RÈGLEMENTS

RÈGLEMENT (UE) N° 611/2013 DE LA COMMISSION

du 24 juin 2013

concernant les mesures relatives à la notification des violations de données à caractère personnel en vertu de la directive 2002/58/CE du Parlement européen et du Conseil sur la vie privée et les communications électroniques

LA COMMISSION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne,

vu la 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) [1], et notamment son article 4, paragraphe 5,

après consultation de l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA),

après consultation du groupe de protection des personnes à l'égard du traitement des données à caractère personnel, institué par l'article 29 de la 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 [2] (ci-après dénommé le «groupe de travail Article 29»),

après consultation du Contrôleur européen de la protection des données (CEPD),

considérant ce qui suit:

(1) La directive 2002/58/CE prévoit l'harmonisation des dispositions nationales nécessaires pour assurer un niveau équivalent de protection des droits et libertés fondamentaux, et en particulier du droit à la vie privée et à la confidentialité, en ce qui concerne le traitement des données à caractère personnel dans le secteur des communications électroniques, ainsi que la libre circulation de ces données et des équipements et services de communications électroniques dans l'Union.

(2) En vertu de l'article 4 de la directive 2002/58/CE, les fournisseurs de services de communications électroniques accessibles au public sont tenus de notifier les violations de données à caractère personnel aux autorités nationales compétentes et, dans certains cas, aux abonnés et aux particuliers concernés. Les violations de données à caractère personnel sont définies à l'article 2, point i), de la directive 2002/58/CE comme des violations 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 l'Union.

(3) Afin d'assurer une mise en œuvre cohérente des mesures visées à l'article 4, paragraphes 2, 3 et 4, de la directive 2002/58/CE, l'article 4, paragraphe 5, de celle-ci habilite la Commission à adopter des mesures techniques d'application concernant les circonstances, le format et les procédures relatives aux exigences en matière d'information et de notification visées audit article.

(4) La diversité des exigences nationales en la matière peut être un facteur d'insécurité juridique, entraîner des procédures plus complexes et plus lourdes ainsi que des frais administratifs importants pour les fournisseurs ayant une activité transnationale. La Commission estime donc qu'il est nécessaire d'adopter de telles mesures techniques d'application.

(5) Le présent règlement ne concerne que la notification des violations de données à caractère personnel et ne prévoit donc pas de mesures techniques d'application relatives à l'article 4, paragraphe 2, de la directive 2002/58/CE sur l'information des abonnés en cas de risque particulier de violation de la sécurité du réseau.

(6) Il découle de l'article 4, paragraphe 3, premier alinéa, de la directive 2002/58/CE que les fournisseurs devraient notifier toutes les violations de données à caractère personnel à l'autorité nationale compétente. Aussi un fournisseur ne devrait-il pas avoir le choix d'informer ou pas l'autorité nationale compétente. Toutefois, cela ne devrait pas empêcher l'autorité nationale compétente concernée de hiérarchiser l'instruction de certaines violations de la façon qu'elle juge appropriée conformément à la législation applicable, ni de prendre les mesures nécessaires pour éviter qu'il y ait trop ou trop peu de violations de données à caractère personnel signalées.

(7) Il convient de prévoir un système de notification des violations de données à caractère personnel à l'autorité nationale compétente, qui comporte, si certaines conditions sont remplies, plusieurs stades auxquels s'appliquent des délais. Ce système est destiné à faire en sorte que l'autorité nationale compétente soit informée aussi rapidement et complètement que possible sans toutefois gêner inutilement le fournisseur dans ses efforts pour enquêter sur la violation et prendre les mesures nécessaires afin d'en limiter les conséquences et d'y remédier.

[1] JO L 201 du 31.7.2002, p. 37.
[2] JO L 281 du 23.11.1995, p. 31.

(8) Le fait de simplement soupçonner qu'une violation de données à caractère personnel s'est produite ou de simplement constater un incident sans disposer d'informations suffisantes, malgré tous les efforts déployés à cette fin par un fournisseur, ne permet pas de considérer qu'une telle violation a été constatée aux fins du présent règlement. Le fait de disposer des informations visées à l'annexe I devrait, à cet égard, mériter une attention particulière.

(9) Dans le cadre de l'application du présent règlement, les autorités nationales compétentes concernées devraient coopérer en cas de violation de données à caractère personnel de dimension transnationale.

(10) Le présent règlement ne prévoit pas de spécification supplémentaire concernant l'inventaire des violations de données à caractère personnel que les fournisseurs doivent tenir à jour, étant donné que l'article 4 de la directive 2002/58/CE en définit le contenu de façon exhaustive. Toutefois, les fournisseurs peuvent se référer au présent règlement pour déterminer le format de l'inventaire.

(11) Toutes les autorités nationales compétentes devraient mettre un moyen électronique sécurisé à la disposition des fournisseurs pour qu'ils notifient les violations de données à caractère personnel dans un format commun reposant sur une norme telle que XML et reprenant les informations visées à l'annexe I dans les langues correspondantes, de façon à permettre à tous les fournisseurs à l'intérieur de l'Union de suivre une procédure de notification similaire indépendamment de l'endroit où ils se trouvent et où la violation s'est produite. À cet égard, la Commission devrait faciliter la mise en œuvre du moyen électronique sécurisé, en organisant des réunions avec les autorités nationales compétentes si nécessaire.

(12) Pour déterminer si une violation de données à caractère personnel est susceptible de porter atteinte aux données à caractère personnel ou à la vie privée d'un abonné ou d'une personne, il conviendrait en particulier de prendre en compte la nature et la teneur des données concernées, notamment s'il s'agit de données relatives à des informations financières comme les numéros de carte de crédit et coordonnées bancaires; de catégories de données particulières visées à l'article 8, paragraphe 1, de la directive 95/46/CE; et de certaines données spécifiquement liées à la fourniture de services de téléphonie et internet, c'est-à-dire les données relatives au courrier électronique, les données de localisation, les fichiers journaux, les historiques de sites consultés et les listes d'appels détaillées.

(13) Dans certains cas exceptionnels, le fournisseur devrait être autorisé à retarder la notification à l'abonné ou au particulier s'il y a un risque que la notification nuise à l'efficacité de l'enquête sur la violation de données à caractère personnel. Dans ce contexte, les cas exceptionnels peuvent recouvrir les enquêtes judiciaires ainsi que d'autres violations de données à caractère personnel qui ne sont pas équivalentes à un délit grave mais peuvent justifier de reporter la notification. En tout état de cause, il devrait incomber à l'autorité nationale compétente de décider, cas par cas et compte tenu des circonstances, d'accepter le report ou d'exiger la notification.

(14) Les fournisseurs devraient disposer des coordonnées de leurs abonnés, étant donné qu'ils sont directement liés par contrat, mais pas de celles des autres personnes lésées par la violation de données à caractère personnel. Dans ce cas, le fournisseur devrait être autorisé à d'abord informer ces personnes par des avis dans de grands médias nationaux ou régionaux, tels que les journaux, puis à leur faire parvenir dès que possible une notification individuelle comme prévu dans le présent règlement. Le fournisseur n'est donc pas expressément tenu de recourir aux médias, mais il est plutôt habilité à le faire, s'il le souhaite, lorsqu'il en est encore à identifier toutes les personnes atteintes.

(15) Les informations concernant la violation devraient se limiter à celle-ci et ne pas être associées à des informations concernant autre chose. Par exemple, faire figurer des informations concernant une violation de données à caractère personnel sur une facture courante ne devrait pas être considéré comme un moyen approprié de notifier une telle violation.

(16) Le présent règlement ne prévoit pas de mesures de protection technologiques spécifiques justifiant de déroger à l'obligation de notifier les violations de données à caractère personnel aux abonnés ou aux particuliers car, avec le temps, de telles mesures peuvent évoluer en fonction des progrès techniques. La Commission devrait toutefois être en mesure de publier une liste indicative de ces mesures de protection technologiques spécifiques, selon les pratiques actuelles.

(17) Le fait de recourir au cryptage ou au hachage ne devrait pas être considéré comme suffisant en soi pour que les fournisseurs puissent prétendre, plus largement, avoir rempli l'obligation générale de sécurité énoncée à l'article 17 de la directive 95/46/CE. À cet égard, les fournisseurs devraient également mettre en œuvre les mesures techniques et d'organisation appropriées pour prévenir, détecter et empêcher les violations de données à caractère personnel. Les fournisseurs devraient examiner tout risque pouvant subsister après la réalisation de contrôles afin de comprendre où les violations de données à caractère personnel sont susceptibles de se produire.

(18) Si le fournisseur recourt à un autre fournisseur pour assurer une partie du service, par exemple en ce qui concerne la facturation ou des tâches de gestion, cet autre fournisseur, qui n'est pas directement lié par contrat avec l'utilisateur final, ne devrait pas être tenu de notifier les violations de données à caractère personnel. En revanche, il devrait alerter et informer le fournisseur avec lequel il est directement lié par contrat. Cela

devrait également valoir dans le cadre de la fourniture en gros de services de communications électroniques, lorsque le fournisseur en gros n'est en général pas directement lié par contrat avec l'utilisateur final.

(19) La directive 95/46/CE définit le cadre général de la protection des données à caractère personnel dans l'Union européenne. La Commission a soumis une proposition de règlement du Parlement européen et du Conseil (ci-après dénommé le «règlement sur la protection des données») afin de remplacer la directive 95/46/CE. Le règlement proposé sur la protection des données instaurerait, en se fondant sur l'article 4, paragraphe 3, de la directive 2002/58/CE, l'obligation, pour tous les responsables du traitement des données, de notifier les violations de données à caractère personnel. Le présent règlement de la Commission est parfaitement conforme à cette proposition de mesure.

(20) Le règlement proposé sur la protection des données apporte aussi un nombre limité de modifications techniques à la directive 2002/58/CE pour prendre en compte la transformation de la directive 95/46/CE en règlement. Les conséquences juridiques de fond du nouveau règlement pour la directive 2002/58/CE feront l'objet d'un examen de la part de la Commission.

(21) Trois ans après l'entrée en vigueur du présent règlement, son application et ses dispositions devraient faire l'objet d'un réexamen à la lumière du cadre juridique en vigueur à ce moment-là, y compris du règlement proposé sur la protection des données. Un tel réexamen devrait être associé, si possible, à tout réexamen futur de la directive 2002/58/CE.

(22) L'application du présent règlement peut notamment être évaluée à l'aide des statistiques établies par les autorités nationales compétentes concernant les violations de données à caractère personnel qui leur sont notifiées. Ces statistiques peuvent, par exemple, indiquer le nombre de violations de données à caractère personnel notifiées à l'autorité nationale compétente, à l'abonné ou au particulier, le temps nécessaire pour remédier à la violation, et si des mesures de protection technologiques ont été prises. Ces statistiques devraient fournir à la Commission et aux États membres des données cohérentes et comparables et ne devraient révéler ni l'identité du fournisseur notifiant ni celle des abonnés ou personnes concernés. La Commission peut aussi, à cette fin, organiser régulièrement des réunions avec les autorités nationales compétentes et d'autres parties intéressées.

(23) Les mesures prévues au présent règlement sont conformes à l'avis du comité des communications,

A ADOPTÉ LE PRÉSENT RÈGLEMENT:

Article premier

Champ d'application

Le présent règlement s'applique à la notification, par les fournisseurs de services de communications électroniques accessibles au public (ci-après dénommés le «fournisseur»), des violations de données à caractère personnel.

Article 2

Notification à l'autorité nationale compétente

1. Le fournisseur notifie toutes les violations de données à caractère personnel à l'autorité nationale compétente.

2. Le fournisseur notifie la violation de données à caractère personnel à l'autorité nationale compétente, au plus tard vingt-quatre heures après le constat de la violation, si possible.

Le fournisseur fournit les informations visées à l'annexe I dans sa notification à l'autorité nationale compétente.

Le constat d'une violation de données à caractère personnel est considéré comme établi dès lors que le fournisseur dispose d'assez d'éléments indiquant qu'il s'est produit un incident de sécurité ayant compromis des données à caractère personnel pour justifier une notification conformément au présent règlement.

3. Si les informations visées à l'annexe I ne sont pas toutes disponibles et si la violation de données à caractère personnel exige une enquête plus approfondie, le fournisseur est autorisé à transmettre une notification initiale à l'autorité nationale compétente, au plus tard vingt-quatre heures après le constat de la violation. Cette notification initiale comprend les informations visées à la partie 1 de l'annexe I. Le fournisseur transmet une seconde notification à l'autorité nationale compétente le plus rapidement possible et au plus tard trois jours après la notification initiale. Cette seconde notification comprend les informations visées à la partie 2 de l'annexe I et, si nécessaire, actualise les informations déjà fournies.

Si le fournisseur, malgré ses recherches, n'est pas en mesure de fournir toutes les informations dans le délai de trois jours à compter de la notification initiale, il notifie toutes les informations qu'il a recueillies dans ce délai et présente à l'autorité nationale compétente une justification valable de la notification tardive des informations restantes. Le fournisseur notifie dès que possible les informations restantes à l'autorité nationale compétente et, si nécessaire, actualise les informations déjà fournies.

4. L'autorité nationale compétente met à la disposition de tous les fournisseurs établis dans l'État membre concerné un moyen électronique sécurisé de notification des violations de données à caractère personnel ainsi que des informations sur les procédures pour y accéder et l'utiliser. Si nécessaire, la Commission organise des réunions avec les autorités nationales compétentes pour faciliter l'application de cette disposition.

5. Si la violation de données à caractère personnel porte atteinte à des abonnés ou des particuliers d'États membres autres que celui de l'autorité nationale compétente à laquelle la violation a été notifiée, ladite autorité informe les autres autorités nationales concernées.

Pour faciliter l'application de cette disposition, la Commission établit et tient à jour une liste des autorités nationales compétentes et des points de contact appropriés.

Article 3

Notification à l'abonné ou au particulier

1. Lorsque la violation de données à caractère personnel est susceptible de porter atteinte aux données à caractère personnel ou à la vie privée d'un abonné ou d'un particulier, le fournisseur, en plus de la notification visée à l'article 2, notifie également la violation à l'abonné ou au particulier.

2. Il est déterminé si une violation de données à caractère personnel est susceptible de porter atteinte aux données à caractère personnel ou à la vie privée d'un abonné ou d'un particulier en prenant notamment en compte les éléments suivants:

a) la nature et la teneur des données concernées, en particulier s'il s'agit de données relatives à des informations financières, de catégories de données particulières visées à l'article 8, paragraphe 1, de la directive 95/46/CE ainsi que de données de localisation, fichiers journaux internet, historiques de sites web consultés, données relatives au courrier électronique et listes d'appels téléphoniques détaillées;

b) les conséquences vraisemblables de la violation de données à caractère personnel pour l'abonné ou le particulier concerné, notamment les cas où la violation pourrait entraîner un vol ou une usurpation d'identité, une atteinte à l'intégrité physique, une souffrance psychologique, une humiliation ou une atteinte à la réputation; et

c) les circonstances de la violation de données à caractère personnel, en particulier l'endroit où les données ont été volées ou le moment auquel le fournisseur sait que les données sont en possession d'un tiers non autorisé.

3. La notification à l'abonné ou au particulier est effectuée sans retard injustifié après constat de la violation de données à caractère personnel tel que défini à l'article 2, paragraphe 2, troisième alinéa. Cela est indépendant de la notification de la violation de données à caractère personnel à l'autorité nationale compétente, visée à l'article 2.

4. Le fournisseur fournit les informations visées à l'annexe II dans sa notification à l'abonné ou au particulier. La notification à l'abonné ou au particulier est rédigée dans une langue claire et aisément compréhensible. Le fournisseur n'utilise pas la notification comme un moyen de promouvoir ou d'annoncer des services nouveaux ou supplémentaires.

5. Dans certains cas exceptionnels, s'il y a un risque que la notification à l'abonné ou au particulier nuise à l'efficacité de l'enquête sur la violation de données à caractère personnel, le fournisseur est autorisé, après avoir obtenu l'accord de l'autorité nationale compétente, à retarder la notification jusqu'au moment où ladite autorité juge possible de notifier la violation conformément au présent article.

6. Le fournisseur notifie la violation de données à caractère personnel à l'abonné ou au particulier par des moyens de communication qui garantissent une réception rapide de l'information et qui sont sécurisés conformément aux règles de l'art. Les informations concernant la violation se limitent à celle-ci et ne sont pas associées à des informations concernant autre chose.

7. Si le fournisseur directement lié par contrat avec l'utilisateur final, malgré les efforts raisonnables déployés, n'est pas en mesure d'identifier dans le délai fixé au paragraphe 3 toutes les personnes susceptibles d'être lésées par la violation de données à caractère personnel, il peut, dans le même délai, informer ces personnes par des avis dans de grands médias nationaux ou régionaux dans les États membres concernés. Ces avis contiennent les informations visées à l'annexe II, si nécessaire sous une forme condensée. Dans ce cas, le fournisseur continue à déployer tous les efforts raisonnables pour identifier ces personnes et leur notifier dès que possible les informations visées à l'annexe II.

Article 4

Mesures de protection technologiques

1. Par dérogation à l'article 3, paragraphe 1, la notification d'une violation de données à caractère personnel à l'abonné ou au particulier concerné n'est pas nécessaire si le fournisseur a prouvé, à la satisfaction de l'autorité nationale compétente, qu'il a mis en œuvre les mesures de protection technologiques appropriées et que ces dernières ont été appliquées aux données concernées par ladite violation de sécurité. De telles mesures de protection technologiques rendent les données incompréhensibles à toute personne qui n'est pas autorisée à y avoir accès.

2. Les données sont considérées comme incompréhensibles si:

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

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

3. La Commission peut, après avoir consulté les autorités nationales compétentes par l'intermédiaire du groupe de travail Article 29, l'Agence européenne chargée de la sécurité des réseaux et de l'information et le Contrôleur européen de la protection des données, publier une liste indicative des mesures de protection technologiques appropriées, visées au paragraphe 1, selon les pratiques actuelles.

Article 5

Recours à un autre fournisseur

Lorsque, pour fournir une partie du service de communications électroniques, il est fait appel à un autre fournisseur qui n'est pas directement lié par contrat avec les abonnés, cet autre fournisseur informe immédiatement celui qui l'a engagé en cas de violation de données à caractère personnel.

Article 6

Rapport et réexamen

Dans les trois ans suivant l'entrée en vigueur du présent règlement, la Commission établit un rapport sur l'application du règlement, son efficacité et son impact sur les fournisseurs, les abonnés et les particuliers. Sur la base de ce rapport, la Commission procède au réexamen du présent règlement.

Article 7

Entrée en vigueur

Le présent règlement entre en vigueur le 25 août 2013.

Le présent règlement est obligatoire dans tous ses éléments et directement applicable dans tout État membre.

Fait à Bruxelles, le 24 juin 2013.

Par la Commission
Le président
José Manuel BARROSO

ANNEXE I

Contenu de la notification à l'autorité nationale compétente

Partie 1

Identification du fournisseur

1. Nom du fournisseur

2. Identité et coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues

3. Mention indiquant s'il s'agit d'une première ou d'une deuxième notification

Informations initiales sur la violation de données à caractère personnel (à compléter dans des notifications ultérieures le cas échéant)

4. Date et heure de l'incident (si elles sont connues; une estimation peut être fournie si nécessaire) et du constat de l'incident

5. Circonstances de la violation de données à caractère personnel (par exemple, perte, vol, reproduction)

6. Nature et teneur des données à caractère personnel concernées

7. Mesures techniques et d'organisation appliquées (ou à appliquer) par le fournisseur aux données à caractère personnel concernées

8. Recours à d'autres fournisseurs ayant joué un rôle (le cas échéant)

Partie 2

Informations supplémentaires sur la violation de données à caractère personnel

9. Résumé de l'incident à l'origine de la violation de données à caractère personnel (y compris le lieu physique de la violation et le moyen de stockage concerné)

10. Nombre d'abonnés ou de particuliers concernés

11. Conséquences et préjudices potentiels pour les abonnés ou particuliers

12. Mesures techniques et d'organisation prises par le fournisseur pour atténuer les préjudices potentiels

Notification supplémentaire éventuelle aux abonnés ou aux particuliers

13. Contenu de la notification

14. Moyens de communication utilisés

15. Nombre d'abonnés ou de particuliers informés

Questions transnationales éventuelles

16. Violation de données à caractère personnel concernant des abonnés ou des particuliers dans d'autres États membres

17. Notification à d'autres autorités nationales compétentes

ANNEXE II

Contenu de la notification à l'abonné ou au particulier

1. Nom du fournisseur

2. Identité et coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues

3. Résumé de l'incident à l'origine de la violation de données à caractère personnel

4. Date estimée de l'incident

5. Nature et teneur des données à caractère personnel concernées, conformément à l'article 3, paragraphe 2

6. Conséquences vraisemblables de la violation de données à caractère personnel pour l'abonné ou le particulier concerné, conformément à l'article 3, paragraphe 2

7. Circonstances de la violation de données à caractère personnel, conformément à l'article 3, paragraphe 2

8. Mesures prises par le fournisseur pour remédier à la violation de données à caractère personnel

9. Mesures recommandées par le fournisseur pour atténuer les préjudices potentiels