un journal.

- **Le nombre de personnes concernées**

118. Une violation peut toucher uniquement une personne, un nombre restreint de personnes ou des milliers de personnes, voire davantage. En général, plus le nombre de personnes concernées est élevé, plus les conséquences potentielles d'une violation sont nombreuses. Une violation peut cependant également avoir de graves conséquences ne serait-ce que pour une seule personne en fonction de la nature des données à caractère personnel et du contexte dans lequel elles ont été compromises. La solution consiste à nouveau à évaluer la probabilité et la gravité des conséquences pour les personnes concernées.

- **Éléments généraux**

119. Lorsqu'il évalue le risque susceptible de résulter d'une violation, le responsable du traitement devrait ainsi examiner à la fois la gravité des conséquences potentielles pour les droits et libertés des personnes concernées et la probabilité que ces conséquences se produisent. Il est évident que lorsque les conséquences d'une violation sont potentiellement plus graves, le risque est plus élevé. De même, lorsque la probabilité que celles-ci se produisent est plus importante, le risque s'en verra également renforcé. En cas de doute, le responsable du traitement devrait opter pour la prudence et procéder à

une notification. L'annexe B fournit une série d'exemples utiles de différents types de violations représentant un risque ou un risque élevé pour les personnes concernées.

120. L'Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information (ENISA) a publié des recommandations relatives à la méthodologie à adopter pour évaluer la gravité d'une violation que les responsables du traitement et les sous-traitants pourraient trouver utiles lors de la conception de leur plan de réaction et d'intervention en cas de violation[46].

V. RESPONSABILITÉ ET TENUE DE REGISTRES

A. Documenter les violations

121. Qu'une violation doive être notifiée à l'autorité de contrôle ou non, le responsable du traitement est tenu de documenter toutes les violations, comme expliqué à l'article 33, paragraphe 5, du RGPD:

> «*Le responsable du traitement documente toute violation de données à caractère personnel, en indiquant les faits concernant la violation des données à caractère personnel, ses effets et les mesures prises pour y remédier. La documentation ainsi constituée permet à l'autorité de contrôle de vérifier le respect du présent article*.»

122. Cette obligation de documentation est liée au principe de responsabilité du RGPD figurant à l'article 5, paragraphe 2, dudit règlement. Cette exigence de tenir des registres des violations, qu'elles soient sujettes à notification ou non, est également liée aux obligations du responsable du traitement au titre de l'article 24 du RGPD, et l'autorité de contrôle peut demander à voir lesdits registres. Les responsables du traitement sont donc encouragés à établir un registre interne des violations, qu'ils soient tenus de les notifier ou non[47].

123. S'il appartient au responsable du traitement de déterminer la méthode et la structure à utiliser pour documenter une violation, certaines informations clés devraient être incluses en toutes circonstances. Comme requis à l'article 33, paragraphe 5, du RGPD, le responsable du traitement doit reprendre des informations concernant la violation, y compris les causes, les faits et les données à caractère personnel concernées. Il devrait également inclure les effets et les conséquences de la violation ainsi que les mesures prises par le responsable du traitement pour y remédier.

124. Le RGPD ne définit pas la période de conservation d'une telle documentation. Lorsque de tels registres contiennent des données à caractère personnel, il incombera au responsable du traitement de déterminer la période de conservation appropriée conformément aux principes liés au traitement de données à caractère personnel[48] et au fondement juridique du traitement[49]. Il devra conserver cette documentation conformément à l'article 33, paragraphe 5, du RGPD dès lors que l'autorité de contrôle pourrait la réclamer à titre de preuve du respect dudit article, ou plus généralement du principe de responsabilité. De toute évidence, si les registres en eux-mêmes ne contiennent pas de données à caractère personnel, le principe de limitation de la conservation[50] du RGPD ne s'applique pas.

---

[46] ENISA, Recommendations for a methodology of the assessment of severity of personal data breaches, https://www.enisa.europa.eu/publications/dbn-severity

[47] Le responsable du traitement peut décider de documenter les violations dans le cadre de son registre des activités de traitement tenu conformément à l'article 30 du RGPD. Un registre séparé n'est pas nécessaire, à condition que les informations concernant les violations soient clairement identifiables en tant que telles et puissent être extraites sur demande.

[48] Voir l'article 5 du RGPD.

[49] Voir les articles 6 et 9 du RGPD.

[50] Voir l'article 5, paragraphe 1, point e), du RGPD.

125. Outre ces informations, le CEPD recommande que le responsable du traitement documente également le raisonnement justifiant les décisions prises en réaction à la violation. En particulier, lorsqu'une violation n'est pas notifiée, la justification de cette décision devrait être documentée. Cette justification devrait inclure les raisons pour lesquelles le responsable du traitement considère que la violation est peu susceptible d'engendrer un risque pour les droits et libertés des individus[51]. Si le responsable du traitement considère que l'une des conditions visées à l'article 34, paragraphe 3, du RGPD est remplie, il devrait également pouvoir fournir des éléments de preuve appropriés à cet égard.

126. Lorsque le responsable du traitement ne notifie pas une violation à l'autorité de contrôle, mais que la notification est retardée, le responsable du traitement doit être en mesure de fournir les raisons d'un tel retard; une documentation à cet égard pourrait contribuer à démontrer que le retard de notification est bien justifié et n'est pas excessif.

127. Lorsque le responsable du traitement communique une violation aux personnes concernées, il devrait être transparent en ce qui concerne la violation en question et communiquer de façon efficace et en temps utile. Conserver la trace d'une telle communication aiderait ainsi le responsable du traitement à démontrer son respect du principe de responsabilité et du RGPD en général.

128. Dans le but de favoriser leur conformité avec les articles 33 et 34 du RGPD, il serait bénéfique à la fois pour les responsables du traitement et les sous-traitants de disposer d'une procédure de notification documentée définissant la procédure à suivre lorsqu'une violation est détectée, y compris concernant la façon d'endiguer, de gérer et de remédier à l'incident, d'évaluer le risque et de notifier la violation. À cet égard, toujours afin de prouver leur conformité avec le RGPD, il pourrait être utile de démontrer que les employés ont été informés de l'existence de tels mécanismes et procédures et qu'ils savent comment réagir en cas de violation.

129. Il convient de noter qu'en cas de manquement à cette obligation de documenter correctement une violation, l'autorité de contrôle pourrait exercer ses pouvoirs au titre de l'article 58 du RGPD et/ou imposer une amende administrative conformément à l'article 83 du RGPD.

B. Rôle du délégué à la protection des données

130. Un responsable du traitement ou un sous-traitant peut disposer d'un délégué à la protection des données (DPD)[52] comme exigé à l'article 37 du RGPD ou sur une base volontaire à titre de bonne pratique. L'article 39 du RGPD définit un certain nombre de tâches obligatoires pour le DPD, mais n'interdit nullement que d'autres tâches lui soient attribuées par le responsable du traitement si nécessaire.

131. Les tâches imposées au DPD et présentant un intérêt particulier pour la notification des violations comprennent, entre autres, celle d'informer et de conseiller le responsable du traitement ou le sous-traitant en matière de protection des données, de contrôler le respect du RGPD et de dispenser des conseils en ce qui concerne l'AIPD. Le DPD doit également coopérer avec l'autorité de contrôle et faire office de point de contact pour celle-ci ainsi que pour les personnes concernées. Il convient également de noter que, lors de la notification d'une violation à l'autorité de contrôle, l'article 33, paragraphe 3, point b), du RGPD exige du responsable du traitement qu'il communique le nom et les coordonnées de son DPD ou d'un autre point de contact.

132. Pour ce qui est de la documentation des violations, le responsable du traitement ou le sous-traitant pourrait solliciter l'avis de son DPD concernant la structure, l'organisation et l'administration d'une telle documentation. Le DPD pourrait également être chargé de tenir de tels registres.

---

[51] Voir le considérant 85 du RGPD.

[52] Voir les lignes directrices du G29 concernant les DPD à l'adresse suivante: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

133. Ces tâches indiquent que le DPD devrait jouer un rôle clé dans la prévention des violations et la préparation à une violation en fournissant des conseils et en contrôlant le respect du RGPD, ainsi que lors d'une telle violation (p. ex. lors de la notification à l'autorité de contrôle) et durant l'enquête subséquente de l'autorité de contrôle. À cet égard, le comité européen pour la protection des données recommande que le DPD soit rapidement informé de l'existence d'une violation et participe à la gestion et au processus de notification de la violation.

VI. OBLIGATIONS DE NOTIFICATION EN VERTU D'AUTRES INSTRUMENTS JURIDIQUES

134. Outre la notification et la communication au titre du RGPD, et indépendamment de celles-ci, les responsables du traitement devraient également avoir connaissance de toute obligation de notification d'incidents de sécurité pouvant s'appliquer en vertu d'autres législations associées, ainsi que de la possibilité qu'ils soient ainsi tenus de notifier parallèlement à l'autorité de contrôle une violation de données à caractère personnel. De telles obligations peuvent varier d'un État membre à l'autre. Des exemples d'obligations de notification définies par d'autres instruments juridiques et de la façon dont celles-ci interagissent avec le RGPD peuvent toutefois être trouvés ci-dessous:

- *Règlement (UE) nº 910/2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur (règlement eIDAS)*[53].

135. L'article 19, paragraphe 2, du règlement eIDAS exige des prestataires de services de confiance qu'ils notifient à l'organe de contrôle toute atteinte à la sécurité ou toute perte d'intégrité ayant une incidence importante sur le service de confiance fourni ou sur les données à caractère personnel qui y sont conservées. Le cas échéant – c.-à-d. lorsqu'une telle atteinte ou perte constitue une violation de données à caractère personnel en vertu du RGPD – le prestataire de services de confiance devrait également avertir l'autorité de contrôle.

- *Directive (UE) 2016/1148 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union (directive SRI)*[54].

136. Les articles 14 et 16 de la directive SRI exigent des opérateurs de services essentiels et des fournisseurs de service numérique qu'ils notifient tout incident à leur autorité compétente. Le considérant 63 de la directive SRI[55] reconnaît que dans de nombreux cas, des données à caractère personnel peuvent être compromises à la suite d'incidents. Si la directive en question prévoit que les autorités compétentes et les autorités de contrôle coopèrent et échangent des informations dans ce cadre, il n'en reste pas moins que lorsque de tels incidents sont, ou deviennent, des violations de données à caractère personnel en vertu du RGPD, ces opérateurs et/ou fournisseurs sont tenus d'avertir l'autorité de contrôle indépendamment des exigences de notification des incidents définies par la directive SRI.

Exemple

Un fournisseur de services en nuage qui notifie une violation en vertu de la directive SRI pourrait également devoir la notifier à un responsable du traitement si ladite violation comprend une violation de données à caractère personnel. De la même façon, un prestataire de services de confiance au sens

[53] Voir http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.FRA

[54] Voir http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.FRA

[55] Considérant 63: *«Dans de nombreux cas, des données à caractère personnel sont compromises à la suite d'incidents. Dans de telles circonstances, les autorités compétentes et les autorités chargées de la protection des données devraient coopérer et échanger des informations sur tous les aspects pertinents de la lutte contre toute atteinte aux données à caractère personnel à la suite d'incidents.»*

du règlement eIDAS peut également être tenu d'informer l'autorité chargée de la protection des données compétente en cas de violation.

- *Directive 2009/136/CE (directive «Droits des citoyens») et règlement (UE) nº 611/2013 (règlement relatif à la notification des violations).*

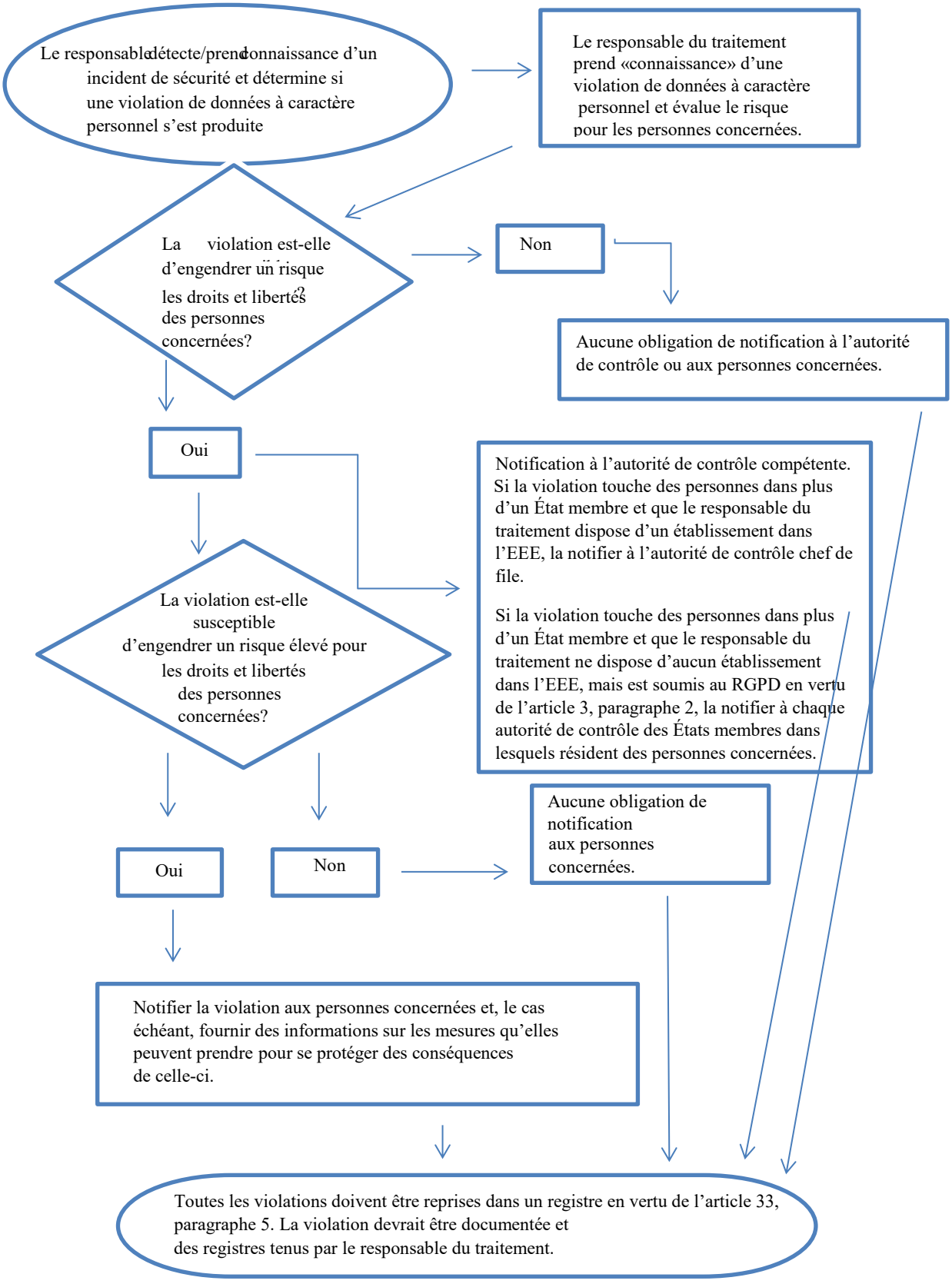
137. Les fournisseurs de services de communications électroniques accessibles au public au sens de la directive 2002/58/CE[56] sont tenus de notifier les violations aux autorités nationales compétentes.

138. Les responsables du traitement devraient également avoir connaissance de toute autre obligation de notification juridique, médicale ou professionnelle en vertu d'autres régimes applicables.

[56] Le 10 janvier 2017, la Commission européenne a proposé un règlement concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques, qui remplacera la directive 2009/136/CE et supprimera les exigences de notification de celle-ci. Toutefois, en attendant l'approbation de cette proposition par le Parlement européen, l'obligation de notification existante reste en vigueur, voir https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electroniccommunications

VII. ANNEXE

A. Organigramme indiquant les obligations de notification



B. Exemples de violations de données à caractère personnel et à qui les notifier

Les exemples suivants, non exhaustifs, aideront les responsables du traitement à déterminer si l'obligation de notification s'applique dans différents cas de violation de données à caractère personnel. Ces exemples peuvent également aider à distinguer un risque d'un risque élevé pour les droits et libertés des personnes concernées.

	Exemple	Notifier la violation à l'autorité de contrôle	Notifier la violation aux personnes concernées	Notes/recommandations
i	Un responsable du traitement a stocké une sauvegarde d'une archive de données à caractère personnel chiffrées sur une clé USB. La clé est volée lors d'un cambriolage.	Non	Non	Tant que les données sont chiffrées à l'aide d'un algorithme de pointe, que des sauvegardes des données existent, que la clé unique n'est pas compromise et que les données peuvent être restaurées en temps utile, cette violation peut ne pas devoir être notifiée. Si les données sont en revanche ultérieurement compromises, la notification est nécessaire.
ii	Un responsable du traitement assure un service en ligne. À la suite d'une cyberattaque sur ce service, des données à caractère personnel de personnes physiques en sont soutirées. Le responsable du traitement n'a de clients que dans un seul État membre.	Oui, avertir l'autorité de contrôle en cas de conséquences probables pour les personnes concernées.	Oui, avertir les personnes concernées en fonction de la nature des données à caractère personnel concernées et si la gravité des conséquences probables pour celles-ci est élevée.	
iii	Une courte panne de courant de quelques minutes dans le centre d'appel d'un responsable du traitement empêche les clients d'appeler ce dernier et d'accéder à leurs dossiers.	Non	Non	Pas d'obligation de notifier la violation, mais l'incident doit être documenté en vertu de l'article 33, paragraphe 5. Des registres appropriés devraient être tenus par le responsable du traitement.

iv	Un responsable du traitement est victime d'une cyberattaque au moyen d'un rançongiciel qui chiffre toutes ses données. Aucune sauvegarde n'est disponible et les données ne peuvent pas être restaurées. L'enquête révèle que la seule fonctionnalité du rançongiciel était de chiffrer les données et qu'aucun autre programme malveillant n'est présent dans le système.	Oui, avertir l'autorité de contrôle en cas de conséquences probables pour les personnes concernées, dès lors qu'il s'agit d'une perte de disponibilité.	Oui, avertir les personnes concernées en fonction de la nature des données à caractère personnel concernées et des conséquences potentielles de la perte de disponibilité des données, ainsi que des autres conséquences probables.	Si une sauvegarde avait été disponible et si les données avaient pu être restaurées en temps utile, il n'aurait pas été nécessaire de notifier la violation à l'autorité de contrôle ou aux personnes concernées dès lors qu'il n'y aurait pas eu de perte permanente de la disponibilité ou de la confidentialité. Toutefois, si l'autorité de contrôle prenait connaissance de l'incident par d'autres moyens, elle pourrait envisager de procéder à une enquête afin d'évaluer le respect des exigences de sécurité plus générales de l'article 32.
v	Une personne appelle le centre d'appel d'une banque pour signaler une violation de données. La personne en question a reçu le relevé mensuel d'une autre personne. Le responsable du traitement procède à une courte enquête (c.-à-d. terminée sous 24 heures), établit, avec un degré de certitude raisonnable, qu'une violation de données à caractère personnel s'est produite et signale l'existence potentielle d'un défaut systémique impliquant que d'autres personnes sont ou pourraient être affectées.	Oui	Seules les personnes concernées sont informées en cas de risque élevé et s'il est évident qu'aucune autre personne n'a été affectée.	Si, après une enquête complémentaire, on s'aperçoit que davantage de personnes sont concernées, il convient de notifier cette évolution à l'autorité de contrôle et de prendre des mesures complémentaires afin d'informer les autres personnes concernées en cas de risque élevé pour celles-ci.

vi	Un responsable du traitement gère un marché en ligne et a des clients dans plusieurs États membres. Le marché en question est victime d'une cyberattaque et les noms d'utilisateur, les mots de passe et les historiques d'achat sont publiés en ligne par le pirate.	Oui, informer l'autorité de contrôle chef de file si l'attaque concerne un traitement transfrontalier.	Oui, dès lors que l'attaque pourrait engendrer un risque élevé.	Le responsable devrait prendre des mesures, p. ex. en forçant la réinitialisation des mots de passe des comptes touchés, ainsi que d'autres mesures pour limiter le risque. Le responsable du traitement devrait également tenir compte d'autres obligations de notification, p. ex. en vertu de la directive SRI en tant que fournisseur de service numérique.
vii	Une entreprise d'hébergement de sites internet agissant en tant que sous-traitant détecte une erreur dans le code qui contrôle l'autorisation utilisateur. En raison de ce défaut, n'importe quel utilisateur peut accéder aux informations de compte de n'importe quel autre utilisateur.	En tant que sous-traitant, l'entreprise d'hébergement de sites internet doit avertir les clients concernés (les responsables du traitement) dans les meilleurs délais. En partant du principe que l'entreprise d'hébergement de sites internet a mené sa propre enquête, les responsables du traitement concernés devraient être relativement certains de l'occurrence éventuelle d'une violation, et ils seront probablement considérés comme ayant «pris connaissance» une fois que l'entreprise d'hébergement (le sous-traitant) les en aura informés. Le responsable du traitement doit alors informer l'autorité de contrôle.	Si la violation est peu susceptible d'entraîner un risque élevé pour les personnes concernées, il ne sera pas nécessaire de la leur notifier.	L'entreprise d'hébergement de sites internet (sous-traitant) doit également tenir compte d'autres obligations de notification (p. ex. en vertu de la directive SRI en tant que fournisseur de service numérique). S'il n'existe aucune preuve que cette vulnérabilité a été exploitée chez l'un des responsables du traitement de l'entreprise, il se pourrait que l'incident ne soit pas soumis à l'obligation de notification, mais il est probable qu'il doive être documenté ou qu'il soit le signe d'une non-conformité à l'article 32.
viii	Une cyberattaque rend indisponibles les dossiers médicaux d'un hôpital pendant 30 heures.	Oui, l'hôpital est tenu de le signaler à l'autorité de contrôle dès lors qu'un risque élevé pour le bien-être des patients et leur vie privée pourrait en résulter.	Oui, informer les personnes concernées.	

ix	Des données à caractère personnel d'un grand nombre d'étudiants sont envoyées par erreur à une mauvaise liste d'adresses contenant plus de 1 000 destinataires.	Oui, avertir l'autorité de contrôle.	Oui, avertir les personnes concernées en fonction de la portée et du type de données à caractère personnel concernées ainsi que de la gravité des conséquences potentielles.	
x	Un courrier électronique de marketing direct est envoyé aux destinataires dans les champs «à:» ou «cc:», permettant ainsi à chaque destinataire de voir l'adresse électronique des autres destinataires.	Oui, il pourrait être obligatoire de le notifier à l'autorité de contrôle si un grand nombre de personnes sont touchées, si des données sensibles sont révélées (p. ex. une liste d'adresses de patients d'un psychothérapeute) ou si d'autres facteurs présentent des risques élevés (p. ex. le courrier électronique contient les mots de passe initiaux).	Oui, avertir les personnes concernées en fonction de la portée et du type de données à caractère personnel concernées ainsi que de la gravité des conséquences potentielles.	La notification pourrait ne pas être nécessaire si aucune donnée sensible n'est révélée et si seul un nombre limité d'adresses électroniques a été divulgué.