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

**00683/11/FR**
**WP 184**

# Document de travail 01/2011 concernant le cadre juridique relatif aux violations de données à caractère personnel actuellement en vigueur dans l'UE et présentant des recommandations quant aux actions à entreprendre à l'avenir

**Adopté le 5 avril 2011**

**Le groupe de travail sur la protection des personnes à l'égard du traitement des données à caractère personnel**

institué par la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 (JO L 281 du 23.11.1995, p. 31),

vu l'article 29 et l'article 30, paragraphe 1, point a), et paragraphe 3, de ladite directive,

vu son règlement intérieur,

a adopté le document de travail ci-après.

## I. INTRODUCTION

1. Le présent document du groupe de travail «Article 29» fait le point de la situation et passe en revue la manière dont les États membres transposent dans leur législation nationale les dispositions relatives aux violations de données à caractère personnel de la directive «vie privée et communications électroniques»[1].

2. Cet exercice poursuit trois objectifs. ***Premièrement***, le groupe de travail «Article 29» souhaite avoir une vue d'ensemble de la situation actuelle dans ce domaine. Celle-ci englobe à la fois des éléments fondamentaux, comme la situation en matière de transposition, et des questions plus complexes, telles que les différences d'approche initiale dans certains domaines (portée de l'obligation, adoption prévue ou non de lignes directrices nationales développant certains aspects de la directive «vie privée et communications électroniques», autorité nationale compétente, etc.). Même à ce stade tardif, l'identification des différences d'approche qui se dessinent au niveau national pourrait aider les États membre à aligner leurs vues et à assurer une mise en œuvre uniforme.

3. ***Deuxièmement,*** ces travaux permettent aux autorités nationales chargées de la protection des données de prendre connaissance des conclusions formulées et ont attiré leur attention sur la nécessité d'entreprendre les activités de suivi décrites dans le présent document. Il en ressort que les autorités compétentes doivent poursuivre les efforts visant à définir les règles et procédures internes auxquelles les responsables du traitement sont soumis lorsqu'ils notifient des violations aux particuliers et aux autorités compétentes. De plus, étant donné que les responsables du traitement seront de plus en plus souvent amenés à notifier des violations transfrontalières de données à caractère personnel, il est indispensable que les autorités définissent ensemble une méthode de coopération.

4. ***En outre***, cet exercice a permis au groupe de travail «Article 29» de poursuivre ses réflexions sur la question et de parvenir à une série de conclusions quant aux mesures qui devraient être prises dans le domaine de la notification des violations de données à caractère personnel. Ces conclusions, qui viennent compléter les avis émis sur le sujet à d'autres occasions[2] par le groupe de travail «Article 29», s'appuient sur l'expérience acquise dans le domaine de la notification des failles de sécurité par les autorités nationales

---

1 Directive 2009/136/CE du Parlement européen et du Conseil du 25 novembre 2009 modifiant, entre autres, la directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques, JO L 337 du 18.12.2009, p. 11.

2 Voir le document du groupe de travail «Article 29» intitulé «L'avenir de la protection de la vie privée: Contribution conjointe à la consultation de la Commission européenne sur le cadre juridique du droit fondamental à la protection des données à caractère personnel», adopté le 1.12.2009 (WP 168); l'avis 1/2009 concernant les propositions modifiant la directive 2002/58/CE sur la protection de la vie privée dans le secteur des communications électroniques (directive «vie privée et communications électroniques»), adopté le 10.2.2009 (WP 159); et l'avis 2/2008 sur la révision de la directive 2002/58/CE concernant la protection de la vie privée dans le secteur des communications électroniques (directive «vie privée et communications électroniques»), adopté le 15.5.2008 (WP 150).

chargées de la protection des données à caractère personnel qui se conforment déjà aux exigences en matière de notification des violations de données à caractère personnel. Le groupe de travail «Article 29» souhaite que ces conclusions soient prises en compte dans le cadre des mesures qui seront prises à l'avenir en matière de violations de données à caractère personnel. De telles mesures sont notamment attendues à deux égards:

**a)** pour compléter le cadre juridique relatif aux violations de données à caractère personnel instauré par la directive «vie privée et communications électroniques». L'article 4, paragraphe 5, de cette directive délègue à la Commission le pouvoir d'adopter des mesures techniques d'application (depuis l'adoption du traité de Lisbonne, il s'agit des «pouvoirs délégués» en vertu de l'article 290 TFUE) en vue d'assurer, à certains égards (à savoir les circonstances, le format et les procédures applicables aux exigences en matière d'information et de notification), une mise en œuvre et une application cohérentes du cadre juridique relatif aux violations de données à caractère personnel;

**b)** pour élargir le cadre juridique relatif aux violations de données à caractère personnel de la directive «vie privée et communications électroniques» à l'occasion de la révision de la directive 95/46. La Commission s'est engagée devant le Parlement européen à lancer «sans retard les travaux préparatoires appropriés, y compris une consultation des parties prenantes, afin de soumettre des propositions adéquates en la matière d'ici à fin 2011...»[3]. Elle a confirmé cet engagement dans sa communication intitulée «*Une approche globale de la protection des données à caractère personnel dans l'Union européenne*»[4].

5. Les éléments évoqués ci-dessus sont présentés de la manière suivante: après une synthèse des principaux éléments des dispositions en matière de violations des données à caractère personnel contenues dans la directive «vie privée et communications électroniques» (section II), le présent document de travail résume la législation applicable en la matière dans les États membres (section III). Ce résumé s'appuie sur les informations communiquées par les autorités nationales chargées de la protection des données (ci-après «APD»), qui ne seront pas reproduites ici étant donné que la situation en matière de transposition ne cesse d'évoluer. La section IV présente plusieurs mesures à mettre en œuvre par les autorités compétentes et par le groupe de travail «Article 29» en vue de développer des procédures internes et d'instaurer des procédures de coopération. Les sections V et VI, qui sont consacrées aux actions futures, rappellent la portée générale des mesures attendues en matière de violations de données à caractère personnel, décrivent les procédures à respecter et formulent des recommandations stratégiques.

---

3 Voir la déclaration de la Commission concernant la notification de violations de données présentée au Parlement européen en 2009 dans le contexte de la réforme du cadre réglementaire relatif aux communications électroniques. Document consultable à l'adresse suivante: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P6-TA-2009-0360+0+DOC+XML+V0//FR.

4 Document COM(2010)609 final, adopté le 4.11.2010.

6. L'avis exprimé dans le présent document est sans préjudice des éventuelles lignes directrices plus spécifiques qui pourraient être publiées à l'avenir, notamment dans le cadre des mesures techniques d'application adoptées par la Commission en vertu de l'article 4, paragraphe 5, de la directive «vie privée et communications électroniques».

## II. LES VIOLATIONS DE DONNÉES À CARACTÈRE PERSONNEL AUX TERMES DE LA DIRECTIVE «VIE PRIVÉE ET COMMUNICATIONS ÉLECTRONIQUES»

7. La version révisée de la directive «vie privée et communications électroniques» instaure pour la première fois dans l'UE un cadre réglementaire pour la notification obligatoire des violations de données à caractère personnel. Ce cadre ne s'applique qu'aux fournisseurs de services de communications électroniques accessibles au public (les fournisseurs de services de communications électroniques et d'accès à l'internet, par exemple).[5] Il comporte une série d'éléments essentiels devant obligatoirement être transposés dans la législation des États membres.

### II.1 Éléments essentiels communs

8. Les éléments essentiels définis dans la directive «vie privée et communications électroniques» sont les suivants:

   a. La ***définition d'une violation de données*** au sens de l'article 2, point i), selon lequel on entend par violation de données à caractère personnel «*une violation de la sécurité entraînant accidentellement ou de manière illicite la destruction, la perte, l'altération, la divulgation ou l'accès non autorisés de données à caractère personnel transmises, stockées ou traitées d'une autre manière en relation avec la fourniture de services de communications électroniques accessibles au public dans la Communauté»*. Cette violation doit donc porter sur des «données à caractère personnel», telles que définies à l'article 2, point a), de la directive relative à la protection des données[6]. Une violation de données à caractère personnel englobe non seulement la diffusion ou l'accès non autorisés à des données personnelles, mais également la simple destruction

---

5 Tels que définis à l'article 2 de la directive 2002/21/CE du Parlement européen et du Conseil, du 7 mars 2002 relative à un cadre réglementaire commun pour les réseaux et les services de communications électroniques, telle que modifiée par la directive 2009/140/CE et le règlement 544/2009 (directive «cadre»), couvrant les fournisseurs de services fournis normalement contre rémunération qui consistent entièrement ou principalement en la transmission de signaux sur un réseau électronique. Cette définition exclut la fourniture de contenus, ainsi que les services de la société de l'information, qui ne consistent pas entièrement ou principalement en la transmission de signaux sur des réseaux de communication électroniques.

6 Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, JO L 281 du 23.11.1995. Article 2, point a), de la directive relative à la protection des données: «*toute information concernant une personne physique identifiée ou identifiable (personne concernée); est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale*».

ou altération accidentelles qui ne sont pas suivies d'un accès non autorisé (ou qui ne le seront vraisemblablement pas).

b. Les ***seuils*** légaux de déclenchement de l'obligation de notification aux particuliers et aux autorités (article 4, paragraphe 3, premier et deuxième alinéas). Ces seuils définissent les circonstances dans lesquelles une entité victime d'une violation doit notifier celle-ci aux autorités et aux personnes physiques concernées. La directive «vie privée et communications électroniques» exige que les particuliers soient avertis «*lorsque la violation de données à caractère personnel est de nature à affecter négativement les données à caractère personnel ou la vie privée d'un abonné ou d'un particulier...*». Toutes les violations de données doivent être notifiées aux autorités.

c. Le ***contenu et le moment de la notification***. Selon l'article 4, paragraphe 3, premier et deuxième alinéas, les particuliers doivent être avertis «*...sans retard indu*». En ce qui concerne le contenu, la notification doit décrire la nature de la violation de données à caractère personnel, mentionner les informations relatives aux points de contact et recommander des mesures à prendre pour atténuer les conséquences négatives possibles. La notification faite à l'autorité nationale compétente doit également décrire les mesures prises par le fournisseur pour remédier à la violation.

d. Les éventuelles exceptions relatives aux ***mesures de protection technologiques*** et au contrôle de l'application de la législation (article 4, paragraphe 3, troisième alinéa).

9. Bien que ce cadre réglementaire vise à harmoniser la réglementation dans l'ensemble des États membres, il se peut que certains éléments décrits ci-après entraînent des différences d'approche entre les États membres.

## II. 2 Domaines susceptibles de faire l'objet d'approches différentes

10. Des approches différentes pourraient se dessiner dans les trois domaines ci-dessous.

11. ***Champ d'application de l'obligation:*** l'obligation de notifier les violations de données à caractère personnel imposée par la directive «vie privée et communications électroniques» s'applique aux fournisseurs de services de communications électroniques accessibles au public. Le considérant 59 de ladite directive encourage toutefois les États membres à en élargir le champ d'application (soulignement ajouté): «*... Dans l'attente d'un examen, mené par la Commission, de toute la législation communautaire applicable dans ce domaine, la Commission, après consultation du contrôleur européen de la protection des données, devrait prendre les mesures appropriées pour promouvoir, sans retard, l'application, dans l'ensemble de la Communauté, des principes inscrits dans les règles relatives à la notification des violations des données contenues dans la directive 2002/58/CE (directive "vie privée et communications électroniques"), quel que soit le secteur ou le type de données concerné.*»

12. ***Adoption de lignes directrices par les autorités compétentes:*** La directive «vie privée et communications électroniques» (article 4, paragraphe 4) autorise expressément les autorités nationales compétentes à adopter des lignes directrices et à édicter des instructions sur les trois éléments suivants:
    a. les circonstances dans lesquelles le fournisseur est tenu de notifier la violation de données à caractère personnel;
    b. le format applicable à la notification, et
    c. la procédure de transmission de la notification.

    Le point a) ci-dessus permet notamment aux autorités compétentes de déterminer qu'en raison de leur caractère sensible, certaines données à caractère personnel atteindraient nécessairement le seuil de déclenchement de l'obligation de notification si elles étaient compromises[7]. Il pourrait également leur permettre de définir des situations inférieures à un certain seuil, dans lesquelles la notification ne serait pas obligatoire.
    Certaines différences d'approche pourraient donc apparaître, du moins dans ce domaine, selon que les autorités compétentes décideront ou non d'exercer cette prérogative et en fonction de la manière dont elles procéderont. Les lignes directrices ou instructions éventuellement édictées par les autorités compétentes seront toutefois soumises aux mesures d'application adoptées par la Commission, voir les sections V et VI ci-dessous.

13. ***Mesures de protection technologiques:*** des différences pourraient également caractériser l'application de l'exception relative aux mesures de protection technologiques, qui doivent rendre les données incompréhensibles à toute personne qui n'est pas autorisée à y avoir accès. En effet, l'article 4, paragraphe 3, prévoit que c'est aux autorités nationales compétentes qu'il incombe d'apprécier si les mesures technologiques sont adéquates et si elles ont été appliquées.

## III. LES VIOLATIONS DE DONNÉES À CARACTÈRE PERSONNEL DANS LES ÉTATS MEMBRES

14. Le groupe de travail «Article 29» a examiné l'état d'avancement de la transposition des nouvelles dispositions relatives aux violations de données à caractère personnel dans la législation des États membres. Cet examen a une portée limitée (il ne couvre que les grandes lignes) et donne un aperçu de la situation actuelle, qui ne cesse d'évoluer à mesure que le processus de transposition se poursuit. Les constats ci-dessous doivent donc être considérés comme provisoires, sous réserve des changements qui interviendront à mesure que les États membres achèveront les procédures législatives visant à assurer la mise en œuvre de la directive «vie privée et communications électroniques». Voici une synthèse des constatations qui ont été faites:

15. ***Situation en matière de transposition.*** La transposition de la directive «vie privée et communications électroniques» doit être achevée le 25 mai 2011. À l'heure actuelle, une minorité d'États membres ont lancé une procédure de

[7] Ces données seraient alors «affectées négativement» au sens de l'article 4, paragraphe 3, deuxième alinéa (ces cas viendraient s'ajouter aux violations identifiées au considérant 61 comme ayant toujours des effets négatifs sur les données).

consultation publique. La plupart des États membres ont élaboré des projets de textes, mais la grande majorité d'entre eux n'ont pas encore atteint le stade du dépôt au Parlement. Aucun État membre ne semble avoir déjà adopté de texte législatif.

16. A priori, ces informations révèlent que les États membres n'ont guère déployé d'efforts pour assurer la mise en œuvre jusqu'à présent. Il est regrettable de constater que bon nombre d'entre eux ne seront vraisemblablement pas en mesure de respecter le délai de transposition.

17. ***Éléments essentiels communs.*** Il ressort des informations sur l'état d'avancement de la transposition recueillies par les autorités nationales chargées de la protection des données que la plupart des États membres transposent les dispositions de la directive «vie privée et communications électroniques» en reproduisant assez fidèlement leur libellé. Plus spécifiquement:

    a. **Définitions.** La plupart des États membres semblent avoir repris les définitions contenues dans la directive «vie privée et communications électroniques».

    b. **Seuils de déclenchement de l'obligation de notification aux particuliers.** La plupart des États membres semblent avoir repris le seuil de déclenchement prévu par la directive. Certains d'entre eux ont cependant introduit quelques changements. Par exemple, la République tchèque propose d'ajouter «grave» et la Suède a proposé de rendre la notification obligatoire lorsque la violation «peut être considérée comme exerçant un impact plus important [sur l'abonné ou sur l'utilisateur dont les données sont affectées]».

18. **Domaines dans lesquels des approches différentes pourraient apparaître.** Les informations transmises par les États membres témoignent de l'apparition des légères différences d'approche décrites ci-dessous.

    a. ***Champ d'application***. Bien qu'ils aient été incités à élargir le champ d'application de l'obligation à des acteurs autres que les fournisseurs de services de communications électroniques, la plupart des États membres n'ont pas pris de dispositions en ce sens. L'Allemagne et l'Autriche font cependant exception à cette règle, ce qui s'explique par le fait que ces États membres avaient déjà adopté des lois instaurant un cadre réglementaire en matière de violation de données à caractère personnel applicable à tous les secteurs. Signalons également que dans d'autres États membres, les autorités nationales chargées de la protection des données à caractère personnel ont élevé la notification des violations à elles-mêmes et aux particuliers concernés au rang de bonne pratique à encourager. C'est notamment le cas du Royaume-Uni et de l'Irlande.

    b. ***Lignes directrices.*** Près de la moitié des États membres qui ont élaboré un projet de texte ou qui ont déposé un projet de loi prévoient d'adopter des lignes directrices.

L'organe compétent pour leur adoption varie selon les cas. La définition de lignes directrices est généralement confiée à l'autorité nationale chargée de la protection des données à caractère personnel (c'est le cas en Estonie, au Luxembourg, au Royaume-Uni et, potentiellement, en France[8]) ou à l'autorité nationale de régulation des communications électroniques (en Suède et en Finlande). Dans d'autres cas, cette compétence est partagée (Allemagne).

Dans la plupart des États membres, les matières censées faire l'objet de lignes directrices correspondent en gros à celles qui sont mentionnées dans la directive «vie privée et communications électroniques». Dans certains États membres, il semble toutefois que les matières couvertes soient plus nombreuses. C'est notamment le cas de l'Estonie (où l'autorité nationale chargée de la protection des données peut instaurer des exceptions à l'obligation de notification) et, potentiellement, de la France[9]. Le champ d'application des lignes directrices envisagées semble parfois indéterminé (c'est le cas en Italie) ou plus limité que celui prévu par la directive. Si la plupart des autorités compétentes n'ont pas encore élaboré de lignes directrices, certaines s'en sont déjà dotées ou ont adopté des bonnes pratiques (c'est le cas du Royaume-Uni, de l'Irlande et de l'Allemagne).

## IV. ACTIONS FUTURES À METTRE EN ŒUVRE PAR LES AUTORITÉS NATIONALES COMPÉTENTES ET PAR LE GROUPE DE TRAVAIL «ARTICLE 29»

19. Cet exercice a démontré que le degré de sensibilisation et le niveau de transposition des procédures de notification des violations de données à caractère personnel, varient selon les États membres. Comme indiqué ci-dessus, certains États membres, mais pas tous, ont déjà acquis une expérience dans ce domaine.

### *a) Création d'une plate-forme visant à sensibiliser davantage les autorités aux procédures en matière de violation de sécurité*

20. Le groupe de travail «Article 29» estime qu'il importe de remédier à cette situation afin de mettre toutes les autorités nationales chargées de la protection des données sur un pied d'égalité. À cet effet, il s'engage à créer un sous-groupe qui fonctionnera comme une plate-forme d'échange d'avis et de connaissances. Celle-ci aura pour but de favoriser le développement de procédures et de concepts uniformes qui seront applicables à la notification des violations de sécurité dans tous les États membres[10].

---

8 Selon les discussions en cours: la législation adoptée pourrait comporter des différences.

9 Idem.

10 Il convient de noter qu'il incombe aux États membres de désigner l'autorité nationale compétente qui doit satisfaire aux exigences de l'article 3 de la directive-cadre. Ainsi, dans certains États membres, ce sont les autorités nationales chargées de la protection des données qui seront compétentes pour recevoir les notifications de violations de données à caractère personnel. Dans d'autres États membres, cette mission sera confiée à d'autres organismes, tels que l'autorité nationale de régulation.

21. Plus spécifiquement, et sans préjudice des changements susceptibles d'être apportés à la liste ci-dessous en fonction des besoins, le groupe de travail «Article 29» souhaite se concentrer dans un premier temps sur les domaines suivants: *i)* la création d'un pool de connaissances concernant les circonstances dans lesquelles il est nécessaire de notifier les violations aux particuliers; *ii)* l'élaboration de lignes directrices relatives à la procédure à suivre et au moment auquel la notification doit être effectuée (que ce soit aux autorités nationales chargées de la protection des données ou aux particuliers concernés); et *iii)* la définition de critères indiquant comment mesurer l'efficacité des mesures techniques de protection.

***b) Coordination des procédures en cas de violations transfrontalières de données***

22. La plate-forme devrait également être utilisée pour coordonner les procédures en cas de violations transfrontalières de données. De nombreuses violations de données comporteront vraisemblablement des éléments transfrontaliers. Par exemple, il se peut que le responsable du traitement soit établi dans un État membre, mais que la violation se produise dans un ou plusieurs autres États membres si des ressources ont été piratées à cet endroit. Il se peut également que l'État membre dans lequel la violation a eu lieu ne soit pas celui où se trouvent la plupart des particuliers concernés ou que la violation de données se produise simultanément dans plusieurs établissements. Parfois, il est difficile de déterminer l'endroit où une violation a été commise, alors que les effets se font sentir dans de nombreux États membres. Dans tous les cas mentionnés ci-dessus (et vraisemblablement dans d'autres), il se peut que les autorités compétentes doivent coordonner leurs actions.

23. Compte tenu de ce qui précède, le groupe de travail «Article 29» s'engage à lancer un exercice de coordination, dont la première étape consisterait à analyser la législation applicable et l'autorité compétente en cas de violation transfrontalière de données à caractère personnel. Il conviendrait également d'étudier les obligations d'information et de rapport et d'instaurer les procédures adéquates.

24. Cette plate-forme sera créée dès que possible. Cette initiative sera très utile puisqu'elle permettra au groupe de travail «Article 29» d'apporter une contribution dans le contexte de la future action législative de l'UE en matière de violations de données à caractère personnel (voir les sections V et VI).

## V. ACTION LÉGISLATIVE FUTURE DE L'UE EN MATIÈRE DE VIOLATIONS DE DONNÉES À CARACTÈRE PERSONNEL

25. Comme expliqué ci-dessus, les développements législatifs en matière de violations de données à caractère personnel devraient intervenir dans les deux domaines décrits ci-après.

---

Quoi qu'il en soit, les autorités nationales chargées de la protection des données s'attendent à participer à cet exercice.

26. Le premier domaine est celui de la ***directive «vie privée et communications électroniques».*** Celle-ci instaure le cadre réglementaire général en matière de violations de données à caractère personnel. La directive délègue toutefois certains pouvoirs à la Commission (article 4, paragraphe 5) afin de garantir une mise en œuvre et une application cohérentes. Cette délégation de pouvoirs se justifie par la nécessité de garantir un niveau élevé de protection à tous les particuliers de l'UE et de veiller à ce que les entités qui ont été victimes de violations de données à caractère personnel ne soient pas embarrassées par des exigences disparates en matière de notification. Plus spécifiquement, elle fait expressément référence aux circonstances, formats et procédures applicables aux exigences en matière d'information et de notification. Tels sont les domaines dans lesquels les autorités nationales compétentes sont habilitées à publier des lignes directrices.

27. Compte tenu notamment des diverses consultations que la Commission est tenue d'entreprendre, la procédure d'adoption des mesures techniques d'application peut durer au moins un an[11]. Avant d'adopter des mesures, la Commission doit consulter une série d'entités. L'article 4, paragraphe 5, mentionne plus particulièrement l'ENISA, le CEPD et le groupe de travail «Article 29». Cette disposition prévoit également que la Commission doit associer d'autres *«parties prenantes concernées»* à la procédure, notamment pour être informée des meilleures solutions techniques et économiques disponibles pour assurer la mise en œuvre.

28. ***Une évolution des politiques concernant les violations de données à caractère personnel a également été annoncée dans le cadre de la révision de la directive 95/46.*** La révision de la directive «vie privée et communications électroniques» a offert l'occasion au législateur d'instaurer des règles contraignantes en matière de violation des données à caractère personnel. Eu égard au champ d'application de la directive «vie privée et communications électroniques», l'obligation de notification des violations de données à caractère personnel n'était applicable qu'aux fournisseurs de services de communications électroniques accessibles au public. Or, cette disposition sectorielle doit s'accompagner d'un élargissement de l'obligation de notification à tous les responsables du traitement, qui interviendra dans le contexte de la révision de la directive 95/46. Dans sa communication intitulée «*Une approche globale de la protection des données à caractère personnel dans l'Union européenne»*, la Commission a réaffirmé qu'il importe que les particuliers soient informés lorsque des données les concernant ont été accidentellement ou illégalement détruites, perdues, altérées ou consultées par des personnes non autorisées. Conformément à cette communication, la Commission a l'intention d'examiner les modalités d'introduction, dans le cadre juridique global, d'une obligation de notification des violations de données à caractère personnel couvrant tous les secteurs, qui devrait être

[11] La procédure comporte la préparation des mesures (après consultation des parties prenantes), l'avis du comité composé de représentants des États membres et l'adoption finale par la Commission. Il existe ensuite un droit de contrôle du Parlement européen.

cohérente avec celle prévue par la directive «vie privée et communications électroniques»[12].

29. Le groupe de travail «Article 29» se félicite de cette initiative, car il est convaincu que l'existence d'une obligation de notification des violations de sécurité applicable à tous les secteurs aidera les particuliers à prendre les mesures qui s'imposent pour réduire les dommages susceptibles de résulter d'une telle compromission. En outre, l'obligation de notifier les violations de sécurité incitera les sociétés à améliorer la sécurité de leurs données et les rendra davantage responsables.

## VI. RECOMMANDATIONS POUR L'AVENIR EN MATIÈRE DE NOTIFICATION DES VIOLATIONS DE DONNÉES

30. Après avoir analysé la situation dans les États membres (section III), ainsi que la situation actuelle au niveau de l'UE (sections II et IV), le groupe de travail «Article 29» souhaite formuler les conclusions et recommandations ci-après.

***Quant au champ d'application de l'obligation***

31. Le groupe de travail «Article 29» soutient l'introduction d'une disposition relative à la notification des violations de données à caractère personnel dans le cadre juridique global en vue d'élargir cette obligation à tous les responsables du traitement. La raison d'être de cette obligation s'applique tout autant aux responsables du traitement autres que les fournisseurs de services de communications électroniques. **Par conséquent, le groupe de travail «Article 29» se félicite que la Commission envisage d'élargir le champ d'application de cette obligation dans le contexte de la révision de la directive 95/46.**

***Quant aux éléments essentiels (définitions, seuils de déclenchement) du cadre réglementaire en matière de violations de données à caractère personnel***.

32. Il semble que la plupart des États membres transposent assez fidèlement les éléments essentiels des dispositions relatives aux violations de données à caractère personnel qui sont contenues dans la directive «vie privée et communications électroniques». Il s'agit notamment des définitions, des seuils de déclenchement et d'autres éléments principaux. Il est donc vraisemblable que les autorités nationales compétentes et les acteurs concernés y fassent de plus en plus souvent appel face aux violations de données à caractère personnel. Au cours des prochaines années, ces concepts et procédures seront donc amenés à se «consolider» dans les États membres de l'Union.

33. Par conséquent, pour élargir l'obligation à d'autres acteurs, **la Commission devrait s'appuyer sur des éléments essentiels identiques ou très similaires à ceux contenus dans la directive «vie privée et communications**

[12] Voir les pages 6 et 7 de la communication de la Commission intitulée «*Une approche globale de la protection des données à caractère personnel dans l'Union européenne*», COM(2010) 609 final, adoptée le 4.11.2010.

**électroniques»**. Ceci s'applique à la définition et, plus particulièrement, au seuil de déclenchement de l'obligation de notification aux personnes concernées, selon lequel la violation des données à caractère personnel doit être notifiée lorsqu'elle est de nature à affecter négativement les données à caractère personnel ou la vie privée des particuliers.

34. Dès lors que ces critères ont commencé à être appliqués, il serait contre-productif d'imposer des règles différentes aux responsables du traitement des données autres que les fournisseurs de services de communications électroniques. De surcroît, les dispositions relatives aux violations de données à caractère personnel qui sont contenues dans la version révisée de la directive «vie privée et communications électroniques» ont fait l'objet d'un débat approfondi durant la procédure législative préalable à l'adoption de ladite directive. Dans le cadre de ce débat, les avis du groupe de travail «Article 29»[13] et du CEPD,[14] ainsi que le point de vue d'autres parties prenantes, ont été pris en considération. Ces règles reflètent les vues de diverses parties prenantes. Elles résultent d'une mise en balance des intérêts: les critères de déclenchement de l'obligation de notification aux particuliers suffisent en principe à protéger ces derniers sans pour autant imposer des exigences trop contraignantes et inutiles. En dernière analyse, une violation de données à caractère personnel reste une violation de données à caractère personnel, que le responsable du traitement soit un transporteur, une banque, un fabricant ou un organisme public. Les règles doivent donc être les mêmes pour tous, faute de quoi les opérateurs ne seront pas sur un pied d'égalité. Cette approche semble trouver confirmation dans la communication intitulée «*Une approche globale de la protection des données à caractère personnel dans l'Union européenne*», où la Commission affirme qu'«*il y a lieu de garantir l'adoption d'une approche systématique et cohérente à cet égard*» et ajoute que ce processus n'aura aucune incidence sur la directive «vie privée et communications électroniques».

***Pouvoirs délégués /mesures d'application***

35. De nombreux États membres font référence à la disposition de la directive «vie privée et communications électroniques» qui autorise leurs autorités nationales compétentes à adopter des lignes directrices sur les circonstances, le format et les procédures applicables aux exigences d'information et de notification. Ces éléments sont identiques à ceux que la Commission peut réglementer au moyen de mesures d'application.

36. Le groupe de travail «Article 29» estime qu'il serait bénéfique d'instaurer dans tous les États membres un cadre réglementaire harmonisé en matière de violations de données à caractère personnel et reconnaît que celui-ci devrait

---

13 Voir les avis 150 et 159 du groupe de travail «Article 29» susmentionnés.

14 Deuxième avis du contrôleur européen de la protection des données relatif au réexamen de la directive 2002/58/CE 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 C 128 du 6.6.2009, p. 28.

tenir compte de l'expérience acquise par les autorités nationales compétentes qui sont déjà confrontées à de telles violations.

***a) Quant au calendrier***

37. Compte tenu de la durée des procédures relatives aux mesures d'application et de l'obligation de consulter diverses parties prenantes, ainsi que l'ENISA, le groupe de travail «Article 29» et le CEPD, le ***groupe de travail «Article 29» invite la Commission à s'atteler à la tâche aussi rapidement que possible***. À cette fin, il suggère notamment que la Commission réalise une étude sur les premières pratiques développées par les autorités compétentes et propose que les mesures soient mises en œuvre à la lumière des retours d'information ainsi recueillis. L'expérience actuellement acquise au sein des États membres peut alimenter utilement les travaux. Il importe tout particulièrement d'uniformiser les circonstances dans lesquelles toutes les violations pertinentes sont notifiées, notamment lorsque les organisations sont établies dans plusieurs États membres. Une intervention tardive augmenterait le risque de voir s'installer définitivement des approches divergentes entre les États membres.

***b) Quant au contenu***

38. Sur la base du cadre fourni par la directive «vie privée et communications électroniques», le groupe de travail «Article 29» souhaite encourager la Commission à envisager d'exercer ses pouvoirs délégués dans les domaines ci-après.

***Premièrement,*** standardiser les circonstances dans lesquelles une violation de données à caractère personnel doit être notifiée. À cette fin, il conviendrait de préciser la notion de seuil de déclenchement de l'obligation de notification aux particuliers. Par exemple, elle pourrait couvrir les violations de données à caractère personnel qui, en raison de leur caractère sensible, devraient être considérées comme atteignant le seuil. L'harmonisation des règles dans ce domaine est particulièrement importante pour les opérateurs actifs dans plusieurs États membres (en d'autres termes, il ne serait pas souhaitable que plusieurs autorités compétentes adressent à un opérateur des ordres de notification différents pour une seule et même violation de données à caractère personnel).

***Deuxièmement,*** définir la procédure à suivre en cas de violation de données. Il serait notamment envisageable d'imposer des délais de notification plus précis aux autorités ou de prévoir des étapes procédurales spécifiques, telles que l'envoi d'une demande de confirmation de la sécurité du système ou l'obligation de s'assurer la participation d'enquêteurs de la police scientifique et technique pour établir les faits et circonstances entourant la violation.

***Troisièmement,*** sur la base de l'expérience acquise par les autorités nationales compétentes, y compris au niveau de l'application des articles 19, 20 et 21 de la directive 95/46, le groupe de travail «Article 29» invite la Commission à mettre au point un format de notification standard européen. Les notifications adressées aux autorités compétentes devraient comporter au moins des

rubriques telles que la description de la violation, les effets de celle-ci et les mesures prises ou proposées, afin d'aider ces instances à évaluer la violation dans le cadre de leurs pouvoirs de contrôle.

***Quatrièmement,*** le groupe de travail «Article 29» est favorable à ce que la Commission définisse, dans le cadre de ses compétences d'exécution, les modalités autorisées de transmission des notifications aux particuliers, en précisant si celles-ci peuvent être effectuées par courrier électronique ou par téléphone. Ceci vaut également pour les cas où la notification aux particuliers peut être effectuée par l'intermédiaire des journaux, etc. (si l'adresse est inconnue, par exemple). Ces règles devraient également permettre aux autorités compétentes d'exercer leur pouvoir d'appréciation à la lumière des circonstances propres à chaque cas.

***Cinquièmement,*** des orientations devraient également être définies en ce qui concerne le format des informations relatives aux violations de données dont les fournisseurs de services sont censés tenir un inventaire[15].

***Sixièmement,*** à la lumière de l'expérience acquise par les organes compétents des États membres et de la contribution des parties prenantes visées à l'article 4, paragraphe 5, le groupe de travail «Article 29» invite également la Commission à publier des orientations sur les mesures de protection technologiques qui, si elles ont été appliquées et en fonction de la manière dont elles ont été mises en œuvre, pourraient justifier une exonération de l'obligation de notification.

***c) Quant à leur champ d'application***

39. Enfin et surtout, le groupe de travail «Article 29» estime que les mesures d'application adoptées en vertu de la directive «vie privée et communications électroniques» doivent également s'appliquer à d'autres catégories de responsables du traitement des données**.** La Commission devrait donc résister à la tentation d'adopter des mesures sectorielles et se concentrer plutôt sur des mesures généralement applicables. Une répétition inutile des efforts ne trouverait aucune justification.

Fait à Bruxelles, le 5 avril 2011

*Par le groupe de travail*
*Le président*
*Jacob KOHNSTAMM*

[15] Conformément à l'article 4, paragraphe 4, deuxième alinéa, les entités couvertes doivent tenir à jour un inventaire des violations suffisant pour permettre aux autorités de vérifier le respect de leurs obligations de notification.