VERORDENINGEN

VERORDENING (EU) Nr. 611/2013 VAN DE COMMISSIE

van 24 juni 2013

betreffende maatregelen voor het melden van inbreuken in verband met persoonsgegevens op grond van Richtlijn 2002/58/EG van het Europees Parlement en de Raad betreffende privacy en elektronische communicatie

DE EUROPESE COMMISSIE,

Gezien het Verdrag betreffende de werking van de Europese Unie,

Gezien Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie) ([1]), en met name artikel 4, lid 5,

Na raadpleging van het Europees Agentschap voor netwerk- en informatiebeveiliging (Enisa),

Na raadpleging van de Groep voor de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens, ingesteld bij artikel 29 van Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens ([2]) (de Groep artikel 29),

Na raadpleging van de Europese Toezichthouder voor gegevensbescherming (EDPS),

Overwegende hetgeen volgt:

(1) Richtlijn 2002/58/EG voorziet in de harmonisering van de nationale bepalingen die nodig zijn om te zorgen voor een gelijk niveau van bescherming van fundamentele rechten en vrijheden, met name het recht op een persoonlijke levenssfeer en het vertrouwelijke karakter in verband met de verwerking van persoonsgegevens in de elektronischecommunicatiesector en om het vrije verkeer van dergelijke data en van de elektronischecommunicatieapparatuur en -diensten in de Unie te garanderen.

(2) Overeenkomstig artikel 4 van Richtlijn 2002/58/EG moeten aanbieders van openbare elektronischecommunicatiediensten de nationale bevoegde autoriteiten en in sommige gevallen ook de betrokken abonnees en andere personen in kennis stellen van inbreuken in verband met persoonsgegevens. Inbreuken in verband met persoonsgegevens worden in artikel 2, onder i), van Richtlijn 2002/58/EG omschreven als inbreuken op de beveiliging die resulteren in een accidentele of onwettige vernietiging, wijziging, niet-geautoriseerde vrijgave van of toegang tot persoonsgegevens die zijn verstuurd, opgeslagen of anderszins verwerkt in verband met de levering van een openbare elektronischecommunicatiedienst in de Unie.

(3) Om een samenhangende tenuitvoerlegging te waarborgen van de in artikel 4, leden 2, 3 en 4, van Richtlijn 2002/58/EG bedoelde maatregelen, kan de Commissie op grond van artikel 4, lid 5, technische uitvoeringsmaatregelen vaststellen in verband met de omstandigheden, het formaat en de procedures die gelden voor de in dit artikel bedoelde informatieverstrekkings- en kennisgevingseisen.

(4) Wanneer deze eisen per land verschillen, kan dit leiden tot rechtsonzekerheid, meer complexe en omslachtige procedures en aanzienlijke administratieve kosten voor aanbieders die grensoverschrijdend actief zijn. De Commissie vindt het derhalve noodzakelijk dergelijke technische uitvoeringsmaatregelen vast te stellen.

(5) Deze verordening heeft alleen betrekking op de melding van inbreuken in verband met persoonsgegevens en omvat dan ook geen technische uitvoeringsmaatregelen met betrekking tot de verplichting van artikel 4, lid 2, van Richtlijn 2002/58/EG om, wanneer er een bijzonder risico bestaat van inbreuken op de beveiliging van het netwerk, de abonnees hiervan in kennis te stellen.

(6) Uit artikel 4, lid 3, eerste alinea, van Richtlijn 2002/58/EG volgt dat aanbieders de bevoegde nationale autoriteit in kennis moeten stellen van alle inbreuken in verband met persoonsgegevens. Aanbieders mogen dan ook niet zelf bepalen of zij een inbreuk in verband met persoonsgegevens al dan niet aan de bevoegde nationale autoriteit melden. Dit mag de bevoegde nationale autoriteit echter niet verhinderen om naar eigen goeddunken voorrang te verlenen aan het onderzoek van bepaalde inbreuken in overeenstemming met het toepasselijk recht en passende maatregelen te nemen om over- of onderrapportering te voorkomen.

(7) Er moet dan ook een systeem worden vastgesteld voor het aanmelden van inbreuken in verband met persoonsgegevens aan de bevoegde nationale autoriteit dat, indien wordt voldaan aan bepaalde voorwaarden, bestaat uit verschillende fasen, met telkens een bepaalde termijn. Dit systeem moet ervoor zorgen dat de bevoegde nationale autoriteit zo vroeg en zo volledig mogelijk in kennis wordt gesteld zonder dat de aanbieder daarbij onnodig wordt gehinderd bij zijn pogingen om de inbreuk te onderzoeken en de nodige maatregelen te treffen om de inbreuk te beperken en de gevolgen ervan te verhelpen.

([1]) PB L 201 van 31.7.2002, blz. 37.
([2]) PB L 281 van 23.11.1995, blz. 31.

(8) Noch een simpel vermoeden dat een inbreuk in verband met persoonsgegevens heeft plaatsgevonden, noch een simpele opsporing van een incident zonder dat voldoende informatie beschikbaar is, ondanks het feit de aanbieder hiertoe al het mogelijke heeft gedaan, is voldoende om ervan uit te gaan dat een inbreuk in verband met persoonsgegevens is ontdekt in de zin van deze verordening. In dit verband moet met name worden gelet op de beschikbaarheid van de in Bijlage I bedoelde informatie.

(9) In de context van de toepassing van deze verordening moeten de bevoegde nationale autoriteiten hun medewerking verlenen in gevallen van inbreuken in verband met persoonsgegevens met een grensoverschrijdende dimensie.

(10) Een aanvullende specificatie van de inventaris van inbreuken op persoonsgegevens die aanbieders moeten bijhouden is op grond van deze verordening niet verplicht omdat de inhoud hiervan al uitvoerig is beschreven in artikel 4 van Richtlijn 2002/58/EG. Om het formaat van de inventaris te bepalen kunnen aanbieders echter gebruikmaken van deze verordening.

(11) Alle bevoegde nationale autoriteiten moeten beveiligde elektronische middelen ter beschikking stellen zodat aanbieders in een gemeenschappelijk formaat, gebaseerd op een norm als XML, inbreuken in verband met persoonsgegevens kunnen melden, met inbegrip van de in bijlage I vermelde informatie in de desbetreffende talen, zodat alle aanbieders in de Unie een soortgelijke kennisgevingsprocedure kunnen volgen, ongeacht hun vestigingsplaats of de plaats waar de inbreuk in verband met persoonsgegevens plaatsvond. In dit verband moet de Commissie indien noodzakelijk de tenuitvoerlegging van beveiligde elektronische middelen vergemakkelijken door bijeenkomsten te organiseren met de bevoegde nationale autoriteiten.

(12) Om na te gaan of een inbreuk op persoonsgegevens wellicht negatieve gevolgen kan hebben voor de persoonsgegevens of de privacy van een abonnee of een ander persoon, moet vooral rekening worden gehouden met de aard en inhoud van de betrokken persoonsgegevens, met name wanneer de gegevens betrekking hebben op financiële informatie zoals creditcardgegevens of informatie met betrekking tot een bankrekening; de bijzondere categorieën gegevens van artikel 8, lid 1, van Richtlijn 95/46/EG; en bepaalde gegevens die specifiek betrekking hebben op het verstrekken van telefoon- of internetdiensten, dat wil zeggen, e-mail gegevens, locatiegegevens, internetlogbestanden, webbrowsegeschiedenis en gespecificeerde lijsten van oproepen.

(13) In uitzonderlijke omstandigheden moet, wanneer kennisgeving aan een abonnee of een andere persoon de doeltreffendheid van het onderzoek naar de inbreuk in verband met persoonsgegevens in gevaar zou brengen, de aanbieder de kennisgeving aan een abonnee of een persoon kunnen uitstellen. Uitzonderlijke omstandigheden zijn in deze context niet alleen strafrechtelijke onderzoeken maar ook andere inbreuken in verband met persoonsgegevens die geen ernstig delict vormen maar uitstel van de termijn voor kennisgeving wel kunnen rechtvaardigen. Het is in ieder geval aan de bevoegde nationale autoriteit om per geval en rekening houdend met de omstandigheden te beoordelen of uitstel gerechtvaardigd is dan wel of kennisgeving noodzakelijk is.

(14) Aanbieders moeten weliswaar in het bezit zijn van contactgegevens van hun abonnees, gezien hun rechtstreekse contractuele relatie, maar niet van dergelijke gegevens van andere personen voor wie inbreuk op persoonsgegevens ook gevolgen kunnen hebben. In dat geval moet de aanbieder de personen in kwestie zo spoedig mogelijk, in eerste instantie via advertenties in de voornaamste nationale of regionale media, zoals kranten, en vervolgens, overeenkomstig onderhavige verordening, via een individuele kennisgeving, hiervan op de hoogte kunnen brengen. De aanbieder is derhalve niet verplicht kennisgeving te doen via de media, maar kan hiertoe desgewenst wel overgaan wanneer hij nog bezig is met het identificeren van de betrokkenen.

(15) De informatie over de inbreuk mag alleen betrekking hebben op de inbreuk en mag geen verband houden met informatie over andere onderwerpen. Het bijsluiten van informatie over een inbreuk op persoonsgegevens in een periodieke factuur kan derhalve niet worden beschouwd als een adequate manier om kennisgeving te doen van een inbreuk in verband met persoonsgegevens.

(16) In deze verordening worden geen specifieke maatregelen inzake technologische bescherming vastgesteld die een afwijking rechtvaardigen van de verplichting om abonnees of andere personen in kennis te stellen van inbreuken op persoonsgegevens omdat dergelijke maatregelen met de technische vooruitgang kunnen evolueren. Wel moet de Commissie, overeenkomstig de huidige praktijken, een indicatieve lijst kunnen publiceren van dergelijke specifieke maatregelen inzake technologische bescherming.

(17) Aanbieders kunnen zich niet alleen op encryptie of hashing beroepen om te verklaren dat zij voldaan hebben aan de algemene beveiligingsverplichting van artikel 17 van Richtlijn 95/46/EG. Aanbieders moeten in dit verband ook adequate organisatorische en technische maatregelen nemen om inbreuk in verband met persoonsgegevens te voorkomen, op te sporen en te blokkeren. Aanbieders moeten elk risico dat na controles eventueel nog bestaat, onderzoeken om na te gaan waar inbreuken op persoonsgegevens zich eventueel kunnen voordoen.

(18) Wanneer de aanbieder voor het uitvoeren van een deel van zijn diensten gebruik maakt van een andere aanbieder, bijvoorbeeld voor facturering of managementdiensten, is die andere aanbieder, die geen rechtstreekse contractuele overeenkomst heeft met de eindgebruiker, niet verplicht kennisgeving te doen van inbreuken in verband met persoonsgegevens. Deze derde partij moet de inbreuk echter wel signaleren en de aanbieder, waarmee

hij een rechtstreekse contractuele overeenkomst heeft, hiervan in kennis stellen. Dit geldt ook in de context van wholesalelevering van elektronischecommunicatiediensten, waar de wholesaleaanbieder normaliter geen rechtstreekse contractuele overeenkomst met de eindgebruiker heeft.

(19) In Richtlijn 95/46/EG wordt een definitie gegeven van een algemeen kader voor de bescherming van persoonsgegevens in de Europese Unie. De Commissie heeft een voorstel ingediend voor een verordening van het Europees Parlement en de Raad die de plaats moet innemen van Richtlijn 95/46/EG (de gegevensbeschermingsverordening). De voorgestelde gegevensbeschermingsverordening zou alle voor de verwerking van gegevens verantwoordelijke personen ertoe verplichten om, voortbouwend op artikel 4, lid 3, van Richtlijn 2002/58/EG, kennisgeving te doen van inbreuken in verband met persoonsgegevens. De onderhavige verordening van de Commissie is volledig in overeenstemming met deze voorgestelde maatregel.

(20) De voorgestelde gegevensbeschermingsverordening houdt ook een beperkt aantal technische aanpassingen in van Richtlijn 2002/58/EG teneinde rekening te houden met de omvorming van Richtlijn 95/46/EG tot een verordening. De inhoudelijke juridische gevolgen van de nieuwe verordening voor Richtlijn 2002/58/EG zullen door de Commissie worden geëvalueerd.

(21) De toepassing van deze verordening moet drie jaar na de inwerkingtreding ervan worden geëvalueerd en de inhoud moet worden herzien in het licht van het juridisch kader dat op dat moment van toepassing is, met inbegrip van de voorgestelde gegevensbeschermingsverordening. De herziening van deze verordening moet waar mogelijk worden gekoppeld aan een eventuele toekomstige herziening van Richtlijn 2002/58/EG.

(22) De toepassing van deze verordening kan onder meer worden beoordeeld op basis van eventuele door de bevoegde nationale autoriteiten bijgehouden statistieken over bij hen aangemelde inbreuken op persoonsgegevens. Deze statistieken kunnen bijvoorbeeld informatie bevatten over het aantal bij de bevoegde nationale autoriteit aangemelde inbreuken, het aantal inbreuken in verband met persoonsgegevens waarvan kennisgeving werd gedaan bij de abonnee of een andere persoon, de tijd die nodig was om de inbreuk op persoonsgegevens op te lossen en informatie over genomen maatregelen inzake technologische bescherming. Deze statistieken moeten de Commissie en de lidstaten consistente en vergelijkbare statistische gegevens verstrekken en de identiteit van noch de aanbieder die de inbreuk aanmeldt, noch de abonnee of andere personen voor wie de inbreuk ook gevolgen kunnen hebben, onthullen. De Commissie kan met het oog hierop ook periodiek bijeenkomen met de bevoegde nationale autoriteiten en andere betrokkenen.

(23) De in deze verordening vervatte maatregelen zijn in overeenstemming met het advies van het Comité voor communicatie,

HEEFT DE VOLGENDE VERORDENING VASTGESTELD:

Artikel 1

Toepassingsgebied

Deze verordening is van toepassing op de aanmelding van inbreuken in verband met persoonsgegevens door aanbieders van openbare elektronischecommunicatiediensten („de aanbieder").

Artikel 2

Aanmelding bij de bevoegde nationale autoriteit

1. De aanbieder stelt de bevoegde nationale autoriteit in kennis van alle inbreuken in verband met persoonsgegevens.

2. De aanbieder stelt de bevoegde nationale autoriteit waar mogelijk uiterlijk 24 uur na opsporing in kennis van de inbreuk in verband met persoonsgegevens.

De aanbieder vermeldt in zijn kennisgeving aan de bevoegde nationale autoriteit de in bijlage I vermelde informatie.

Opsporing van een inbreuk in verband met persoonsgegevens wordt geacht te hebben plaatsgevonden zodra de aanbieder zich voldoende bewust is van een veiligheidsincident dat heeft geleid tot een inbreuk in verband met persoonsgegevens, om een zinvolle kennisgeving te kunnen doen, zoals vereist is op grond van deze verordening.

3. Wanneer niet alle in bijlage I vermelde informatie beschikbaar is en de inbreuk in verband met persoonsgegevens verder onderzoek vergt, kan de aanbieder de bevoegde nationale autoriteit niet later dan 24 uur na opsporing van de inbreuk in verband met persoonsgegevens voorlopige kennisgeving hiervan doen. Deze voorlopige kennisgeving aan de bevoegde nationale autoriteit omvat de in deel 1 van bijlage I vermelde informatie. De aanbieder doet de bevoegde nationale autoriteit zo spoedig mogelijk, en ten laatste binnen drie dagen volgend op de voorlopige kennisgeving, een tweede kennisgeving. Deze tweede kennisgeving omvat de in deel 2 van bijlage I vermelde informatie en eventueel bijgewerkte informatie.

Wanneer de aanbieder ondanks zijn onderzoek niet binnen drie dagen na de voorlopige kennisgeving alle informatie kan verstrekken, geeft hij de bevoegde nationale autoriteit alle informatie door die hij binnen die termijn heeft kunnen verzamelen en licht hij toe waarom de overige informatie laattijdig wordt ingediend. De aanbieder stelt de bevoegde nationale autoriteit zo spoedig mogelijk in kennis van de overige informatie en werkt deze waar nodig bij.

4. De bevoegde nationale autoriteit stelt alle in de desbetreffende lidstaat gevestigde aanbieders beveiligde elektronische middelen ter beschikking zodat zij inbreuken in verband met persoonsgegevens kunnen aanmelden en informatie over de procedures voor toegang tot en gebruik van deze middelen kunnen verstrekken. Indien nodig organiseert de Commissie vergaderingen met de bevoegde nationale autoriteiten om de toepassing van deze bepaling te vergemakkelijken.

5. Wanneer de inbreuk in verband met persoonsgegevens betrekking heeft op abonnees of andere personen in andere lidstaten dan die van de bevoegde nationale autoriteit die in kennis is gesteld van de inbreuk in verband met persoonsgegevens, informeert de bevoegde nationale autoriteit de andere betrokken nationale autoriteiten hierover.

Om de toepassing van deze bepaling te vergemakkelijken stelt de Commissie een lijst op van de bevoegde nationale autoriteiten en de desbetreffende contactpunten.

Artikel 3

Kennisgeving aan de abonnee of andere betrokkenen

1. Wanneer de inbreuk in verband met persoonsgegevens waarschijnlijk ook gevolgen zal hebben voor de persoonsgegevens of de privacy van een abonnee of een ander persoon, stelt de aanbieder, los van de in artikel 2 bedoelde kennisgeving, ook deze abonnee of andere persoon in kennis van de inbreuk in verband met persoonsgegevens.

2. Of een inbreuk in verband met persoonsgegevens waarschijnlijk ook negatieve gevolgen zal hebben voor de persoonsgegevens of de privacy van een abonnee of een ander persoon wordt beoordeeld op grond van met name de volgende omstandigheden:

a) de aard en de inhoud van de desbetreffende persoonsgegevens, met name wanneer het om financiële gegevens gaat die onder de bijzondere categorieën van artikel 8, lid 1, van Richtlijn 95/46/EG vallen, alsmede locatiegegevens, internetlogbestanden, webbrowsegeschiedenis, e-mailgegevens en gespecificeerde lijsten van oproepen;

b) de vermoedelijke gevolgen van de inbreuk op persoonsgegevens voor de betrokken abonnee of andere persoon, met name wanneer een inbreuk kan leiden tot bijvoorbeeld identiteitsdiefstal of -fraude, lichamelijke schade, ernstige vernedering of aantasting van de reputatie; alsmede

c) de omstandigheden van de inbreuk in verband met persoonsgegevens, met name wanneer de gegevens zijn gestolen of wanneer de aanbieder weet dat de gegevens in het bezit zijn van een niet-geautoriseerde derde.

3. De kennisgeving aan de abonnee of de andere persoon geschiedt zonder onnodige vertraging na opsporing van de inbreuk in verband met persoonsgegevens zoals beschreven in artikel 2, lid 2, derde alinea. Een dergelijke kennisgeving staat los van de kennisgeving van de inbreuk in verband met persoonsgegevens aan de bevoegde nationale autoriteit, als bedoeld in artikel 2.

4. De aanbieder voegt bij de kennisgeving aan de abonnee of de andere persoon de informatie van bijlage II. De kennisgeving aan de abonnee of de andere persoon moet zijn opgesteld in heldere en begrijpelijke taal. De aanbieder gebruikt de kennisgeving niet als een mogelijkheid om nieuwe of aanvullende diensten te bevorderen of als reclame.

5. In uitzonderlijke omstandigheden, kan de aanbieder, wanneer kennisgeving aan de abonnee of de andere persoon een correct onderzoek van de inbreuk in verband met persoonsgegevens in gevaar kan brengen, na toestemming van de bevoegde nationale autoriteit te hebben ontvangen, de kennisgeving aan de abonnee of de andere persoon uitstellen tot het moment waarop de bevoegde nationale autoriteit kennisgeving van de inbreuk in verband met persoonsgegevens overeenkomstig dit artikel mogelijk acht.

6. De aanbieder stelt de abonnee of de andere persoon in kennis van de inbreuk in verband met persoonsgegevens via een communicatiemiddel dat een snelle ontvangst van de informatie waarborgt en volgens de laatste technische ontwikkelingen is beveiligd. De informatie over de inbreuk heeft alleen betrekking op de inbreuk en kan niet aan een ander onderwerp worden gekoppeld.

7. Wanneer de aanbieder die een rechtstreekse contractuele overeenkomst met de eindgebruiker heeft, ondanks redelijke inspanningen er niet in is geslaagd binnen de in lid 3 vermelde termijn alle personen die waarschijnlijk negatieve gevolgen zullen ondervinden van de inbreuk in verband met persoonsgegevens te identificeren, kan hij hen binnen die termijn hiervan op de hoogte brengen via een advertentie in de grote nationale of regionale media in de betrokken lidstaten. Deze advertenties bevatten de in bijlage II vermelde informatie, eventueel in beknopte vorm. In dat geval blijft de aanbieder al het nodige doen om deze betrokkenen te identificeren en hen zo spoedig mogelijk kennisgeving te doen van de in bijlage II vermelde informatie.

Artikel 4

Maatregelen inzake technologische bescherming

1. In afwijking van artikel 3, lid 1, is kennisgeving van een inbreuk in verband met persoonsgegevens niet vereist als de aanbieder ten genoegen van de bevoegde nationale autoriteit heeft aangetoond dat zij passende maatregelen inzake technologische bescherming heeft genomen en dat die maatregelen zijn toegepast op de gegevens die door de inbreuk zijn getroffen. Dergelijke maatregelen inzake technologische bescherming maken de gegevens onbegrijpelijk voor personen zonder geautoriseerde toegang tot deze gegevens.

2. Gegevens worden als onbegrijpelijk beschouwd als ze:

a) op veilige wijze zijn versleuteld met een standaardalgoritme, de sleutel voor decryptie door geen enkele inbreuk gevaar heeft gelopen en de sleutel voor decryptie zodanig werd gegenereerd dat personen zonder geautoriseerde toegang de sleutel met de beschikbare technologische middelen niet kunnen vinden; of

b) zijn vervangen door een met een cryptografisch versleutelde hashfunctie berekende hashwaarde, de sleutel die hiervoor werd gebruikt door geen enkele inbreuk gevaar heeft gelopen en deze voor datahashing gebruikte sleutel zodanig is gegenereerd dat personen zonder geautoriseerde toegang de sleutel niet kunnen vinden met de beschikbare technologische middelen.

3. De Commissie kan, na raadpleging van de bevoegde nationale autoriteiten via de Groep artikel 29, het Europees Agentschap voor netwerk- en informatiebeveiliging en de Europese Toezichthouder voor gegevensbescherming, een indicatieve lijst bekendmaken van de in lid 1 bedoelde, volgens de huidige gebruiken passende maatregelen inzake technologische bescherming.

Artikel 5

Beroep doen op een andere aanbieder

Wanneer de levering van een deel van de elektronischecommunicatiediensten is uitbesteed aan een andere aanbieder die geen rechtstreekse contractuele overeenkomst met de abonnees heeft, moet deze andere aanbieder onmiddellijk de uitbestedende aanbieder op de hoogte brengen wanneer zich een inbreuk in verband met persoonsgegevens voordoet.

Artikel 6

Verslag en herziening

Binnen drie jaar na de inwerkingtreding van deze verordening brengt de Commissie een verslag uit over de toepassing van deze verordening, de doelmatigheid ervan en de impact op aanbieders, abonnees en andere betrokkenen. Op basis van dat verslag gaat de Commissie over tot een herziening van deze verordening.

Artikel 7

Inwerkingtreding

Deze verordening treedt in werking op 25 augustus 2013.

Deze verordening is verbindend in al haar onderdelen en is rechtstreeks toepasselijk in elke lidstaat.

Gedaan te Brussel, 24 juni 2013.

Voor de Commissie
De voorzitter
José Manuel BARROSO

BIJLAGE I

Inhoud van de kennisgeving aan de bevoegde nationale autoriteit

Deel 1

Gegevens van de aanbieder

1. Naam van de aanbieder

2. Naam en contactgegevens van de functionaris voor gegevensbescherming of ander contactpunt waar verdere informatie kan worden verkregen

3. Vermelding of het om een eerste of een tweede kennisgeving gaat

Voorlopige informatie over de inbreuk in verband met persoonsgegevens (die eventueel in latere kennisgevingen moet worden aangevuld)

4. Datum en tijdstip van het incident (indien bekend; eventueel bij benadering) en van het moment waarop dit werd vastgesteld

5. Omstandigheden van de inbreuk in verband met persoonsgegevens (bv. diefstal, verlies kopiëren)

6. Aard en inhoud van de desbetreffende gegevens

7. Technische en organisatorische maatregelen die met betrekking tot de desbetreffende persoonsgegevens door de aanbieder zijn (of worden) toegepast

8. Indien van toepassing, vermelding van de andere aanbieders waarop een beroep is gedaan

Deel 2

Verdere informatie over de inbreuk in verband met persoonsgegevens

9. Samenvatting van het incident dat de inbreuk in verband met persoonsgegevens heeft veroorzaakt (met inbegrip van de fysieke locatie waar de inbreuk plaatsvond en de betrokken opslagmedia)

10. Aantal betrokken abonnees of andere personen

11. Potentiële gevolgen en potentiële negatieve gevolgen voor abonnees of andere personen

12. Technische en organisatorische maatregelen die de aanbieder heeft genomen om de potentiële negatieve gevolgen tegen te gaan

Mogelijke aanvullende kennisgeving aan abonnees of andere personen

13. Inhoud van de kennisgeving

14. Gebruikte communicatiemiddelen

15. Aantal in kennis gestelde abonnees of andere personen

Mogelijke grensoverschrijdende problemen

16. Inbreuk in verband met persoonsgegevens die betrekking heeft op abonnees of andere personen in andere lidstaten

17. Kennisgeving aan andere bevoegde nationale autoriteiten

BIJLAGE II

Inhoud van de kennisgeving aan de abonnee of de andere persoon

1. Naam van de aanbieder

2. Naam en contactgegevens van de functionaris voor gegevensbescherming of ander contactpunt waar verdere informatie kan worden verkregen

3. Samenvatting van het incident dat de inbreuk in verband met persoonsgegevens heeft veroorzaakt

4. Vermoedelijke datum van het incident

5. Aard en inhoud van de in artikel 3, lid 2, bedoelde persoonsgegevens

6. Waarschijnlijke gevolgen van de inbreuk in verband met persoonsgegevens voor de in artikel 3, lid 2 bedoelde abonnee of andere persoon

7. Omstandigheden van de in artikel 3, lid 2 bedoelde inbreuk in verband met persoonsgegevens

8. Door de aanbieder genomen maatregelen om de inbreuk in verband met persoonsgegevens aan te pakken

9. Door de aanbieder aanbevolen maatregelen om mogelijke negatieve gevolgen tegen gaan