EUROPESE
COMMISSIE

Brussel, 10.1.2017
SWD(2017) 4 final

WERKDOCUMENT VAN DE DIENSTEN VAN DE COMMISSIE

SAMENVATTING VAN DE EFFECTBEOORDELING

bij

Voorstel voor een verordening van het Europees Parlement en de Raad

met betrekking tot de eerbiediging van het privéleven en de bescherming van persoonsgegevens in elektronische communicatie, en tot intrekking van Richtlijn 2002/58/EG (richtlijn betreffende privacy en elektronische communicatie)

{COM(2017) 10 final}
{SWD(2017) 3 final}
{SWD(2017) 5 final}
{SWD(2017) 6 final}

A. Behoefte aan actie

Wat is het probleem en waarom is het een probleem?

De effectbeoordeling is tegelijkertijd met de ex-postevaluatie van de e-privacyrichtlijn verricht in het kader van het programma voor gezonde en resultaatgerichte regelgeving (Refit).

De algemene conclusie is dat de doelstellingen van de e-privacyrichtlijn nog steeds relevant zijn.

Bij de Refit-evaluatie zijn drie belangrijke reeksen problemen geconstateerd:

- De persoonlijke levenssfeer van burgers is niet voldoende en niet doelmatig beschermd wanneer zij online communiceren;
- burgers zijn niet doeltreffend beschermd tegen ongewenste marketing;
- bedrijven worden geconfronteerd met belemmeringen ten gevolge van gefragmenteerde wetgeving, verschillende interpretaties in de lidstaten en onduidelijke en verouderde bepalingen.

In de Refit-evaluatie is ook geconcludeerd dat er ruimte is voor vereenvoudiging, met name met betrekking tot het bestaan van een aantal verouderde of overbodige bepalingen en de voorschriften inzake handhaving.

Dit wordt ook ondersteund door een advies van het Refit-platform waarin gepleit wordt voor een sterkere bescherming van de persoonlijke levenssfeer van burgers door de e-privacyrichtlijn af te stemmen op de algemene verordening gegevensbescherming en voor de toevoeging van uitzonderingen op de "toestemmingsregel" voor cookies. Ook moeten de problemen die zich bij de nationale uitvoering voordoen, door de Commissie worden aangepakt.

Wat is het streefdoel?

De specifieke doelstellingen van de herziening zijn:

1. zorgen voor daadwerkelijke vertrouwelijkheid van elektronische communicatie;
2. zorgen voor daadwerkelijke bescherming tegen ongewenste commerciële communicatie;
3. meer harmonisering en vereenvoudiging/actualisering van het wettelijk kader.

Wat is de meerwaarde van actie op EU-niveau?

Aangezien elektronische communicatie, met name op basis van het internetprotocol, een mondiaal bereik heeft, krijgt het probleem een veel ruimere dimensie dan het grondgebied van de afzonderlijke lidstaten. Nationale regels betreffende vertrouwelijkheid van communicatie verschillen sterk wat de toepassingssfeer en de inhoud betreft. Hoewel het voor de lidstaten dus mogelijk is een beleid te voeren om te waarborgen dat dit recht niet wordt geschonden, zou dit zonder regels van de Unie niet op eenvormige wijze worden bereikt en zou dit leiden tot belemmeringen voor het grensoverschrijdende verkeer van persoonsgegevens betreffende elektronische-communicatiediensten naar andere lidstaten die niet aan dezelfde normen inzake gegevensbescherming voldoen.

De aanstaande herziening van de e-privacyrichtlijn wordt geacht te voldoen aan de beginselen van subsidiariteit en evenredigheid, aangezien de harmonisatiebenadering en het samenwerkingsmechanisme bewaard blijven, terwijl de lidstaten afwijkende maatregelen kunnen

nemen voor specifieke legitieme doeleinden.

B. Oplossingen

Welke opties dienen zich aan? Is er al dan niet een voorkeursoptie? Zo nee, waarom niet?

De opties zijn gegroepeerd volgens hun niveau van groeiende ambitie (d.w.z. optie 1 is de minst ambitieuze en optie 4 de meest ambitieuze) om de bovengenoemde doelstellingen (privacy en vereenvoudiging) te realiseren. In optie 5 wordt de intrekking van de e-privacyrichtlijn voorgesteld.

1. **Optie 1: Niet-wetgevende maatregelen ("soft law"):** deze omvat richtsnoeren van de Commissie, het stimuleren van zelfregulerende initiatieven en andere „soft law"-maatregelen.

2. **Optie 2: Beperkte versterking van privacy/vertrouwelijkheid en harmonisatie:** deze optie voorziet in een minimale versterking van de rechten op privacy en vertrouwelijkheid (door een verduidelijking van het toepassingsgebied van de e-privacyrichtlijn, dat ook OTT's, openbaar beschikbare Wi-Fi en IoT-apparaten moet omvatten) en bescherming tegen ongewenste oproepen (verduidelijking van de huidige regels en verplichting van gebruik van een standaardkengetal) en vereenvoudiging (intrekking van beveiligingsvoorschriften, versterking van de samenwerking in grensoverschrijdende zaken).

3. **Optie 3: Matige versterking van privacy/vertrouwelijkheid en harmonisatie:** deze optie voorziet in een aanzienlijke verscherping van het recht op privacy/vertrouwelijkheid (uitbreiding van het toepassingsgebied, grotere transparantie van de privacyinstellingen, meer transparantie, versterking van handhavingsbevoegdheden), bescherming tegen ongewenste communicatie (invoering van opt-in voor marketingoproepen) en vereenvoudiging (verruiming van uitzonderingen, verdere intrekking van overbodige bepalingen en stroomlijning van de handhaving door bevoegdheden toe te vertrouwen aan de autoriteiten die verantwoordelijk zijn voor de handhaving van de algemene verordening gegevensbescherming en uitbreiding van het coherentiemechanisme van deze verordening).

4. **Optie 4: Ingrijpende versterking van privacy/vertrouwelijkheid en harmonisatie:** deze optie voorziet in verreikende maatregelen bovenop de maatregelen van optie 3, zoals een algemeen verbod op „cookie walls", de intrekking van de uitzondering van eerdere zakelijke relatie voor marketing via e-mail en sms, bijkomende intrekkingen en uitvoeringsbevoegdheden van de Commissie.

5. **Optie 5: Intrekking van de e-privacyrichtlijn:** deze optie voorziet in de intrekking van de e-privacyrichtlijn en in de daaruit volgende toepasbaarheid van de algemene verordening gegevensbescherming, met inbegrip van het handhavingssysteem voor de bescherming van de vertrouwelijkheid van persoonsgegevens betreffende elektronische communicatie; de veralgemeende toepassing van een opt-outsysteem voor ongewenste communicatie en de toepassing van het coherentiemechanisme van de algemene verordening gegevensbescherming.

Wie zijn de verschillende belanghebbenden? Wie steunt welke optie?

- De rechten van **burgers** worden beïnvloed door het niveau van bescherming van de vertrouwelijkheid van hun communicatie. Zij pleiten voor opties die hun rechten versterken, zoals de opties 2, 3 en 4.
- De **nationale autoriteiten en de Europese Toezichthouder voor gegevensbescherming** zouden voorstander zijn van opties die leiden tot een sterkere en coherentere

privacybescherming zoals de opties 2, 3 en 4.

- **Aanbieders van elektronische communicatie** vormen de voornaamste adressaten van de in de e-privacyrichtlijn voorgeschreven verplichtingen. Zij zijn sterke voorstanders van optie 5. Als tweede beste keuze kunnen zij instemmen met de opties 2 en 3 die ervoor zorgen dat concurrerende OTT's aan dezelfde regels worden onderworpen.
- **Over-the-topaanbieders** zouden ook voorstander zijn van de opties 1 en 5 aangezien zij normaliter liever niet worden onderworpen aan strengere regelgevingsvereisten. Optie 3 zou na deze twee de meest aanvaardbare optie vormen, gelet op de marge van flexibiliteit die daarmee gegarandeerd wordt.
- **Uitgevers van websites en OBA-exploitanten** zouden duidelijk de voorkeur geven aan optie 5, om dezelfde redenen als elektronische-communicatiediensten en OTT's.
- **Aanbieders van browsers** zouden belast worden met specifieke verantwoordelijkheden onder optie 3. Zij zouden daarom geen voorstander zijn van de opties 3 en 4.
- **Kleine en middelgrote ondernemingen** zouden over het algemeen voorstander zijn van de opties 1 en 5. Indien zij elektronische-communicatiediensten zijn, zouden zij voorstander zijn van opties 2 en 3 voor het gelijke speelveld met OTT's. indien zij OTT's zijn, geven zij de voorkeur aan de opties 1 en 5, met daarna optie 3 als de meest aanvaardbare.

C. Effecten van de voorkeursoptie

Wat zijn de voordelen van de voorkeursoptie (indien er een voorkeur is, anders van de belangrijkste opties)?

De voorkeur gaat uit naar optie 3. De voornaamste voordelen zijn:

- betere bescherming van vertrouwelijkheid door middel van een technologisch neutrale definitie, versterking van de vereisten inzake gebruikerscontrole en transparantie en effectievere handhaving.
- betere bescherming tegen ongewenste communicatie, dankzij de invoering van de opt-in voor marketinggesprekken, de invoering van een kengetal en het daaruit voortvloeiende verbod op anonieme marketingoproepen en de versterkte mogelijkheden om oproepen van ongewenste nummers te blokkeren.
- vereenvoudiging door harmonisatie en verduidelijking van het regelgevingsklimaat dankzij de beperking van de manoeuvreerruimte voor de lidstaten, de intrekking van achterhaalde bepalingen en de verruiming van de uitzonderingen op de toestemmingsregels.

Wat zijn de kosten van de voorkeursoptie (indien er een voorkeur is, anders van de belangrijkste opties)?

De voorkeursoptie zal naar verwachting besparingen opleveren ten gevolge van bijkomende harmonisatie en vereenvoudiging. Bijvoorbeeld zijn er besparingen tot 70 % van de kosten met betrekking tot e-privacy berekend via een gecentraliseerd beheer van de privacykeuzes die eens en voor altijd gelden voor alle websites en applicaties.

Op het niveau van specifieke categorieën belanghebbenden zouden **OTT-actoren** een reeks kosten moeten dragen om de wettigheid van hun bedrijfsmodellen te evalueren. Deze kosten zouden echter naar verwachting niet hoog oplopen. **Uitgevers van websites** kunnen te maken krijgen met enige beperkte aanpassingskosten. **Browsers en aanbieders van soortgelijke applicaties die toegang tot het internet mogelijk maken** zouden aanzienlijke kosten moeten maken om ervoor te zorgen dat aan de gebruikers de passende keuzes worden aangeboden met betrekking tot hun privacyinstellingen. **Handelaars** zouden worden geconfronteerd met extra kosten als gevolg van de invoering van de opt-in voor marketingoproepen.

Zijn er significante gevolgen voor de nationale begrotingen en overheden?
De belangrijkste gevolgen voor de nationale begrotingen en overheden zouden voortvloeien uit de invoering van het coherentiemechanisme en de eventuele verplichting om handhavingsbevoegdheden alleen aan gegevensbeschermingsautoriteiten toe te wijzen. Het effect wordt niet aanzienlijk geacht aangezien gebruik zou kunnen worden gemaakt van de synergieën met reeds bestaande coördinerende instanties in de EU (bijvoorbeeld op het gebied van gegevensbescherming).
Zijn er nog andere significante gevolgen?
Neen
Is de evenredigheid gewaarborgd?
De voorkeursoptie bevat evenwichtige maatregelen die allemaal noodzakelijk worden geacht om de betrokken doelstellingen te bereiken zonder buitensporige lasten voor de desbetreffende belanghebbenden. Voorts zijn de maatregelen flexibel ontworpen, met de nodige uitzonderingen, en technologisch neutraal om verstoring van de mededinging tot een minimum te beperken en te zorgen voor een gelijk speelveld.
D. Follow up
Wanneer wordt dit beleid geëvalueerd?
Permanent toezicht zal worden gewaarborgd, onder meer doordat de lidstaten verslag moeten uitbrengen aan de Commissie, die op haar beurt verslag uitbrengt aan het Europees Parlement, de Raad en het Europees Economisch en Sociaal Comité.