REGULAMENTOS

REGULAMENTO (UE) N.º 611/2013 DA COMISSÃO

de 24 de junho de 2013

relativo às medidas aplicáveis à notificação da violação de dados pessoais em conformidade com a Diretiva 2002/58/CE do Parlamento Europeu e do Conselho relativa à privacidade e às comunicações eletrónicas

A COMISSÃO EUROPEIA,

Tendo em conta o Tratado sobre o Funcionamento da União Europeia,

Tendo em conta a Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas (Directiva relativa à privacidade e às comunicações electrónicas) [1], nomeadamente o artigo 4.º, n.º 5,

Tendo consultado a Agência Europeia para a Segurança das Redes e da Informação (ENISA),

Tendo consultado o grupo de trabalho para a proteção das pessoas no que diz respeito ao tratamento de dados pessoais, instituído pelo artigo 29.º da Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados [2] (grupo de trabalho do artigo 29.º),

Tendo consultado a Autoridade Europeia para a Proteção de Dados (AEPD),

Considerando o seguinte:

(1) A Diretiva 2002/58/CE prevê a harmonização das disposições nacionais necessárias para garantir um nível equivalente de proteção dos direitos e liberdades fundamentais, nomeadamente o direito à privacidade e à confidencialidade, no que respeita ao tratamento de dados pessoais no setor das comunicações eletrónicas, e para garantir a livre circulação desses dados e dos equipamentos e serviços de comunicações eletrónicas na União.

(2) Nos termos do artigo 4.º da Diretiva 2002/58/CE, os operadores de serviços de comunicações eletrónicas publicamente disponíveis são obrigados a comunicar às autoridades nacionais competentes e, em determinados casos, também aos assinantes e às outras pessoas em causa, a violação de dados pessoais. A violação de dados pessoais é definida no artigo 2.º, alínea i), da Diretiva 2002/58/CE como uma violação da segurança que provoca, de modo acidental ou ilegal, a destruição, a perda, a alteração, a divulgação ou acesso não autorizados a dados pessoais transmitidos, armazenados ou de outro modo tratados no contexto da prestação de serviços de comunicações eletrónicas publicamente disponíveis na União.

(3) Para assegurar coerência na aplicação das medidas a que se refere o artigo 4.º, n.ºs 2, 3 e 4, da Diretiva 2002/58/CE, o n.º 5 do mesmo artigo confere à Comissão o poder de adotar medidas técnicas de execução respeitantes às circunstâncias, ao formato e aos procedimentos aplicáveis aos requisitos de informação e notificação a que se refere aquele artigo.

(4) A existência de requisitos nacionais diferentes nesta matéria pode originar insegurança jurídica, procedimentos mais complexos e morosos e custos administrativos significativos para os operadores com atividades transfronteiras. Por conseguinte, a Comissão considera ser necessário adotar tais medidas técnicas de execução.

(5) O presente regulamento abrange apenas a notificação dos casos de violação de dados pessoais, pelo que não estabelece medidas técnicas de execução do artigo 4.º, n.º 2, da Diretiva 2002/58/CE, respeitantes à informação a transmitir aos assinantes no caso de um determinado risco de violação da segurança da rede.

(6) O artigo 4.º, n.º 3, primeiro parágrafo, da Diretiva 2002/58/CE determina que os operadores devem comunicar à autoridade nacional competente todos os casos de violação de dados pessoais. Por conseguinte, não deve ser dada ao operador a possibilidade de optar por não comunicar essas violações. No entanto, isso não deve impedir a autoridade nacional competente de atribuir prioridade à investigação de determinados casos de violação, como melhor entender, em conformidade com a legislação aplicável, e de tomar as medidas necessárias para evitar que a comunicação de violações de dados pessoais seja excessiva ou insuficiente.

(7) Convém prever um sistema de notificação dos casos de violação de dados pessoais à autoridade nacional competente, que compreenda, caso estejam preenchidas determinadas condições, várias fases, cada uma delas submetida a um determinado prazo. Este sistema visa garantir que a autoridade nacional competente é informada assim que possível e de forma tão circunstanciada quanto possível, sem, no entanto, dificultar indevidamente os esforços do operador para investigar a violação e tomar as medidas necessárias para a confinar e para obviar às suas consequências.

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

(8) A simples suspeita de que ocorreu uma violação de dados pessoais ou a simples deteção de um incidente sobre o qual não há informações suficientes, apesar de todos os esforços do operador no sentido de as obter, não é suficiente, para efeitos do presente regulamento, para se considerar que foi detetada uma violação de dados pessoais. A este respeito, deve ser dada especial atenção à disponibilidade das informações a que se refere o anexo I.

(9) No contexto da aplicação do presente regulamento, as autoridades nacionais competentes em causa devem cooperar nos casos de violação de dados pessoais de dimensão transfronteiras.

(10) O presente regulamento não prevê especificações suplementares do inventário dos casos de violação de dados pessoais que os operadores devem manter, dado que o artigo 4.º da Diretiva 2002/58/CE especifica o seu conteúdo de modo exaustivo. No entanto, os operadores podem tomar como referência o presente regulamento para determinarem o formato do inventário.

(11) Todas as autoridades nacionais competentes devem disponibilizar aos operadores meios eletrónicos seguros para estes notificarem os casos de violação de dados pessoais segundo um formato comum, baseado numa norma, por exemplo, a XML, que inclua as informações enumeradas no anexo I nas línguas pertinentes, de modo a que todos os operadores na União possam seguir procedimentos de notificação similares, independentemente do local onde se encontrem estabelecidos ou do local onde tenha ocorrido a violação de dados pessoais. A este respeito, a Comissão deve facilitar a aplicação de meios eletrónicos seguros, organizando para tal, quando necessário, reuniões com as autoridades nacionais competentes.

(12) Para se determinar se um caso de violação de dados pessoais é suscetível de afetar negativamente os dados pessoais ou a privacidade do assinante ou de outra pessoa em causa, deve ter-se em conta, em especial, a natureza e o teor dos dados pessoais em causa, nomeadamente quando se trata de informações financeiras, como os dados relativos a cartões de crédito ou a contas bancárias, de dados das categorias especiais a que se refere o artigo 8.º, n.º 1, da Diretiva 95/46/CE ou de determinados dados especificamente relacionados com o fornecimento de serviços de telefonia ou de Internet, ou seja, dados de correio eletrónico, dados de localização, dados de acesso à Internet, histórico da navegação na Internet e listas discriminadas de chamadas.

(13) Em circunstâncias excecionais, o operador deve ter a possibilidade de adiar a notificação ao assinante ou a outra pessoa em causa, caso essa notificação possa pôr em risco a eficácia da investigação da violação de dados pessoais. Neste contexto, poderão ser consideradas circunstâncias excecionais as investigações criminais, bem como outras violações de dados pessoais que, embora não constituam crimes graves, justificam o adiamento da notificação. De qualquer modo, deve incumbir à autoridade nacional competente determinar, em cada caso e à luz das circunstâncias, se o adiamento é ou não aceitável.

(14) Os operadores, embora devam ter dados de contacto dos seus assinantes, dada a sua relação contratual direta, podem não ter dados de contacto de outras pessoas afetadas pela violação de dados pessoais. Nesses casos, o operador deve poder notificar essas pessoas inicialmente através de anúncios nos mais importantes meios de comunicação social nacionais ou regionais, nomeadamente jornais, seguindo-se, assim que possível, a notificação individual em conformidade com o presente regulamento. Consequentemente, o operador não é estritamente obrigado a proceder à notificação através dos meios de comunicação social, mas pode decidir fazê-lo durante o processo de identificação de todas as pessoas afetadas.

(15) A informação sobre a violação de dados deve incidir nessa violação e não estar associada a informações sobre outras matérias. Por exemplo, a inclusão de informações sobre um caso de violação de dados pessoais numa fatura normal não deve ser considerada um meio adequado de notificação dessa violação.

(16) O presente regulamento não estabelece medidas tecnológicas específicas de proteção que justifiquem uma derrogação da obrigação de notificar os casos de violação de dados pessoais aos assinantes ou às outras pessoas em causa, pois tais medidas podem, com o tempo, mudar, em função do progresso tecnológico. A Comissão deve, contudo, poder publicar uma lista indicativa dessas medidas tecnológicas específicas de proteção em consonância com as práticas correntes.

(17) A aplicação de métodos de cifragem ou *hashing* não deve ser considerada, por si só, suficiente para os operadores poderem alegar, de um modo mais geral, que cumpriram o dever de segurança geral estabelecido no artigo 17.º da Diretiva 95/46/CE. A este respeito, os operadores devem igualmente pôr em prática medidas organizativas e técnicas adequadas para prevenir, detetar e bloquear a violação de dados pessoais. Os operadores devem avaliar os riscos residuais que possam existir após a realização das operações de controlo, para melhor entenderem como e onde poderá ocorrer a violação de dados pessoais.

(18) Caso o operador recorra a outro operador para realizar parte do serviço, designadamente no que respeita às

funções de faturação ou gestão, esse outro operador, que não tem qualquer relação contratual direta com o utilizador final, não deve ser obrigado a emitir notificações em caso de violação de dados pessoais; deve, antes, alertar e informar o operador com o qual tem uma relação contratual direta. Esta regra deve aplicar-se igualmente no contexto da oferta grossista de serviços de comunicações eletrónicas, em que, normalmente, o operador grossista não tem uma relação contratual direta com o utilizador final.

(19) A Diretiva 95/46/CE define um quadro geral para a proteção de dados pessoais na União Europeia. A Comissão apresentou uma proposta de regulamento do Parlamento Europeu e do Conselho que substitui a Diretiva 95/46/CE (Regulamento Proteção de Dados). Esse regulamento proposto estabelece a obrigação, para todos os responsáveis pelo tratamento de dados, de notificação dos casos de violação de dados pessoais, com base no artigo 4.º, n.º 3, da Diretiva 2002/58/CE. O presente regulamento da Comissão é plenamente coerente com essa medida proposta.

(20) O Regulamento Proteção de Dados proposto prevê também um pequeno número de adaptações técnicas da Diretiva 2002/58/CE, decorrentes da transformação da Diretiva 95/46/CE num regulamento. Os efeitos jurídicos substantivos do novo regulamento na Diretiva 2002/58/CE serão objeto de análise pela Comissão.

(21) A aplicação do presente regulamento deve ser avaliada três anos após a sua entrada em vigor e o seu conteúdo deve ser revisto à luz do quadro jurídico em vigor nessa altura, inclusive do Regulamento Proteção de Dados proposto. A revisão do presente regulamento deve ser associada, se possível, às futuras revisões da Diretiva 2002/58/CE.

(22) A aplicação do presente regulamento pode ser avaliada tomando como base, nomeadamente, as estatísticas, mantidas pelas autoridades nacionais competentes, dos casos de violação de dados pessoais que lhes tenham sido notificados. Essas estatísticas poderão incluir, por exemplo, informações sobre o número de casos de violação de dados pessoais notificados à autoridade nacional competente, o número de casos de violação de dados pessoais notificados aos assinantes ou às outras pessoas em causa, o tempo que foi necessário para solucionar cada caso de violação de dados pessoais e as medidas tecnológicas de proteção eventualmente adotadas. Tais estatísticas devem fornecer à Comissão e aos Estados-Membros dados coerentes e comparáveis, mas não devem revelar a identidade dos operadores notificantes nem a dos assinantes ou outras pessoas afetadas. A Comissão pode ainda organizar, para esse efeito, reuniões periódicas com as autoridades nacionais competentes e com outras partes interessadas.

(23) As medidas previstas no presente regulamento estão conformes com o parecer do Comité das Comunicações,

ADOTOU O PRESENTE REGULAMENTO:

Artigo 1.º

Âmbito de aplicação

O presente regulamento é aplicável à notificação, pelos operadores de serviços de comunicações eletrónicas publicamente disponíveis («os operadores»), dos casos de violação de dados pessoais.

Artigo 2.º

Notificação à autoridade nacional competente

1. O operador deve notificar todos os casos de violação de dados pessoais à autoridade nacional competente.

2. O operador deve notificar a violação de dados pessoais à autoridade nacional competente no prazo de 24 horas após a deteção dessa violação, se possível.

O operador deve incluir na sua notificação à autoridade nacional competente as informações enumeradas no anexo I.

Considera-se que a deteção de uma violação de dados pessoais teve lugar quando o operador obteve conhecimento suficiente de que ocorreu um incidente de segurança que afetou dados pessoais para efetuar uma notificação pertinente, como previsto no presente regulamento.

3. Caso não estejam disponíveis todas as informações enumeradas no anexo I e seja necessária uma investigação suplementar da violação de dados pessoais, o operador deve poder proceder a uma primeira notificação à autoridade nacional competente no prazo de 24 horas após a deteção dessa violação. Essa primeira notificação deve incluir as informações enumeradas na secção 1 do anexo I. O operador deve proceder a uma segunda notificação à autoridade nacional competente assim que possível, o mais tardar três dias após a primeira notificação. Essa segunda notificação deve incluir as informações enumeradas na secção 2 do anexo I e, se necessário, atualizar as informações já fornecidas.

Se, apesar da investigação efetuada, não estiver em condições de comunicar todas as informações no prazo de três dias a contar da primeira notificação, o operador deve comunicar, dentro desse prazo, todas as informações de que disponha e apresentar à autoridade nacional competente uma justificação fundamentada para o atraso da notificação das informações restantes. O operador deve, assim que possível, comunicar essas informações restantes à autoridade nacional competente e, se necessário, atualizar as informações já fornecidas.

4. A autoridade nacional competente deve fornecer a todos os operadores estabelecidos no Estado-Membro em causa meios eletrónicos seguros para a notificação das violações de dados pessoais e informações sobre os procedimentos de acesso e utilização dos mesmos. Se necessário, a Comissão convoca reuniões com as autoridades nacionais competentes, para facilitar a aplicação da presente disposição.

5. Caso a violação de dados pessoais afete assinantes ou outras pessoas de outros Estados-Membros, a autoridade nacional competente deve informar as restantes autoridades nacionais em causa.

Para facilitar a aplicação da presente disposição, a Comissão cria e mantém uma lista das autoridades nacionais competentes e dos pontos de contacto adequados.

Artigo 3.º

Notificação ao assinante ou a outra pessoa em causa

1. Caso a violação de dados pessoais seja suscetível de afetar negativamente os dados pessoais ou a privacidade de um assinante ou de outra pessoa, o operador deve notificar essa violação não só à autoridade nacional competente, como prevê o artigo 2.º, mas também ao assinante ou à outra pessoa em causa.

2. Para se determinar se uma violação de dados pessoais é suscetível de afetar negativamente os dados pessoais ou a privacidade de um assinante ou de outra pessoa em causa, devem ter-se em conta, em especial, as seguintes circunstâncias:

a) a natureza e o teor dos dados pessoais em causa, nomeadamente quando se trata de informações financeiras, de dados das categorias especiais a que se refere o artigo 8.º, n.º 1, da Diretiva 95/46/CE, ou ainda de dados de localização, dados de acesso à Internet, histórico da navegação na Internet, dados de correio eletrónico e listas discriminadas de chamadas;

b) as prováveis consequências da violação de dados pessoais para o assinante ou outra pessoa em causa, nomeadamente quando essa violação pode conduzir ao roubo ou à usurpação de identidade, a danos físicos ou psicológicos, a humilhações ou a prejuízos para a reputação; e ainda

c) as circunstâncias da violação de dados pessoais, em especial quando esses dados foram roubados ou o operador tem conhecimento de que os dados se encontram na posse de terceiros não autorizados.

3. A notificação ao assinante ou a outra pessoa em causa deve ser efetuada sem demora indevida após a deteção da violação de dados pessoais, como previsto no artigo 2.º, n.º 2, terceiro parágrafo. Tal notificação é independente da notificação da violação de dados pessoais à autoridade nacional competente, a que se refere o artigo 2.º.

4. O operador deve incluir na sua notificação ao assinante ou a outra pessoa em causa as informações enumeradas no anexo II. A notificação ao assinante ou a outra pessoa em causa deve ser feita numa linguagem clara e facilmente compreensível. O operador não deve aproveitar a notificação para promover ou publicitar serviços novos ou suplementares.

5. Em circunstâncias excecionais, caso a notificação ao assinante ou a outra pessoa em causa possa pôr em risco a eficácia da investigação da violação de dados pessoais, o operador pode, com o acordo da autoridade nacional competente, adiar a notificação ao assinante ou a outra pessoa em causa até ao momento em que a autoridade nacional competente considere ser possível notificar a violação de dados pessoais em conformidade com o presente artigo.

6. O operador deve notificar a violação de dados pessoais ao assinante ou a outra pessoa em causa mediante uma comunicação que assegure a rápida receção das informações e que seja convenientemente protegida, segundo as práticas mais avançadas. A comunicação deve dizer respeito unicamente à violação, não devendo incluir informações sobre outras matérias.

7. Se, apesar dos esforços significativos realizados, não estiver em condições de identificar, no prazo previsto no n.º 3, todas as pessoas que possam ter sido negativamente afetadas pela violação de dados pessoais, o operador que tem uma relação contratual direta com o utilizador final pode notificar, dentro daquele prazo, essas pessoas, através de anúncios nos mais importantes meios de comunicação social, nacionais ou regionais, dos Estados-Membros em causa. Esses anúncios devem incluir as informações enumeradas no anexo II, se necessário de forma condensada. Nesse caso, o operador deve continuar a envidar todos os esforços para identificar aquelas pessoas e lhes transmitir as informações enumeradas no anexo II assim que possível.

Artigo 4.º

Medidas tecnológicas de proteção

1. Em derrogação ao disposto no artigo 3.º, n.º 1, a notificação de uma violação de dados pessoais a um assinante ou a outra pessoa em causa não é necessária se o operador provar cabalmente à autoridade nacional competente que adotou as medidas tecnológicas de proteção adequadas e que essas medidas foram aplicadas aos dados eventualmente afetados pela violação. Essas medidas tecnológicas de proteção devem tornar os dados ininteligíveis para qualquer pessoa que não esteja autorizada a aceder aos mesmos.

2. Considera-se que os dados são ininteligíveis se:

a) tiverem sido cifrados de forma segura, com um algoritmo normalizado e a chave utilizada para decifrar os dados não tiver sido afetada por qualquer falha de segurança e tiver sido gerada de tal modo que não possa ser determinada por meios tecnológicos disponíveis para qualquer pessoa que não esteja autorizada a aceder a essa chave; ou

b) tiverem sido substituídos pelos seus valores calculados por meio de uma função *hash* criptográfica normalizada com chave, a chave utilizada para a transformação dos dados pela função *hash* não tiver sido afetada por qualquer falha de segurança e essa chave tiver sido gerada de tal modo que não possa ser determinada por meios tecnológicos disponíveis para qualquer pessoa que não esteja autorizada a aceder a essa chave.

3. A Comissão, tendo consultado as autoridades nacionais competentes através do grupo de trabalho do artigo 29.º, a Agência Europeia para a Segurança das Redes e da Informação e a Autoridade Europeia para a Proteção de Dados, pode publicar uma lista indicativa das medidas tecnológicas de proteção adequadas a que se refere o n.º 1, em consonância com as práticas correntes.

Artigo 5.º

Recurso a outro operador

Caso outro operador que não tenha uma relação contratual direta com os assinantes seja contratado para fornecer parte do serviço de comunicações eletrónicas, esse outro operador deve informar imediatamente o operador contratante de qualquer violação de dados pessoais.

Artigo 6.º

Relatório e revisão

No prazo de três anos a contar da entrada em vigor do presente regulamento, a Comissão apresenta um relatório sobre a aplicação do presente regulamento, a sua eficácia e o seu impacto nos operadores, nos assinantes e nas outras pessoas em causa. Com base nesse relatório, a Comissão procede à revisão do presente regulamento.

Artigo 7.º

Entrada em vigor

O presente regulamento entra em vigor em 25 de agosto de 2013.

O presente regulamento é obrigatório em todos os seus elementos e diretamente aplicável em todos os Estados-Membros.

Feito em Bruxelas, em 24 de junho de 2013.

Pela Comissão

O Presidente

José Manuel BARROSO

ANEXO I

Teor da notificação à autoridade nacional competente

Secção 1

Identificação do operador

1. Nome do operador

2. Identidade e dados de contacto do responsável pela proteção de dados ou outro ponto de contacto onde possam ser obtidas informações suplementares

3. Indicação de que se trata da primeira ou da segunda notificação

Informações iniciais sobre a violação de dados pessoais (a fornecer em notificações posteriores, consoante o caso)

4. Data e hora do incidente (caso sejam conhecidas; se necessário, pode indicar-se uma estimativa) e da deteção do incidente

5. Circunstâncias da violação de dados pessoais (por exemplo, perda, roubo, cópia)

6. Natureza e teor dos dados pessoais em causa

7. Medidas técnicas e organizativas aplicadas (ou a aplicar) pelo operador aos dados pessoais afetados

8. Recurso a outros operadores que tenham desempenhado um papel nesta matéria (se for o caso)

Secção 2

Informações suplementares sobre a violação de dados pessoais

9. Resumo do incidente que deu origem à violação de dados pessoais (incluindo o local físico da violação e os meios de armazenamento envolvidos):

10. Número de assinantes ou outras pessoas em causa

11. Eventuais consequências e efeitos negativos para os assinantes ou as outras pessoas em causa

12. Medidas técnicas e organizativas adotadas pelo operador para atenuar os eventuais efeitos negativos

Eventual notificação suplementar aos assinantes ou às outras pessoas em causa

13. Teor da notificação

14. Meios de comunicação utilizados

15. Número de assinantes ou outras pessoas em causa notificados

Eventuais questões transfronteiras

16. Violação de dados pessoais que envolva assinantes ou outras pessoas noutros Estados-Membros

17. Notificação às restantes autoridades nacionais competentes

ANEXO II

Teor da notificação ao assinante ou a outra pessoa em causa

1. Nome do operador

2. Identidade e dados de contacto do responsável pela proteção de dados ou outro ponto de contacto onde possam ser obtidas informações suplementares

3. Resumo do incidente que deu origem à violação de dados pessoais

4. Data estimada do incidente

5. Natureza e teor dos dados pessoais em causa, como previsto no artigo 3.º, n.º 2

6. Prováveis consequências da violação de dados pessoais para o assinante ou outra pessoa em causa, como previsto no artigo 3.º, n.º 2

7. Circunstâncias da violação de dados pessoais, como previsto no artigo 3.º, n.º 2

8. Medidas adotadas pelo operador para dar resposta à violação de dados pessoais

9. Medidas recomendadas pelo operador para atenuar os eventuais efeitos negativos