EUROPEAN DATA PROTECTION SUPERVISOR

Lignes directrices sur les notifications de violations de données à caractère personnel

à l'intention des institutions et organes de l'Union européenne

21 novembre 2018

TABLE DES MATIÈRES

SYNTHÈSE

Les lignes directrices entendent présenter aux institutions et organes de l'Union européenne (ci-après «IUE») des **conseils pratiques** sur la manière de se conformer aux dispositions relatives aux violations de données à caractère personnel des articles 34 et 35 du règlement sur le traitement des données à caractère personnel par les IUE.

Le règlement intègre les principes du règlement général sur la protection des données [règlement (UE) 2016/679, ci-après le «RGPD»], y compris ceux relatifs aux violations de données à caractère personnel, dans les règles de protection des données applicables aux institutions de l'UE.

Les présentes lignes directrices exposent des recommandations et des bonnes pratiques en ce qui concerne la mise en œuvre de la responsabilité de la protection des données à caractère personnel en **aidant à évaluer et à gérer les risques relatifs à la protection des données, à la vie privée et à d'autres droits fondamentaux des personnes physiques en cas de violation de données à caractère personnel**. Elles rassemblent et consolident les conseils que le Contrôleur européen de la protection des données (CEPD) a prodigués aux IUE ces dernières années, au sujet des premiers appels d'offres interinstitutionnels par exemple.

Les présentes lignes directrices décrivent la démarche que les IUE devraient adopter pour réagir adéquatement en cas de violation de données à caractère personnel.

Le CEPD considère les bonnes pratiques mentionnées ci-après comme **une référence** lors de l'analyse du respect du règlement. Les IUE peuvent choisir d'autres mesures, également efficaces, que celles présentées dans le présent document, en fonction de leurs besoins spécifiques. Dans ce cas, ils devront démontrer de quelle manière ces mesures entraînent une protection équivalente des données à caractère personnel.

Les IUE devraient régulièrement procéder à une évaluation de leurs procédures en matière de violation de données à caractère personnel. L'évaluation a pour vocation de montrer que l'IUE en question peut en principe réagir efficacement pour prévenir ou réduire le risque de violation des données à caractère personnel à un niveau acceptable.

Les lignes directrices décrivent:

- en quoi consiste une violation de données à caractère personnel;

- comment évaluer une violation de données à caractère personnel;

- comment notifier une violation de données à caractère personnel au CEPD;

- comment communiquer une violation de données à la personne concernée;

- comment documenter une violation de données à caractère personnel.

En outre, les lignes directrices fournissent un modèle de formulaire de notification de violation de données à caractère personnel au CEPD par les institutions de l'UE.

1. Introduction

1 Les présentes lignes directrices ont pour objet de formuler des conseils pratiques à l'intention des institutions et organes de l'UE (ci-après les «IUE») afin qu'ils se conforment au règlement (UE) 2018/1725 (ci-après le «règlement»)[1], qui a remplacé le règlement (CE) nº 45/2001[2], en les aidant à réagir efficacement en cas de violations de données à caractère personnel. Le règlement introduit l'obligation, pour les IUE, d'informer le CEPD lorsqu'une violation de données à caractère personnel présente un risque pour les droits et libertés des personnes concernées et d'informer les personnes physiques dont les données ont été affectées par la violation en cas de risque élevé. Le règlement harmonise les règles de protection des données applicables aux IUE par rapport au règlement général sur la protection des données [règlement (UE) 2016/679, ci-après le «RGPD»][3] applicable dans les États membres de l'UE et de l'EEE aux entités des secteurs privé et public.

2 En tant qu'autorité de contrôle indépendante compétente pour le traitement des données à caractère personnel par les IUE, le CEPD peut, entre autres, publier des lignes directrices sur des questions spécifiques relatives au traitement des données à caractère personnel.

3 Ces lignes directrices devraient être prises en considération par les délégués à la protection des données (DPD) et les contacts ou coordinateurs de la protection des données (CPD), ainsi que par le personnel informatique et les autres services concernés par la sécurité informatique et physique, par exemple les responsables locaux de la sécurité informatique (RLSI) et les responsables locaux de la sécurité (RLS), ainsi que par tous les agents de l'IUE agissant en qualité de coresponsables du traitement et de sous-traitants. Elles permettront également aux membres de la direction d'encourager une culture de la protection des données depuis le sommet de l'organisation et d'appliquer le principe de responsabilité.

4 L'objectif des lignes directrices est de permettre aux IUE de remplir plus facilement leurs obligations en matière de gestion des violations de données à caractère personnel. Ces institutions et organes restent toutefois responsables du respect des obligations qui leur incombent conformément au principe de responsabilité. Les mesures recommandées dans les présentes lignes directrices permettent aux IUE de concevoir ou d'adapter leurs processus de gestion des violations de données à caractère personnel et de se conformer aux obligations de communication à l'égard du CEPD et des personnes concernées. Les IUE peuvent choisir d'autres mesures, également efficaces, que celles présentées dans les présentes lignes directrices, en fonction de leurs besoins spécifiques. Dans ce cas, ils devront démontrer de

[1] Règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) nº 45/2001 et la décision nº 1247/2002/CE, JO L 295 du 21.11.2018, p. 39; disponible à l'adresse suivante: https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=uriserv%3AOJ.L_.2018.295.01.0039.01.FRA.

[2] Règlement (CE) nº 45/2001 du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données (JO L 8 du 12.1.2001, p. 1).

[3] 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 (règlement général sur la protection des données), JO L 119 du 4.5.2016, p. 1; disponible à l'adresse suivante: http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=OJ:L:2016:119:FULL.

quelle manière ils entendent obtenir une protection équivalente des données à caractère personnel à l'aide de ces autres mesures.

5 Ces lignes directrices seront mises à jour à mesure que les IUE et le CEPD acquièrent de l'expérience et affinent leur pratique en matière de notification et de communication des violations de données à caractère personnel conformément au règlement. La mise à jour tiendra également compte d'une conception commune de la gravité des violations de données à caractère personnel et des risques pour les personnes dont les données ont été violées, élaborée en coopération avec les autorités chargées de la protection des données (APD) des États membres, et garantira la cohérence avec la pratique des APD des États membres en ce qui concerne l'application des dispositions du RGPD en matière de violations de données à caractère personnel.

2. Champ d'application et structure des lignes directrices

2.1. Champ d'application

6 Le règlement fixe les obligations des responsables du traitement des données au sein des IUE en ce qui concerne le traitement des données à caractère personnel relevant de leur responsabilité, et donne aux personnes physiques des droits juridiquement protégés en matière de protection des données.

7 Le traitement des données à caractère personnel par les systèmes d'information des IUE doit respecter pleinement le règlement.

8 Les lignes directrices indiquent comment réagir en cas de violation de données à caractère personnel afin de respecter les articles 34 et 35 du règlement.

9 Les lignes directrices expliquent la notification obligatoire des violations de données à caractère personnel et les exigences en matière de communication prévues par le règlement, ainsi que les mesures de base que les IUE, en tant que responsables du traitement et/ou sous-traitants, doivent prendre pour satisfaire à ces nouvelles obligations.

10 Les lignes directrices se concentrent sur les incidents de violation de données à caractère personnel et sur la manière dont les IUE doivent être prêts non seulement à réagir efficacement et conformément à leurs obligations légales, mais aussi à prévenir ces incidents de manière proactive.

11 Les procédures relatives aux violations de données ne remplacent aucun processus ou aucune procédure de traitement des incidents de sécurité et n'en prennent pas non plus le relais. Elles doivent au contraire être intégrées à ces processus ou procédures.

2.2. Structure

12 Les présentes lignes directrices sont structurées comme suit:

- le chapitre 1 présente l'objet des lignes directrices;
- le chapitre 2 définit le champ d'application et la structure du présent document;
- le chapitre 3 explique en quoi consiste une violation de données à caractère personnel;
- le chapitre 4 explique comment évaluer une violation de données à caractère personnel et les risques;
- le chapitre 5 explique comment notifier une violation de données à caractère personnel au CEPD;
- le chapitre 6 explique comment communiquer une violation de données à caractère personnel aux personnes concernées;
- le chapitre 7 explique comment documenter une violation de données à caractère personnel;
- l'annexe 1 présente le formulaire de notification;
- l'annexe 2 décrit des exemples pratiques;

- l’annexe 3 présente des références à d’autres documents utiles (avis, normes techniques, bonnes pratiques, etc.);
- l’annexe 4 comprend un glossaire;
- l’annexe 5 comprend un organigramme sur les exigences de notification des violations de données applicables aux IUE et présente un résumé des considérations pertinentes concernant les violations de données à caractère personnel.

13 Ce document ne traite pas/ne tient pas compte:

- de manière exhaustive des mesures de sécurité informatique pertinentes pour la détection et la limitation d’une violation de données à caractère personnel;
- des caractéristiques techniques et fonctionnelles de l’infrastructure des TI fournie pour empêcher une violation de données à caractère personnel, comme le type de serveurs, les applications et les plateformes logicielles, les dispositifs réseau, etc.

3. Violation de données à caractère personnel en vertu du règlement sur le traitement des données à caractère personnel par les institutions de l'UE

3.1. Contexte

14 La notification d'une violation de données à caractère personnel est une nouvelle obligation incombant aux IUE et reflète une obligation similaire introduite dans le cadre du RGPD. Cette notion avait été introduite pour la première fois par la directive relative à la vie privée et aux communications électroniques. Une violation de données à caractère personnel risquerait, si l'on n'intervenait pas à temps et de manière appropriée, de causer aux personnes physiques concernées des dommages physiques, matériels ou un préjudice moral.

15 Dans tous les cas, le responsable du traitement doit atténuer l'effet de toute violation de données à caractère personnel et en particulier son incidence sur les personnes concernées. Les responsables du traitement doivent adopter une procédure de traitement des violations de données à caractère personnel comprenant également la notification au CEPD et la communication aux personnes concernées, le cas échéant. La procédure de traitement des violations de données à caractère personnel ne remplace aucun autre processus ou aucune procédure de traitement des incidents et n'en prend pas non plus le relais. Concrètement, les responsables du traitement sont invités à intégrer des procédures de traitement des violations de données à caractère personnel dans leurs procédures de gestion des incidents liés à la sécurité de l'information. En outre, la procédure de traitement des violations de données à caractère personnel devrait être liée au plan de continuité des activités du responsable du traitement et, le cas échéant, aux activités menées par ses équipes de communication.

16 Afin de respecter les délais fixés par le règlement en ce qui concerne la notification et la communication des violations de données à caractère personnel, il est vivement conseillé aux responsables du traitement d'adopter une procédure en matière de violation de données à caractère personnel intégrant des stratégies d'atténuation. Cette procédure peut compléter les procédures/manuels de sécurité informatique existants. Tout le personnel doit être informé de cette obligation et des procédures connexes (par exemple, formation des nouveaux arrivants, exercice concernant l'ensemble du personnel).

17 Une violation de données à caractère personnel risque d'entraîner une série d'effets négatifs importants pour les personnes concernées, lesquels peuvent engendrer des dommages physiques, matériels ou un préjudice moral. Le RGPD et le règlement expliquent que cette violation peut inclure une perte de contrôle de leurs données à caractère personnel ou une limitation de leurs droits, une discrimination, un vol ou une usurpation d'identité, une perte financière, un renversement non autorisé du processus de pseudonymisation, une atteinte à la réputation, une perte de confidentialité de données protégées par le secret professionnel ou tout autre dommage économique ou social important pour les personnes concernées[4].

18 La notification des violations de données à l'autorité de contrôle et la communication aux personnes concernées sont devenues des obligations légales en vertu des articles 33 et 34 du RGPD et des articles 34 et 35 du règlement. Les notifications de violations de données sont des mesures visant à permettre aux personnes concernées de faire valoir leurs droits. Elles

[4] Considérant 85 du RGPD, considérant 46 du règlement.

renforcent par ailleurs la responsabilité des responsables du traitement (et des sous-traitants). Les notifications des violations de données visent à assurer une plus grande sécurité des données en Europe.

19 Dans le même temps, il convient de tenir dûment compte des circonstances de la violation concernée, y compris du fait que les données à caractère personnel étaient ou non protégées par des mesures de protection techniques appropriées, limitant efficacement la probabilité d'usurpation d'identité ou d'autres formes d'abus (considérant 88 du RGPD).

20 Bien que la directive 95/46/CE et le règlement (CE) nº 45/2001 n'aient pas abordé cette question, la notion de notification des violations de données n'est pas nouvelle dans la législation de l'Union. Par exemple, les fournisseurs de services de communications électroniques accessibles au public ont l'obligation de notifier les violations de données à caractère personnel aux autorités nationales compétentes et de tenir à jour un inventaire des violations de données, notamment de leur contexte, de leurs effets et des mesures prises pour y remédier (article 4 de la directive relative à la vie privée et aux communications électroniques)[5].

21 Au niveau national, avant même l'entrée en vigueur du RGPD, certains États membres ont adopté des mesures de gestion des violations de données. La loi fédérale allemande sur la protection des données a introduit l'obligation de notifier les violations de la confidentialité en 2009[6]. En 2011, l'Irlande a mis en place un code de bonnes pratiques en matière de violation de la sécurité des données à caractère personnel[7]. Entre 2014 et 2015, l'Italie a élaboré différents modèles de notification des violations de données en fonction du type de données concernées[8].

22 Compte tenu de l'importance de la notification et de la communication d'une violation des données à caractère personnel pour renforcer le droit des personnes concernées, accroître la responsabilité des responsables du traitement (et des sous-traitants) et favoriser la sécurité des données en Europe, le règlement introduit une obligation incombant aux responsables du traitement en cas de violation des données survenant au sein des IUE (ou chez leurs sous-traitants).

3.2. En quoi consiste une violation de données à caractère personnel?

23 **En vertu de l'article 3, paragraphe 16, du règlement,** une «violation de données à caractère personnel» désigne une violation de la sécurité entraînant, de manière accidentelle

---

[5] Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques), JO L 201 du 31.7.2002, p. 37, telle que modifiée par la directive 2009/136/CE du 25 novembre 2009, JO L 337 du 18.12.2009, texte consolidé disponible à l'adresse: https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:02002L0058-20091219

[6] Gesetz zur Änderung datenschutzrechtlicher Vorschriften vom 14.8.2009, BGBl. 2009 Teil I Nr. 54, p. 2814, disponible à l'adresse suivante: http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl109s2814.pdf.

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

[8] Pour les données de santé et les données biométriques: http://194.242.234.211/documents/10160/0/Linee+guida+in+materia+di+dossier+sanitario+-+Allegato+B.pdf; https://www.garanteprivacy.it/documents/10160/0/All+B+al+Provv.+513+del+12+novembre+2014+Mod.+segnalazione+data+breach.pdf.

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 sous la responsabilité des IUE, en qualité de responsables du traitement, ou l'accès non autorisé à de telles données;

24 Cette définition d'une violation de données à caractère personnel figurant dans le règlement est conforme à celle du RGPD[9].

25 Si le règlement est enfreint pour un motif différent (par exemple en raison de l'absence de base juridique adéquate pour une opération de traitement, d'une information inadéquate des personnes concernées, etc.), cette infraction ne relève pas des obligations liées à une violation de données à caractère personnel, même si cela reste une violation du règlement. Une violation de la sécurité de l'information qui ne compromet pas les données à caractère personnel ne relève pas non plus de cette obligation. Le caractère intentionnel éventuel de la violation n'a aucune incidence.

26 Tout incident lié à la sécurité de l'information n'est pas nécessairement une violation de données à caractère personnel, mais toute violation de données à caractère personnel est un incident lié à la sécurité de l'information.

27 Dans ses lignes directrices, qui ont été confirmées par le CEPD, le groupe de travail «article 29» («GT29»)[10] a défini trois types de violations de données à caractère personnel selon les trois principes bien connus de la sécurité de l'information:

- «violation de la confidentialité» – en cas de divulgation ou d'accès non autorisés ou accidentels à des données à caractère personnel, à savoir lorsqu'une entité non autorisée à disposer de ces connaissances obtient l'accès à ces données à caractère personnel;
- «violation de la disponibilité» – en cas de destruction ou de perte accidentelles ou non autorisées de l'accès à des données à caractère personnel, à savoir une perte du contrôle de l'accès à des données à caractère personnel ou une suppression inappropriée de données à caractère personnel; et
- «violation de l'intégrité» – en cas d'altération non autorisée ou accidentelle de données à caractère personnel, à savoir des modifications inadéquates de données à caractère personnel.

28 Une violation de données peut survenir pour un certain nombre de raisons, notamment:

a. une négligence,

b. un accident, ou

c. un acte intentionnel commis par des personnes internes ou externes.

[9] Article 4, paragraphe 12, du RGPD.

[10] Lignes directrices du GT29 sur la notification de violations de données à caractère personnel en vertu du règlement 2016/679, adoptées le 3 octobre 2017, révisées pour la dernière fois et adoptées le 6 février 2018, et disponibles à l'adresse suivante: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052. Ces lignes directrices ont été approuvées par le comité européen de la protection des données.

29 En résumé, toute violation de données à caractère personnel est un incident de sécurité[11] et peut concerner, en fonction des circonstances, une violation de la confidentialité, de l'intégrité ou de la disponibilité de données à caractère personnel, ainsi que toute combinaison de celles-ci. Parmi les causes des violations de données figurent la négligence, les accidents ou les défaillances techniques, ainsi que les actes intentionnels commis par des acteurs internes ou externes.

30 Voici quelques exemples de violations de données[12]:

a. des collaborateurs communiquant par erreur des données à caractère personnel à des destinataires erronés (par exemple, en envoyant un courriel aux mauvaises personnes ou en utilisant une liste de diffusion inadéquate);

b. l'utilisation de canaux non autorisés pour l'échange de données à caractère personnel;

c. le stockage d'informations sur un appareil non autorisé par des collaborateurs;

d. un sous-traitant accédant à des données à caractère personnel (par exemple, des données sur le personnel) sans autorisation préalable ou en violation des contrôles techniques;

e. des dossiers papier contenant des données à caractère personnel volés ou oubliés dans des bacs de recyclage ou des poubelles non sécurisés;

f. des collaborateurs accédant à des données à caractère personnel ou les divulguant en dehors du cadre de leur autorisation professionnelle;

g. le piratage de bases de données contenant des données à caractère personnel ou tout accès illicite à ces bases de données par des tiers en dehors du responsable du traitement;

h. la perte ou le vol d'ordinateurs portables, de téléphones mobiles, de dispositifs de stockage amovibles ou de dossiers papier contenant des données à caractère personnel.

31 La procédure de traitement des violations de données à caractère personnel ne remplace aucun processus ou aucune procédure de traitement des incidents et n'en prend pas non plus le relais. En fait, les IUE pourraient éventuellement intégrer des procédures de traitement des violations de données à caractère personnel dans leurs procédures de gestion des incidents liés à la sécurité de l'information. En outre, la procédure de traitement des violations de données à caractère personnel serait liée aux plans de sécurité du responsable du traitement et, le cas échéant, aux activités menées par ses équipes de communication.

[11] Tout incident lié à la sécurité de l'information n'est pas nécessairement une violation de données à caractère personnel, mais toute violation de données à caractère personnel est un incident lié à la sécurité de l'information.

[12] Des exemples supplémentaires figurent à l'annexe 2.

4. Comment évaluer une violation de données à caractère personnel (évaluation de risque et de risque élevé)?

32 L'article 34 du règlement suit l'approche fondée sur le risque adoptée par le RGPD. La gravité de la violation devra être évaluée au cas par cas. Le «risque pour les droits et libertés des personnes physiques» doit servir de base à l'examen de la réaction. Les risques déterminés lors d'une analyse d'impact relative à la protection des données (AIPD) préalable peuvent servir de point de départ.

33 Il convient d'évaluer quelles sont les violations de données comportant un risque et quelles sont celles comportant un risque élevé, étant donné que l'obligation de communiquer aux personnes concernées n'existe que dans le second cas.

34 Lors de l'évaluation d'un risque, il convient de tenir compte à la fois de la probabilité et de la gravité de l'effet négatif pour les droits et libertés des personnes concernées. Ensuite, le risque doit être apprécié sur la base d'une évaluation objective. En cas de violation effective, l'événement indésirable a déjà eu lieu, de sorte que l'évaluation porte uniquement sur l'incidence potentielle de la violation sur les droits et libertés des personnes physiques. Une partie de l'incidence peut s'être matérialisée dès la détection de la violation, une autre peut ne se concrétiser qu'ultérieurement (en cas de vol d'identifiants, par exemple, certains d'entre eux peuvent déjà avoir été utilisés, d'autres peuvent être utilisés par la suite).

35 Comme indiqué dans ce qui précède, une violation de données à caractère personnel est un incident de sécurité. Toutefois, tous les incidents de sécurité ne peuvent être considérés comme des violations de données à caractère personnel. La condition nécessaire pour considérer un incident de sécurité comme une violation de données à caractère personnel est la présence de données à caractère personnel.

36 Les présentes lignes directrices supposent qu'une IUE dispose d'un processus de gestion des incidents de sécurité bien établi, notamment en matière de déclaration. Il est de la plus haute importance de pouvoir déceler une violation de données à caractère personnel.

Tout incident lié à la sécurité de l'information n'est pas nécessairement une violation de données à caractère personnel, mais toute violation de données à caractère personnel est un incident lié à la sécurité de l'information.

Il convient, lors de l'évaluation de chaque incident signalé, de déterminer si des données à caractère personnel sont affectées.

Si des données à caractère personnel sont affectées, l'incident de sécurité est considéré comme une violation de données à caractère personnel.

37 Le délégué à la protection des données (DPD) est immédiatement consulté en présence d'une indication selon laquelle un incident de sécurité est susceptible d'avoir une incidence sur des données à caractère personnel.

Une fois que l'incident de sécurité est considéré comme une violation de données à caractère personnel, il convient d'évaluer quelle serait son incidence sur les droits et libertés des personnes concernées à l'étape suivante.

38 Une fois que l'incident de sécurité est considéré comme une violation de données à caractère personnel, l'IUE évalue l'incidence de la violation sur les droits et libertés des personnes concernées. Cette évaluation doit être aussi objective que possible. Cette étape est très critique, car elle définit les obligations de notification de l'IUE en tant que responsable du traitement.

L'IUE met en œuvre sa propre procédure de gestion des violations de données à caractère personnel ou un ensemble de politiques qui se concentreront sur l'analyse d'impact de chaque violation de données à caractère personnel signalée et sur le choix de la procédure de notification adéquate à l'égard du CEPD et des personnes concernées. Les rôles et les responsabilités sont clairement définis.

39 Il est de la plus haute importance que l'IUE veille à une évaluation correcte des risques, qui constituera l'élément déclencheur de la notification au CEPD et d'une éventuelle communication à une personne concernée.

Dans les cas où il est établi qu'une violation de données à caractère personnel enregistrée ne crée aucun risque pour les droits et libertés des personnes concernées, le responsable du traitement n'est pas tenu d'en informer le CEPD ni les personnes concernées. Toutefois, cette décision devrait être prise au niveau approprié et être adéquatement documentée, afin de permettre au CEPD de vérifier également la conformité de l'IUE pour les violations de données qui n'ont pas été notifiées.

40 L'IUE intègre, dans la procédure de gestion des violations de données ou dans une procédure distincte, des orientations ou une méthodologie échelonnée visant à évaluer objectivement le niveau de risque d'une violation de données à caractère personnel.

Conformément à l'article 34 du règlement, l'IUE doit notifier une violation de données à caractère personnel au Contrôleur européen de la protection des données au plus tard dans les 72 **heures**, à moins qu'elle ne soit pas susceptible d'engendrer un **risque** pour les droits et libertés des personnes.

En outre, conformément à l'article 35, paragraphe 1, du règlement, l'IUE doit également communiquer la violation de données à caractère personnel lorsqu'elle engendre un «**risque élevé**» pour les droits et libertés de la personne physique.

41 Dans tous les cas, le responsable du traitement doit atténuer les effets de toute violation de données à caractère personnel et, en particulier, son incidence sur les personnes concernées.

4.1. Évaluation des risques et des risques élevés

42 L'obligation de notification des violations de données reflète une approche fondée sur les risques.

La gravité de la violation devra être évaluée au cas par cas. Le «risque pour les droits et libertés des personnes physiques» doit servir de base à l'examen effectué lors de la réalisation d'une

évaluation. Les risques déterminés lors d'une AIPD préalable peuvent faire office de point de départ[13].

43 L'évaluation des violations de données présentant un risque et de celles présentant un risque élevé est pertinente pour l'obligation de notification et de communication. Si un risque n'est pas élevé, l'IUE n'en informe que le CEPD en qualité d'autorité de contrôle, alors qu'en cas de risque élevé, il est obligatoire d'informer également les personnes concernées.

44 Les considérants 46[14] et 47[15] du règlement disposent que l'évaluation d'un risque doit tenir compte à la fois de la probabilité et de la gravité du risque pour les droits et les libertés des personnes concernées. Ensuite, le risque doit être apprécié sur la base d'une évaluation objective. En cas de violation de données effective, l'événement s'est déjà produit, de sorte que l'attention du responsable du traitement porte uniquement sur l'incidence de la violation sur les personnes physiques.[16]

45 L'évaluation de l'incidence de la violation de données sur la personne concernée est importante, car elle aidera également l'IUE à prendre les mesures appropriées pour limiter et combattre la violation.

46 Conformément aux recommandations du GT29 dans ses lignes directrices, les facteurs à prendre en considération lors de l'évaluation des risques sont les suivants:

1. le type de violation;
2. la nature, le caractère sensible et le volume de données à caractère personnel;
3. la facilité d'identification des personnes concernées;
4. la gravité des conséquences pour les personnes concernées;

---

[13] Article 39 du règlement.

[14] «*Des risques pour les droits et libertés des personnes physiques, dont le degré de probabilité et de gravité varie, peuvent résulter du traitement de données à caractère personnel qui est susceptible d'entraîner des dommages physiques, matériels ou un préjudice moral, en particulier: lorsque le traitement peut donner lieu à une discrimination, à un vol ou une usurpation d'identité, à une perte financière, à une atteinte à la réputation, à une perte de confidentialité de données protégées par le secret professionnel, à un renversement non autorisé du processus de pseudonymisation ou à tout autre dommage économique ou social important; lorsque les personnes concernées pourraient être privées de leurs droits et libertés ou empêchées d'exercer le contrôle sur leurs données à caractère personnel; lorsque le traitement concerne des données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, la religion ou les convictions philosophiques, l'appartenance syndicale, ainsi que 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; lorsque des aspects personnels sont évalués, notamment dans le cadre de l'analyse ou de la prédiction d'éléments concernant le rendement au travail, la situation économique, la santé, les préférences ou centres d'intérêt personnels, la fiabilité ou le comportement, la localisation ou les déplacements, en vue de créer ou d'utiliser des profils individuels; lorsque le traitement porte sur des données à caractère personnel relatives à des personnes physiques vulnérables, en particulier les enfants; ou lorsque le traitement porte sur un volume important de données à caractère personnel et touche un nombre important de personnes concernées.*»

[15] «*Il convient de déterminer la probabilité et la gravité du risque pour les droits et libertés de la personne concernée en fonction de la nature, de la portée, du contexte et des finalités du traitement. Le risque devrait faire l'objet d'une évaluation objective permettant de déterminer si les opérations de traitement des données comportent un risque ou un risque élevé*.»

[16] Il convient de souligner que cette évaluation objective en cas de violation de données est différente de celle de l'analyse d'impact relative à la protection des données. L'AIPD tient compte à la fois des risques du traitement des données effectué comme prévu et des risques en cas de violation, mais à un niveau hypothétique. Voir également les lignes directrices du GT29 sur la notification de violations de données à caractère personnel en vertu du règlement 2016/679.

5. les caractéristiques particulières des personnes concernées;
6. les caractéristiques particulières du responsable du traitement;
7. le nombre de personnes concernées.

47 Tous les facteurs susmentionnés doivent être soigneusement évalués, chacun séparément ou en combinaison avec les autres, afin d'indiquer le niveau des risques pour les personnes concernées.

Le recensement des risques au cours d'une AIPD peut aider les responsables du contrôle au cours du processus d'évaluation du risque. Il est très probable que les violations de données relatives aux activités de traitement qui nécessitaient une AIPD préalable en vertu de l'article 39 du règlement puissent présenter un risque plus élevé pour les droits et des incidences sur les personnes concernées.

48 Les exemples pratiques de violations de données à caractère personnel se trouvant à l'annexe 2 indiquent le niveau de risque. Des références supplémentaires concernant l'évaluation des risques figurent à l'annexe 3.

5. Comment notifier une violation de données à caractère personnel au CEPD (notification au CEPD)

ADRESSE ÉLECTRONIQUE FONCTIONNELLE DU CEPD POUR LES NOTIFICATIONS DE VIOLATIONS DE DONNÉES

data-breach-notification@edps.europa.eu

TOUTES LES COMMUNICATIONS DOIVENT ÊTRE CHIFFRÉES

Un IUE doit notifier une violation de données à caractère personnel au Contrôleur européen de la protection des données au plus tard dans les 72 heures, à moins qu'elle ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes. L'IUE doit également communiquer la violation de données à caractère personnel lorsqu'elle engendre un «risque élevé» pour les droits et libertés de la personne physique.

49 L'article 34 du règlement prévoit l'obligation de notifier les violations de données à caractère personnel au CEPD. Le responsable du traitement doit informer le CEPD au plus tard 72 heures après avoir pris connaissance de la violation de données. Le responsable du traitement est considéré comme «ayant pris connaissance» lorsqu'il existe un degré de certitude raisonnable qu'une violation de données à caractère personnel s'est produite

50 La procédure de notification au CEPD implique, d'une part, le responsable du traitement (un représentant) et, d'autre part, la personne chargée des questions de protection des données, par exemple le délégué à la protection des données (DPD).

51 Le sous-traitant joue également un rôle important, puisqu'il a l'obligation d'informer le responsable du traitement de toute violation de données.

52 En ce qui concerne l'IUE, il peut s'agir à la fois de responsables du traitement et de sous-traitants dans différentes activités de traitement de données, conformément au règlement. Ils peuvent également disposer de sous-traitants externes tiers (par exemple, de contractants) responsables de certaines activités de traitement de données à caractère personnel.

53 Le responsable du traitement conserve la responsabilité générale de la protection des données à caractère personnel; le sous-traitant peut donner au responsable du traitement les moyens de s'acquitter de ses obligations, lesquelles englobent la notification des violations.

54 Si un sous-traitant découvre une violation de données à caractère personnel dans le cadre du traitement effectué pour le compte du responsable du traitement, il doit la notifier au responsable du traitement «dans les meilleurs délais», c'est-à-dire le plus rapidement possible. Il convient de noter que le sous-traitant n'a pas besoin d'évaluer au préalable les risques découlant d'une violation avant de prévenir le responsable du traitement. C'est ce dernier qui doit procéder à cette évaluation lorsqu'il prend connaissance de la violation. Le sous-traitant doit simplement établir s'il y a eu violation et en informer le responsable du traitement. Le responsable du traitement fait appel au sous-traitant pour atteindre ses objectifs. Par conséquent, le responsable du traitement devrait en principe être considéré comme «ayant pris connaissance» dès que le sous-traitant l'a informé de la violation.

En tant que **responsable du traitement**, il est important de disposer de clauses relatives aux violations des données à caractère personnel dans les contrats conclus avec des contractants agissant en qualité de sous-traitants, pour les obliger à vous informer immédiatement en cas de violation de données à caractère personnel et à communiquer toutes les informations nécessaires en rapport avec la violation.

Un sous-traitant est tenu d'informer immédiatement le(s) responsable(s) du traitement s'il détecte une violation de données à caractère personnel et de communiquer toutes les informations nécessaires concernant l'incident.

55 Le représentant du responsable du traitement doit envoyer la notification au CEPD et garder une trace de tous les faits concernant la violation de données à caractère personnel, ses effets et les mesures prises pour y remédier, avec le soutien de tous les autres gestionnaires de dossiers, comme expliqué au chapitre 7. Le responsable du traitement doit associer le DPD tout au long du processus de gestion et de notification des violations de données à caractère personnel (notification au CEPD et communication à la personne concernée).

56 Lorsqu'il notifie la violation au CEPD, le responsable du traitement communique le nom et les coordonnées de son DPD.

Le responsable du traitement informe rapidement le DPD de l'existence d'une violation de données à caractère personnel et veille à ce que le DPD soit associé tout au long de la procédure de gestion et de notification de la violation (notification au CEPD et communication à la personne concernée).

57 Le DPD doit formuler des conseils, sur demande, au sujet de la nécessité d'une notification ou d'une communication relative à la violation de données à caractère personnel, et veiller au respect des règles, ainsi qu'au cours d'une infraction (à savoir lors de la notification), du suivi et de toute enquête ultérieure menée par le CEPD.

L'IUE doit mettre en place les procédures permettant une communication efficace de l'infraction entre: le sous-traitant et le responsable du traitement; le responsable du traitement et l'autorité de contrôle-le CEPD; le responsable du traitement et la personne concernée.

5.1. Exigences en matière de notification

58 Le responsable du traitement doit envoyer la notification au plus tard 72 heures après avoir pris connaissance de la violation de données.

59 Le responsable du traitement motive son retard de notification s'il ne respecte pas le délai de 72 heures.

60 L'obligation de notification dépend du niveau de risque pour la ou les personnes dont les données ont été violées:

a. en cas de risque improbable, il n'existe aucune obligation de notification au CEPD. Toutefois, le responsable du traitement doit en informer son DPD et documenter la violation;

b. en cas de risque, le responsable du traitement doit notifier la violation au CEPD dans un délai de 72 heures. Une explication doit être présentée en cas de non-respect du délai de 72 heures;

c. en cas de risque élevé, l'obligation prévue à l'article 35 de communiquer une violation de données à caractère personnel à la personne concernée s'applique en plus de la notification au CEPD.

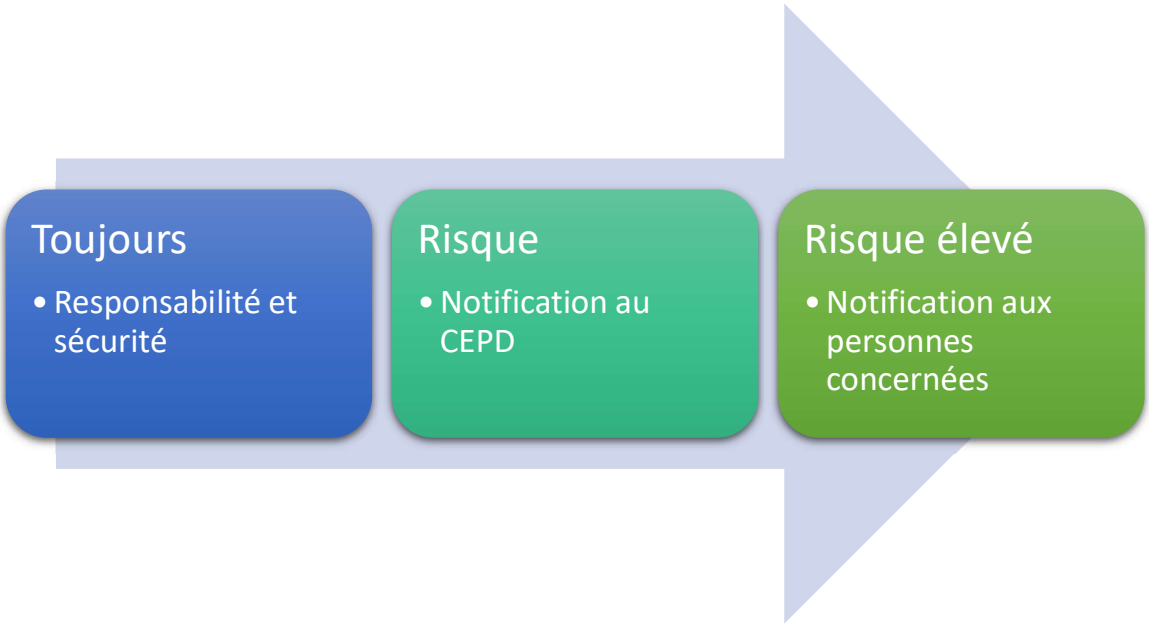


Diagramme 1. Perspective de l'obligation de procéder de manière échelonnée pour les responsables du traitement

61 La notification d'une violation de données à caractère personnel au CEPD doit au minimum contenir les éléments suivants:[17]

1. une description de 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;
2. le nom et les coordonnées du DPD;
3. une description des conséquences probables de la violation de données à caractère personnel;[18]

[17] Voir également chapitre 6.

[18] L'article 34 du règlement renvoie aux conséquences probables. Les responsables du traitement peuvent avoir intérêt à prendre en considération et à décrire non seulement les conséquences probables, mais également les conséquences potentielles, étant donné que le risque de survenance de conséquences peut augmenter au fil du temps (par exemple, des données à caractère personnel étaient sécurisées au moyen d'un chiffrement à la pointe de la technologie au moment de la violation pour éviter toute probabilité de conséquence; néanmoins, si une vulnérabilité importante est ultérieurement découverte dans le chiffrement utilisé, les conséquences sont plus probables). À cet égard, voir exemple 1 à l'annexe 2.

4. une description des mesures prises[19] ou proposées par le responsable du traitement pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuels effets négatifs sur les personnes concernées.

62 Le CEPD fournit, à l'annexe 1, un formulaire de notification sur les notifications de violations de données à caractère personnel, qui peut être utilisé par les institutions de l'UE.

5.2. Notification échelonnée

63 En fonction de la nature de la violation de données, l'IUE, en tant que responsable du traitement, peut avoir besoin d'informations, de recherches et de temps supplémentaires pour établir les faits de la violation de données. L'article 34, paragraphe 5, du règlement reconnaît et autorise la communication échelonnée des informations au CEPD.

64 Les responsables du traitement ne disposent pas toujours de toutes les informations nécessaires concernant une violation de données à caractère personnel dans le délai de 72 heures après en avoir eu connaissance. En conséquence, les détails complets et exhaustifs de l'incident ne sont pas toujours disponibles durant cette période initiale.

65 Il peut s'agir de violations complexes, par exemple de certains types d'incidents liés à la cybersécurité pour lesquels une enquête judiciaire approfondie peut s'avérer nécessaire afin d'établir pleinement la nature de la violation et la mesure dans laquelle des données à caractère personnel ont été compromises. Par conséquent, dans de nombreux cas, le responsable du traitement devra poursuivre son enquête et son suivi avec des informations complémentaires à un stade ultérieur. Dans de tels cas, les responsables du traitement doivent indiquer au CEPD les motifs du retard de la notification complète.

66 Le but premier de l'obligation de notification est de permettre à l'IUE d'agir rapidement en cas de violation, de la contenir et, si possible, de récupérer les données compromises et de demander conseil au CEPD.

67 Le responsable du traitement devrait informer le CEPD s'il ne dispose pas encore de toutes les informations requises. Il communiquera des informations supplémentaires ultérieurement et conviendra des modalités et des délais de transmission des informations supplémentaires. Cela n'empêche pas le responsable du traitement de transmettre des informations complémentaires à un stade ultérieur si des informations utiles supplémentaires concernant la violation devant être communiquées au CEPD sont portées à sa connaissance.

68 Le même formulaire de notification que celui de l'annexe 1 peut être utilisé pour la notification échelonnée.

[19] Les mesures de limitation peuvent notamment être les suivantes: arrêter le système si la violation de données est la conséquence d'une défaillance de celui-ci; modifier les mots de passe et le système des utilisateurs, ainsi que les configurations permettant de contrôler l'accès et l'utilisation; déterminer si des conseils ou une assistance techniques doivent être demandés immédiatement en interne ou en externe pour remédier aux lacunes du système et/ou arrêter le piratage; lever ou modifier les droits d'accès des personnes soupçonnées d'avoir commis la violation de données ou d'y avoir contribué; informer les autorités répressives compétentes si un vol d'identité ou une autre activité criminelle a été commis ou risque de l'être.

6. Comment communiquer une violation de données à la personne concernée?

69 En vertu de l'article 35 du règlement, lorsqu'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.

70 Par conséquent, aucun délai n'est défini dans ce cas pour l'envoi de la communication, mais celui-ci doit intervenir dans les meilleurs délais, c'est-à-dire aussi rapidement que possible. Toutefois, compte tenu du risque élevé, une communication rapide permettra à la personne dont les données à caractère personnel ont été violées de prendre toutes les précautions nécessaires.

71 La communication devrait décrire la nature de la violation de données à caractère personnel et formuler des recommandations à la personne physique concernée pour atténuer les effets négatifs potentiels. Ces communications aux personnes concernées devraient intervenir dès qu'elles sont raisonnablement possibles et en étroite coopération avec le CEPD, dans le respect des consignes communiquées par celui-ci.

72 La violation correspondante devrait être communiquée directement aux personnes concernées, sauf si cela nécessite un effort disproportionné.

73 La communication contient les coordonnées du DPD et décrit, en des termes clairs et simples, au moins:

- la nature de la violation de données à caractère personnel;
- les conséquences probables de la violation de données à caractère personnel[20];
- 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 sur les personnes.

74 L'IUE devrait également, le cas échéant, formuler pour les personnes concernées des conseils spécifiques pour leur permettre de se prémunir des éventuelles conséquences négatives de la violation, par exemple la réinitialisation des mots de passe si leurs identifiants d'accès ont été compromis. Une fois encore, un responsable du traitement peut choisir de communiquer des informations en plus de ce qui est exigé dans ce cas.

75 L'IUE communique directement avec les personnes concernées, sauf si cela exige des efforts disproportionnés [article 35, point c)]. Parmi les exemples de méthodes de communication directe figurent le courrier électronique, le SMS, le message direct et les communications postales.

[20] L'article 35 du règlement renvoie aux conséquences probables. Il pourrait être utile aux responsables du traitement de ne pas uniquement examiner les conséquences probables, mais aussi les conséquences potentielles. Lorsqu'une violation de données ne présente pas de risque élevé pour les personnes concernées parce qu'aucune conséquence n'est susceptible de se produire (par exemple lorsque des données de santé sensibles étaient sécurisées à l'aide d'un chiffrement à la pointe de la technologie au moment de la violation), il n'est pas nécessaire d'informer la personne concernée. Toutefois, si le risque que les conséquences se matérialisent ultérieurement devient plus probable au fil du temps, les personnes concernées devraient être informées de la violation de données. À cet égard, voir exemple 1 à l'annexe 2.

76 Il existe des exceptions à l'obligation incombant à l'IUE de communiquer une violation de données à caractère personnel à la personne concernée (certains exemples pratiques de cas où la communication à la personne concernée n'est pas requise figurent également à l'annexe 2):

- lorsque le responsable du traitement a mis en œuvre les mesures de protection techniques et organisationnelles appropriées et que ces mesures ont été appliquées aux données à caractère personnel affectées par la violation de données à caractère personnel (le chiffrement par exemple);
- lorsque le responsable du traitement a pris des mesures ultérieures qui garantissent que le risque élevé pour les droits et libertés des personnes concernées n'est plus susceptible de se matérialiser.

77 Si une communication individuelle exige des efforts disproportionnés (par exemple, parce que les coordonnées ont été perdues à la suite de la violation), le responsable du traitement peut informer les personnes concernées par le biais d'une communication publique ou de toute mesure similaire permettant aux personnes concernées d'être informées de manière tout aussi efficace.

78 Conformément au principe de responsabilité, les responsables du traitement doivent être en mesure de démontrer au CEPD qu'ils satisfont à une ou plusieurs des conditions susmentionnées s'ils décident de ne pas communiquer une violation aux personnes concernées. Si la communication peut ne pas être initialement obligatoire en l'absence de risque pour les personnes concernées, cette situation peut évoluer dans le temps, auquel cas le risque devrait être réévalué.

79 Le CEPD, s'il estime que la décision de ne pas informer les personnes concernées d'une violation de données à caractère personnel n'est pas fondée compte tenu de la probabilité de voir la violation de données à caractère personnel engendrer un risque élevé, peut imposer au responsable du traitement de s'exécuter. Le non-respect d'une telle injonction peut entraîner l'application de mesures d'exécution.

7. Comment documenter une violation de données à caractère personnel (exigences en matière de responsabilité et de documentation)?

80 En vertu de l'article 34, paragraphe 6, du règlement, le responsable du traitement documente toute violation de données à caractère personnel, en indiquant les faits concernant la violation de données à caractère personnel, ses effets et les mesures prises pour y remédier. La documentation ainsi constituée permet au Contrôleur européen de la protection des données de vérifier le respect de ce règlement.

81 Il est également important de conserver les preuves de la violation de données afin de faciliter l'enquête et de décider des mesures correctives à prendre.

82 En vertu du principe de responsabilité, le responsable du traitement veille à la conformité avec les autres principes relatifs au traitement de données à caractère personnel et est en mesure de démontrer cette conformité. Ces principes comprennent également l'intégrité et la confidentialité, qui sont compromises en cas de violations des données. En d'autres termes, les données sont traitées de façon à garantir une protection 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.

L'IUE met en place un registre interne des violations répertoriant tous les faits concernant les violations de données à caractère personnel, leurs effets et les mesures prises pour y remédier. Ce registre peut compléter le registre des incidents de sécurité informatique existant.

L'IUE peut demander l'avis de son DPD concernant la structure, la création et l'administration de ce registre interne des violations de données. Le DPD pourrait de surcroît être chargé de la tenue de ces registres.

83 Le suivi des violations de données est nécessaire pour que le responsable du traitement puisse prouver qu'il respecte les obligations prévues dans le règlement. En outre, le responsable du traitement serait en mesure d'avoir à sa disposition un répertoire des bonnes pratiques à suivre en cas de violation de données et une liste des incidents de sécurité concernés, susceptibles de permettre le déploiement de stratégies visant à accroître la sécurité du traitement des données.

84 Toutes les informations recueillies dans le cadre de la procédure relative aux violations de données à caractère personnel ou obtenues par cette procédure devraient être exclusivement traitées selon le principe du besoin d'en connaître. La communication sur les violations de données ne devrait pas être effectuée au moyen de systèmes/infrastructures auxquels un événement a pu porter atteinte.

Dans le cas d'une enquête, d'une inspection ou de tout autre besoin de telles informations, le CEPD attend du DPD de l'IUE qu'il soit en mesure de présenter des informations issues du registre des violations et/ou de donner au CEPD un accès à ce registre.

Annexe 1. Modèle de formulaire de notification

CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES

FORMULAIRE DE NOTIFICATION DE VIOLATION DE DONNÉES À CARACTÈRE PERSONNEL

[ARTICLE 34 DU RÈGLEMENT (UE) 2018/1725]

DATE:

A. TYPE DE NOTIFICATION

A.1 COMPLÈTE[21] ☐

A.2 ÉCHELONNÉE[22]: INITIALE:☐ SUIVI[23] ☐ CONCLUSION[24]☐

Numéro de dossier de référence[25]:

A.3 NUMÉRO D'ENREGISTREMENT[26] DE LA VIOLATION DE DONNÉES DANS VOTRE REGISTRE:

OUI ☐ Nº REG: NO☐

B. IUE RESPONSABLE DU TRAITEMENT:

B.1 NOM DE L'ORGANISATION (IUE):

B.2 ADRESSE:

B.3 PERSONNE DE CONTACT:

B.4 TÉLÉPHONE: B.5 COURRIEL:

B.6 DÉLÉGUÉ À LA PROTECTION DES DONNÉES

B.7 TÉLÉPHONE: B.8 COURRIEL:

C. SOUS-TRAITANT: (indiquer si la violation de données a été déclarée par le sous-traitant)

C.1 NOM DE L'ORGANISATION:

C.2 ADRESSE:

C.3 PERSONNE DE CONTACT:

C.4 TÉLÉPHONE :C.5 COURRIEL:

C.6 DÉLÉGUÉ À LA PROTECTION DES DONNÉES:

C.7 TÉLÉPHONE :C.8 COURRIEL:

[21] Sélectionner lorsqu'il s'agit d'une notification complète
[22] Sélectionner lorsqu'il s'agit d'une notification initiale incomplète et que des informations supplémentaires seront transmises (article 34, paragraphe 4, du règlement)
[23] Il s'agit d'un suivi de la notification initiale
[24] Il s'agit des informations définitives relatives à l'incident
[25] Dans le cas d'un type de notification de suivi ou de conclusion, veuillez indiquer l'éventuel numéro de dossier communiqué par le CEPD.
[26] Article 34, paragraphe 6, du règlement 2018/1725.

D. SECTION RELATIVE À LA VIOLATION DE DONNÉES

D.1 Expliquer brièvement l'incident et la manière dont la violation de données a été détectée:

D.2 Critères de sécurité concernés (cocher une ou plusieurs cases)

I. CONFIDENTIALITÉ ☐ divulgation ou accès non autorisé (potentiel)

II. INTÉGRITÉ ☐ altération accidentelle ou illicite

III. DISPONIBILITÉ ☐ destruction ou perte accidentelle ou illicite

D.3 DATE EXACTE OU PÉRIODE DE LA VIOLATION DE DONNÉES:

D.4 DATE DE DÉTECTION[27]: HEURE:

D.5 DATE DE NOTIFICATION[28]: HEURE:

D.6 Si plus de 72 heures se sont écoulées entre la détection et la notification, veuillez expliquer pourquoi vous n'avez pas procédé à la notification dans les délais:

D.7 QUI A ÉTÉ INFORMÉ/IMPLIQUÉ DANS L'INCIDENT:[29]

D.8 CATÉGORIES DE DONNÉES À CARACTÈRE PERSONNEL CONCERNÉES[30]

D.9 NOMBRE APPROXIMATIF DE DONNÉES À CARACTÈRE PERSONNEL CONCERNÉES:

Veuillez préciser le nombre exact si possible:

D.10 CATÉGORIES DE PERSONNES CONCERNÉES[31]:

D.11 NOMBRE APPROXIMATIF DE PERSONNES CONCERNÉES:

D.12 CONSÉQUENCES PROBABLES OU RÉELLES DE LA VIOLATION DE DONNÉES POUR LES PERSONNES CONCERNÉES:

D.13 ESTIMATION DU RISQUE POUR LES DROITS ET LIBERTÉS DES PERSONNES PHYSIQUES:

RISQUE ☐ RISQUE ÉLEVÉ☐

D.14 Expliquez brièvement comment l'évaluation du risque pour les droits et libertés des personnes physiques a été réalisée.

D.15 Avez-vous informé les personnes concernées de la violation? OUI[32] ☐ si oui, QUAND:

NON☐, si la réponse est négative, expliquez pourquoi cela n'a pas (encore) été fait.

D.16 MESURES D'ACTION VISANT À PRÉVENIR LE RISQUE ET LIMITER SON INCIDENCE[33]:

D.17 LANCEMENT D'UN PROCESSUS FORMEL D'INCIDENT DE SÉCURITÉ: OUI ☐ NON☐ en cas de réponse négative, veuillez indiquer les raisons:

D.18 CAUSE FONDAMENTALE DE LA VIOLATION DE DONNÉES[34]:

---

[27] Indiquez la date à laquelle vous avez pris connaissance de la violation de données à caractère personnel.
[28] La date de notification doit se situer moins de 72 heures après que vous avez pris connaissance de la violation. Si tel n'est pas le cas, les motifs du retard doivent être indiqués.
[29] Indiquez les personnes impliquées dans le traitement de l'incident (en interne et en externe) de l'institution de l'UE.
[30] Énumérez tous les éléments/champs de données qui ont été compromis, par exemple les prénoms et les noms, la date de naissance, les données financières, les données relatives à la santé, etc.
[31] Dressez la liste de toutes les catégories de personnes concernées, par exemple personnel de l'UE, députés européens, citoyens européens, enfants, groupes vulnérables tels que personnes handicapées, etc.
[32] Dans l'affirmative, joignez une copie de la communication envoyée à la personne concernée.
[33] Liste des mesures de sécurité et d'atténuation visant à traiter le risque, par exemple les données étaient chiffrées, le système redondant a permis à l'organisation d'avoir accès aux données à des fins de continuité de l'activité.
[34] Expliquez la cause fondamentale de l'incident de sécurité ayant entraîné la violation de données.

Annexe 2. Exemples concrets

Les exemples suivants pourraient aider l'IUE à déterminer s'il est nécessaire de transmettre une notification au CEPD ou une communication à des personnes concernées dans le cadre de différents scénarios de violation de données à caractère personnel. La liste d'exemples n'est pas exhaustive.

Par ailleurs, ces exemples peuvent aider à faire la distinction entre le risque et le risque élevé pour les droits et libertés des personnes.

N'oubliez pas qu'une violation de la sécurité de l'information qui ne compromet pas de données à caractère personnel ne relève pas de cette procédure. Par exemple, si une base de données contenant des données anonymes a été divulguée, il s'agirait d'un incident de sécurité, mais pas d'une violation de données à caractère personnel.

En outre, l'absence de communication, par l'IUE, d'informations adéquates aux personnes concernées au sujet d'un traitement ne constitue pas une violation de données au sens de l'article 35 du règlement.

Le caractère intentionnel éventuel de la violation n'a aucune incidence.

Tout incident lié à la sécurité de l'information n'est pas nécessairement une violation de données à caractère personnel, mais toute violation de données à caractère personnel est un incident lié à la sécurité de l'information.

Il est important de comprendre que le critère régissant les décisions relatives à la notification et à la communication est **le risque pour chacune des personnes concernées**, et **non la gravité de l'incident**, qui est normalement utilisée en tant que critère dans le cadre de la gestion de la sécurité.

La différence entre les deux critères peut être illustrée par l'examen des éléments pris en considération.

Les éléments suivants pourraient être utilisés pour évaluer la **gravité de l'incident**:

- gravité faible: les données compromises sont relativement habituelles dans le contexte du traitement (prénom et nom de famille uniquement, par exemple); des mesures de sécurité sont en place pour limiter l'incidence (les données ont été perdues, mais elles sont chiffrées avec des moyens de chiffrement puissants, par exemple); le nombre de personnes concernées est limité;
- gravité moyenne: les données compromises sont relativement complètes (prénoms et noms avec date de naissance, grade et allocations familiales, ainsi que d'autres informations, par exemple); le nombre de personnes concernées affectées est élevé compte tenu du contexte (par exemple, toutes les personnes travaillant pour la DG XX, la plupart des personnes travaillant sur un projet sensible spécifique, etc.);
- gravité élevée: les données sont sensibles (par exemple, des certificats médicaux) et/ou le nombre de personnes concernées affectées est très élevé (par exemple, l'ensemble du personnel de l'UE) et/ou des figures politiques sont affectées et/ou la violation de données a été exposée dans les médias (atteinte à la réputation de l'IUE).

Le **risque pour la personne** est l'un des éléments à prendre en considération en ce qui concerne la gravité de l'incident, mais il dépend d'éléments spécifiques:

- les catégories de données concernées; par exemple, le risque élevé peut être dû à la divulgation de catégories particulières, de données financières, d'autres éléments de données généralement tenus confidentiels;
- la quantité de données pour une personne physique; par exemple, un risque élevé peut être indiqué lorsqu'un nombre important d'enregistrements de certaines transactions sont divulgués, tels qu'une liste d'appels téléphoniques avec les parties liées, des listes de missions à exécuter, etc., mais aussi lorsque les données concernent de nombreux aspects différents d'une personne, même lorsqu'aucune catégorie particulière n'est concernée, telles que les données relatives à l'adresse du domicile, à la composition du ménage dans le temps, à l'historique de carrière, aux voyages, aux activités sur les réseaux sociaux, aux transactions en ligne ou à toute combinaison similaire de différents aspects de la vie;
- la facilité ou la difficulté d'identification des personnes; par exemple, si l'on peut généralement supposer que le risque associé à des données pseudonymisées est inférieur à celui associé à des données pleinement qualifiées assorties d'attributs d'identification, l'efficacité de la pseudonymisation doit être évaluée. Il se peut que les données permettent l'identification sans ces attributs (par exemple, une liste d'affectations qui peut être unique parmi l'ensemble du personnel d'une organisation et accessible par l'intermédiaire d'outils RH);
- les caractéristiques des personnes concernées; par exemple, des personnes déjà connues comme étant vulnérables, telles que des victimes de harcèlement ou de délits, sont plus susceptibles de présenter un risque élevé que d'autres à la suite d'une violation;
- les caractéristiques du responsable du traitement; par exemple, le fait qu'une personne a été enregistrée dans la base de données d'une organisation traitant de problèmes familiaux peut être plus risqué pour la personne concernée que dans le cas d'une base de données de participants à une conférence technique;
- les propriétés de la violation; par exemple, une violation causée par les activités ciblées d'un acteur malveillant qui a obtenu l'accès à des données confidentielles est plus susceptible de créer un risque élevé pour les personnes qu'une divulgation accidentelle de données similaires à un groupe restreint de destinataires connus.

Le nombre de personnes concernées est un facteur important en ce qui concerne la gravité d'un incident, mais un nombre plus élevé n'augmente pas nécessairement le niveau de risque pour les personnes concernées; par exemple, lorsqu'un acteur malveillant obtient l'accès à un petit nombre d'identifiants de cartes de crédit, la probabilité que chacune d'elles soit utilisée illégalement peut être plus élevée que dans le cas d'un vol de base de données importante.

En ce qui concerne l'obligation de notifier la violation au CEPD ou de la communiquer aux personnes concernées, le niveau de risque est le critère décisif. La gravité de l'incident a une incidence sur la réaction de l'organisation et les mesures d'atténuation et de correction à prendre.

Exemple	Type de violation	Notification au CEPD	Communication à la personne concernée	Explication
Une DG déménage dans un autre bâtiment. Des déménageurs trouvent un casier d'archives RH ouvert et un grand nombre de dossiers sont manquants. Les dossiers contiennent des données relatives à la santé. Une copie de sauvegarde numérique est disponible.	Confidentialité Intégrité	Oui	Oui	Étant donné que les dossiers contiennent des données sensibles, il existe un risque élevé pour les droits et libertés des personnes.
Une agence dotée d'un système de fichiers en réseau concernant des patients de l'Union souffrant de maladies rares gère sa propre infrastructure. Un collaborateur détecte un rançongiciel après utilisation d'une clé USB personnelle et après un certain temps, plus personne ne peut accéder aux données des serveurs de fichiers.	Disponibilité Confidentialité	Oui	Oui	Le caractère sensible des données présente un risque élevé pour les personnes concernées.
Un membre de haut niveau d'un IUE perd une clé USB contenant des copies de projets de décisions et des documents issus des dossiers, notamment des données à caractère personnel. La clé USB est chiffrée au moyen d'un algorithme à la pointe de la technologie. Une copie de sauvegarde des données existe.	Confidentialité	NON	NON	Étant donné que les données sont chiffrées à l'aide d'un algorithme de pointe et qu'il existe des sauvegardes des données, la clé unique n'est pas compromise et les données peuvent être restaurées en temps utile; la notification au CEPD et l'envoi de la communication à la personne concernée ne sont pas nécessaires. Toutefois, si la clé USB est compromise ultérieurement, une notification au CEPD et une communication à la personne concernée seront nécessaires. Tel est

				également le cas si une vulnérabilité grave est découverte ultérieurement dans l'algorithme utilisé pour chiffrer les données sur la clé USB perdue, puisque la probabilité que les données confidentielles soient compromises s'en trouve augmentée. Il s'agit d'un cas dans lequel une violation de données à caractère personnel doit être réévaluée.
La liste des noms d'utilisateur et des mots de passe des comptes de travail du personnel d'une DG a fait l'objet d'une fuite. La fuite a été immédiatement détectée par la sécurité informatique et l'institution a procédé sans attendre à la modification des noms d'utilisateur et à la réinitialisation des mots de passe.	Confidentialité	NON	NON	Étant donné que la DG a pris des mesures immédiates pour traiter et remédier aux effets négatifs de la violation de données à caractère personnel, il n'existe aucun risque pour les personnes concernées.
Un membre des RH envoie accidentellement un courriel à tous les candidats écartés dans le cadre d'une procédure de recrutement en indiquant les adresses électroniques dans le champ «cc», au lieu de les indiquer dans le champ «cci».	Confidentialité	OUI	NON	Dans ce cas, outre le fait que des adresses électroniques personnelles sont communiquées et qu'il est possible de savoir qui a présenté sa candidature pour le poste, il existe un risque pour les droits et libertés de personnes ne souhaitant pas partager ces informations. Aucun risque élevé n'est indiqué dans ce cas.
Un fonctionnaire d'un IUE envoie accidentellement au personnel d'une autre DG ou agence de l'UE un fichier contenant les noms, prénoms, coordonnées et fonctions d'une DG complète.	Confidentialité	NON	NON	Dans ce cas, la notification n'est pas nécessaire, étant donné que ces informations concernant le personnel sont déjà accessibles au public dans des annuaires interinstitutionnels ouverts relatifs au personnel de l'IUE.

Une base de données contenant des informations sur les procédures de lancement d'alerte au sein d'un IUE a été piratée et publiée sur l'internet. Les noms des lanceurs d'alerte et des personnes concernées ont été rendus publics.	Confidentialité	OUI	OUI	Dans ce cas, il existe un risque élevé pour les droits et libertés de personnes concernées. Par conséquent, le CEPD doit recevoir une notification et les lanceurs d'alerte et autres personnes concernées doivent recevoir une communication.
Une agence de l'UE est victime d'une attaque de rançongiciel entraînant le chiffrement de toutes les données à caractère personnel de citoyens de l'UE enregistrées dans un programme de financement particulier. Aucune copie de sauvegarde n'est disponible et les données ne peuvent être restaurées.	Intégrité Disponibilité Confidentialité	OUI	OUI	Une violation constituant une atteinte à l'intégrité, à la disponibilité et, potentiellement, à la confidentialité. Dans ce cas, il existe un risque élevé pour les droits et libertés des personnes concernées. Par conséquent, le CEPD doit recevoir une notification et les personnes concernées doivent recevoir une communication.
Les certificats médicaux des agents d'une DG ont été effacés accidentellement ou, dans l'exemple de données chiffrées de manière sécurisée, la clé de déchiffrement a été perdue. Il n'existe aucune copie de sauvegarde des données des certificats médicaux ni aucun dossier physique.	Disponibilité Intégrité	OUI	OUI	En l'absence de copie de sauvegarde des données et compte tenu de l'impossibilité de restaurer celles-ci, la perte des certificats médicaux des collaborateurs présente un risque élevé pour les droits et libertés de ceux-ci. Le CEPD doit recevoir une notification et les personnes concernées doivent recevoir une communication.
Un ordinateur portable contenant la copie d'une liste de collaborateurs soumis à des mesures disciplinaires a été volé.	Confidentialité	OUI	OUI	Le caractère sensible des données crée un risque élevé pour leurs droits et leurs libertés en cas d'accès par des personnes non autorisées.

Des milliers d'enregistrements contenant des données à caractère personnel sont conservés sans chiffrement sur la plateforme du fournisseur de services d'informatique en nuage. Ce fournisseur est piraté au bout d'un an.	Intégrité Confidentialité	OUI	OUI	Compte tenu du nombre élevé de personnes concernées, il convient d'informer celles-ci de l'incident.
Les données à caractère personnel de contribuables de l'UE acquittant des impôts élevés sont stockées sous forme chiffrée au moyen d'un algorithme AES-512 et la clé se trouve sur le système de fichiers local. Après un an, le RLSI annonce une faille de sécurité du réseau. La clé de chiffrement a été consultée.	Intégrité Confidentialité	OUI	OUI	Une notification devrait être envoyée, compte tenu de la nature de la violation et du risque potentiel pour les personnes concernées.

Annexe 3. Références et conseils de lecture

Documents stratégiques du groupe de travail «article 29» du CEPD

1. **Avis 03/2014 sur la notification des violations de données à caractère personnel du groupe de travail «article 29»**

   http://ec.europa.eu/newsroom/article29/news-overview.cfm

2. **Lignes directrices sur la notification de violations de données à caractère personnel en vertu du règlement (UE) 2016/679, adoptées le 3 octobre 2017, révisées pour la dernière fois et adoptées le 6 février 2018, groupe de travail «article 29»**

   http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052

Documents stratégiques d'autres autorités chargées de la protection des données dans l'UE

1. **Irlande:**

   Personal Data Security Breach Code of Practice (Code de bonnes pratiques en matière de violation de la sécurité des données à caractère personnel), 9 juillet 2011 https://www.dataprotection.ie/docs/Data_Security_Breach_Code_of_Practice/1082.htm

2. **Royaume-Uni:**

   a. Déclaration des violations de données à caractère personnel (Personal data breach reporting) https://ico.org.uk/for-organisations/resources-and-support/getting-ready-for-the-gdpr-resources/pdb/

3. Lignes directrices sur la gestion des violations de la sécurité des données (Guidance on data security breach management): https://ico.org.uk/media/for-organisations/documents/1562/guidance_on_data_security_breach_management.pdf
   Italie:

   Violation de données au titre du RGPD

   http://www.garanteprivacy.it/regolamentoue/approccio-basato-sul-rischio-e-misure-di-accountability-responsabilizzazione-di-titolari-e-responsabili

Documents et références de l'Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information (ENISA)

4. **Recommandations concernant une méthodologie d'évaluation de la gravité des violations de données à caractère personnel**

   https://www.enisa.europa.eu/publications/dbn-severity

5. **Recommandations concernant la mise en œuvre technique de l'article 4**

   https://www.enisa.europa.eu/publications/art4_tech

6. **Outil de notification de violation de données à caractère personnel**

https://www.enisa.europa.eu/topics/data-protection/personal-data-breaches/personal-data-breach-notification-tool

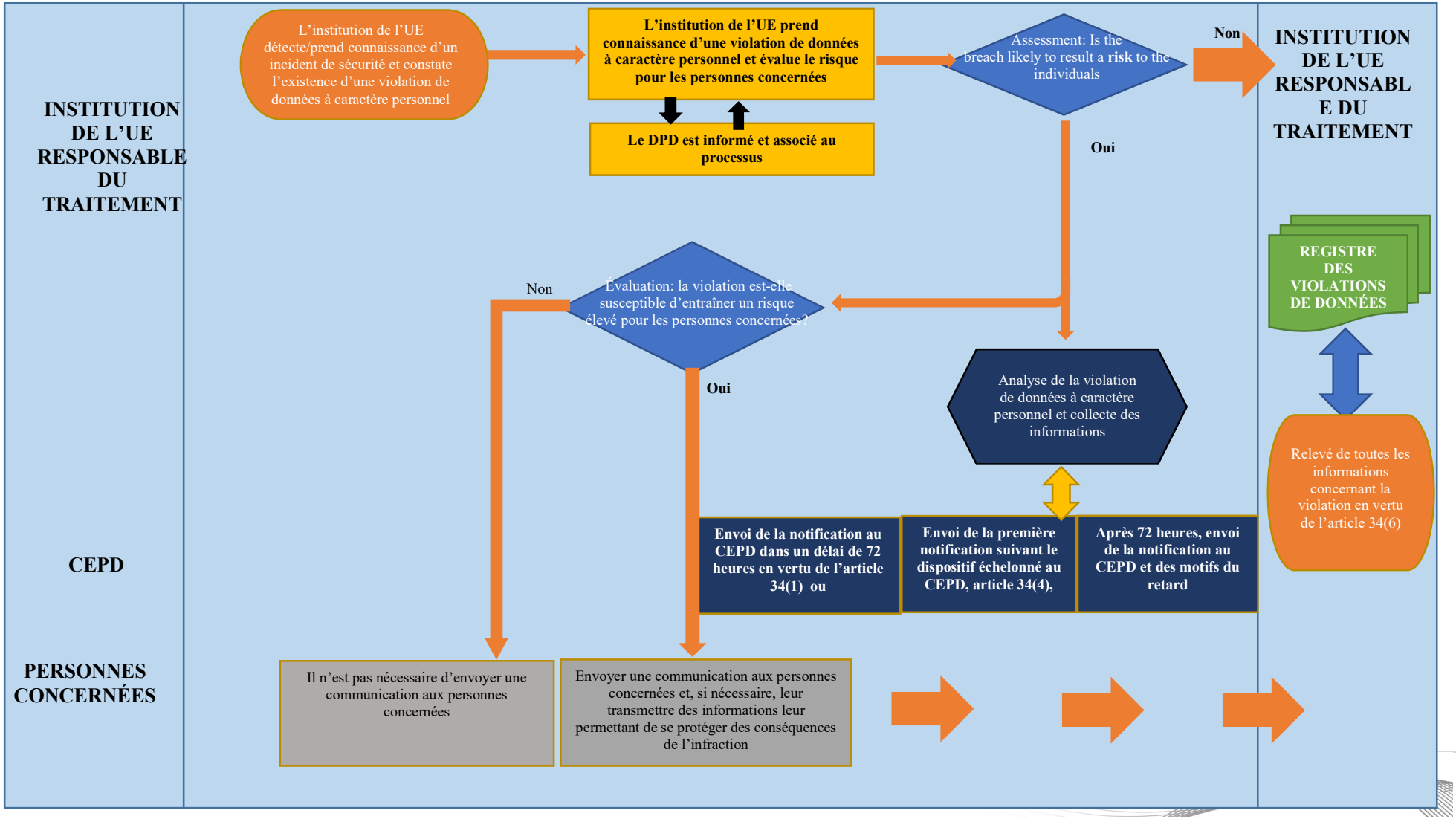
Annexe 4. Glossaire

Terme	Description
Authentification	Le processus visant à garantir et à confirmer l'identité d'un utilisateur ou d'une machine réalisant une opération (généralement par l'intermédiaire d'un système de TI).
Données à caractère personnel	Toute information se rapportant à une personne physique identifiée ou identifiable («personne concernée»); une personne physique identifiable est une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.
Violation de données à caractère personnel	Une atteinte à la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération ou la divulgation non autorisée de données à caractère personnel transmises, stockées ou traitées de quelque manière que ce soit, ou l'accès à ces données.
Catégories particulières (de données à caractère personnel)	Au titre du règlement actuel, il s'agit des données qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que le traitement des données relatives à la santé ou à la vie sexuelle. La proposition de nouveau règlement ajoute les données génétiques et biométriques afin d'identifier de façon unique une personne physique. Ces catégories sont soumises à des règles spécifiques.
Responsable du traitement	L'institution ou organe communautaire, la direction générale, l'unité ou toute autre entité organisationnelle qui, seule ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel.
Sous-traitant	Personne physique ou morale, autorité publique, agence ou tout autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement.
Sous-traitant ultérieur	Personne physique ou morale, autorité publique, agence ou tout autre organisme qui traite des données à caractère personnel pour le compte du sous-traitant.
Délégué à la protection des données (DPD)	Membre du personnel d'une organisation chargé de soutenir l'organisation en garantissant le respect de la législation applicable en matière de protection des données. Sa nomination, ses tâches et ses pouvoirs sont définis dans le règlement (et dans le nouveau

	règlement). Il peut être externe ou commun à différentes institutions.
Personne concernée	Individu dont les données à caractère personnel sont traitées.
Analyse d'impact relative à la protection des données	Analyse des risques pour les droits et les libertés des personnes physiques posés par le traitement de leurs données à caractère personnel. Le nouveau règlement prévoit des éléments obligatoires et des circonstances dans lesquelles l'analyse est obligatoire. Toutefois, les responsables du traitement peuvent réaliser cette analyse et obtenir des avantages intéressants en dehors de ces circonstances.
Risque	Dans un contexte de protection de la vie privée, le risque peut être défini comme l'incidence des événements potentiels sur la vie privée des donneurs d'informations identifiables et se caractérise par son niveau d'incidence et sa probabilité.
Évaluation des risques	Processus global d'identification, d'analyse et d'évaluation des risques
Gestion des risques relatifs à la sécurité des systèmes d'information (gestion des risques SSI)	Processus de gestion des risques visant à garantir que la confidentialité, l'intégrité et la disponibilité des actifs d'une organisation correspondent aux objectifs de celle-ci.
Confidentialité	Caractéristique en vertu de laquelle les informations ne sont ni disponibles, ni divulguées à des personnes ou à des entités non autorisées, ni accessibles à des processus non autorisés.
Intégrité	Caractère complet et exact des informations
Disponibilité	Caractéristique consistant à être accessible et utilisable à la demande d'une entité autorisée
Notification de violation de données (à caractère personnel)	Notification obligatoire de violations de données (à caractère personnel) à l'autorité chargée de la protection des données
Niveau de risque	Ampleur d'un risque exprimée en fonction de ses conséquences et de sa probabilité combinées

Annexe 5. En bref

A. Organigramme concernant les exigences en matière de notification de violations de données applicables aux institutions de l'UE



Rappel:

ADRESSE ÉLECTRONIQUE FONCTIONNELLE DU CEPD POUR LES NOTIFICATIONS DE VIOLATIONS DE DONNÉES

data-breach-notification@edps.europa.eu

Tout incident lié à la sécurité de l'information n'est pas nécessairement une violation de données à caractère personnel, mais toute violation de données à caractère personnel est un incident lié à la sécurité de l'information.

Il convient, lors de l'évaluation de chaque incident signalé, de déterminer si des données à caractère personnel sont affectées.

Si des données à caractère personnel sont affectées, l'incident de sécurité est considéré comme une violation de données à caractère personnel.

Une fois que l'incident de sécurité est considéré comme une violation de données à caractère personnel, il convient d'évaluer quelle serait son incidence sur les droits et libertés des personnes concernées à l'étape suivante.

L'IUE introduit dans son processus de gestion des incidents de sécurité une étape nécessaire permettant la vérification de chaque incident de sécurité signalé lorsque des données à caractère personnel sont concernées, afin de détecter une violation de données à caractère personnel déclenchant le processus de gestion des violations de données.

Un IUE met en œuvre sa propre procédure de gestion des violations de données à caractère personnel ou un ensemble de politiques qui se concentreront sur l'analyse d'impact de chaque violation de données à caractère personnel signalée et sur le choix de la procédure de notification adéquate à l'égard du CEPD et des personnes concernées. Les rôles et les responsabilités sont clairement définis.

Dans les cas où il est établi qu'une violation de données à caractère personnel signalée ne crée aucun risque pour les personnes concernées, le responsable du traitement n'est pas tenu de la notifier au CEPD ni de la communiquer aux personnes concernées. Toutefois, cette décision doit être adéquatement documentée.

Conformément à l'article 34 du règlement, l'IUE doit notifier une violation de données à caractère personnel au Contrôleur européen de la protection des données au plus tard dans les 72 **heures**, à moins qu'elle ne soit pas susceptible d'engendrer un **risque** pour les droits et libertés des personnes.

En outre, conformément à l'article 35, paragraphe 1, l'IUE doit également communiquer la violation de données à caractère personnel lorsqu'elle engendre un «**risque élevé**» pour les droits et libertés de la personne physique.

La gravité de la violation devra être évaluée au cas par cas. Le «risque pour les droits et libertés des personnes physiques» doit servir de base à l'examen.

Le recensement des risques au cours d'une AIPD peut aider les responsables du contrôle au cours du processus d'évaluation du risque. Il est très probable que les violations de données relatives aux activités de traitement qui nécessitaient une AIPD préalable en vertu de l'article 39 du règlement puissent présenter un risque plus élevé pour les droits et des incidences sur les personnes concernées

Un IUE doit notifier une violation de données à caractère personnel au Contrôleur européen de la protection des données au plus tard dans les 72 heures, à moins qu'elle ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes. L'IUE doit également communiquer la violation de données à caractère personnel lorsqu'elle engendre un «risque élevé» pour les droits et libertés de la personne physique.

S'il n'existe pas de copie de sauvegarde des données et que les services ne peuvent être rétablis, cette situation pourrait être considérée comme une violation de données à caractère personnel.

Lorsque des données à caractère personnel sont déjà accessibles au public, la publication de ces mêmes données par des tiers ne constitue pas un risque pour les personnes concernées et n'est pas considérée comme une violation de données à caractère personnel.

L'IUE met en place un registre interne des violations répertoriant tous les faits concernant les violations de données à caractère personnel, leurs effets et les mesures prises pour y remédier. Ce registre peut compléter le registre des incidents de sécurité informatique existant.