EUROPESE COMMISSIE

Brussel, 25.1.2012
SEC(2012) 73 final

COMMISSION STAFF WORKING PAPER

SAMENVATTING VAN DE EFFECTBEOORDELING

bij

Verordening van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (Algemene verordening gegevensbescherming)
en
Richtlijn van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens

{COM(2012) 11 final}
{SEC(2012) 72 final}

COMMISSION STAFF WORKING PAPER

SAMENVATTING VAN DE EFFECTBEOORDELING

bij

Verordening van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (Algemene verordening gegevensbescherming)
en
Richtlijn van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens

1. INLEIDING

Het huidige rechtskader van de EU inzake gegevensbescherming stamt uit 1995. Sindsdien zijn door snelle ontwikkelingen op technologisch en zakelijk gebied nieuwe uitdagingen voor de bescherming van persoonsgegevens ontstaan. De mate waarin gegevens worden verzameld en gedeeld, is enorm gestegen. Door technologie kunnen bedrijven en overheid bij het uitvoeren van hun activiteiten meer dan ooit tevoren gebruikmaken van persoonsgegevens. Mensen maken hun persoonsgegevens steeds vaker wereldwijd bekend, zonder dat zij zich volledig bewust zijn van de risico's daarvan.

Het is voor de economische ontwikkeling cruciaal om vertrouwen in de onlineomgeving tot stand te brengen. Ontbreekt dat vertrouwen, dan zijn consumenten minder geneigd om online aankopen te doen en gebruik te maken van nieuwe diensten, waaronder e-overheidsdiensten. Als dit gebrek aan vertrouwen niet wordt aangepakt, zal het de ontwikkeling van innovatieve toepassingen van nieuwe technologieën blijven vertragen, de economische groei belemmeren en het voor de overheid moeilijk maken om het potentieel van digitalisering van haar dienstverlening te verwezenlijken.

Ook is door het Verdrag van Lissabon een nieuwe rechtsgrondslag voor een gemoderniseerde totaalaanpak van gegevensbescherming en het vrije verkeer van persoonsgegevens ingevoerd: artikel 16 VWEU, dat ook van toepassing is op politiële en justitiële samenwerking in strafzaken.

2. OMSCHRIJVING VAN HET PROBLEEM

In de effectbeoordeling worden drie grote probleemgebieden vastgesteld en geanalyseerd.

2.1. Probleem 1: belemmeringen voor het bedrijfsleven en de overheid als gevolg van fragmentatie, rechtsonzekerheid en inconsequente handhaving

Hoewel de bestaande richtlijn beoogt in de hele EU een gelijkwaardig beschermingsniveau voor persoonsgegevens tot stand te brengen, zijn er nog aanmerkelijke verschillen tussen de

regels die in de lidstaten gelden. Voor de verwerking verantwoordelijken moeten daardoor rekening houden met 27 verschillende nationale wetgevingen en vereisten binnen de EU. Dit heeft geresulteerd in een gefragmenteerd rechtskader, met alle rechtsonzekerheid en ongelijke bescherming van personen van dien. Bedrijven worden daardoor geconfronteerd met onnodige kosten en **administratieve lasten** (in het basisscenario **circa 3 miljard euro per jaar**), wat een ontmoedigend effect heeft voor ondernemingen, ook in het midden- en kleinbedrijf, die op de eengemaakte markt actief zijn en hun activiteiten tot het buitenland willen uitbreiden.

De middelen en bevoegdheden van de nationale autoriteiten die voor gegevensbescherming verantwoordelijk zijn, verschillen bovendien aanzienlijk van lidstaat tot lidstaat. Soms kunnen zij daardoor hun handhavingstaak niet naar behoren uitvoeren. De samenwerking tussen deze autoriteiten op Europees niveau (via de Groep artikel 29) leidt niet altijd tot consequente handhaving en moet dan ook worden verbeterd.

2.2. Probleem 2: het is voor personen moeilijk om de controle over hun persoonsgegevens te behouden

Doordat de nationale wetgevingen inzake gegevensbescherming niet zijn geharmoniseerd en de bevoegdheden van de nationale autoriteiten niet gelijklopen, is het voor personen in sommige lidstaten moeilijker dan in andere om hun rechten uit te oefenen, met name in een onlineomgeving.

Mensen hebben de controle over hun eigen gegevens verloren door de enorme omvang van de gegevens die iedere dag opnieuw worden gedeeld en ook doordat zij er vaak niet van op de hoogte zijn dat hun gegevens worden verzameld. Volgens veel Europeanen is het bekendmaken van persoonsgegevens steeds meer onderdeel van het moderne leven[1], maar toch is 72% van de internetgebruikers in Europa bezorgd dat hun online te veel om persoonsgegevens wordt gevraagd. Internetters weten vaak ook niet hoe zij online hun rechten kunnen uitoefenen.

2.3. Probleem 3: lacunes en inconsequenties bij de bescherming van persoonsgegevens in het kader van politiële en justitiële samenwerking in strafzaken

Politiële en justitiële samenwerking in strafzaken is uitdrukkelijk uitgesloten van het toepassingsgebied van de richtlijn, die op een rechtsgrondslag voor de interne markt is gebaseerd. Het kaderbesluit dat in 2008 is vastgesteld om de verwerking van gegevens op het gebied van politiële samenwerking en justitiële samenwerking in strafzaken te reglementeren, weerspiegelt de specifieke kenmerken van de pijlerstructuur van de EU, zoals die vóór het Verdrag van Lissabon bestond. Het heeft een **beperkt toepassingsgebied** en kent een aantal **andere lacunes** die vaak aanleiding geven tot rechtsonzekerheid voor zowel personen als rechtshandhavingsautoriteiten en tot praktische uitvoeringsproblemen. Bovendien voorziet het kaderbesluit in ruime mogelijkheden om op nationaal niveau van de algemene gegevensbeschermingsregels af te wijken, waardoor er geen sprake is van harmonisering. Niet alleen dreigen deze beginselen daarmee van hun zin te worden ontdaan, wat het fundamentele recht van personen op de bescherming van hun persoonsgegevens op dit gebied aantast, maar ook wordt daardoor de vlotte uitwisseling van persoonsgegevens tussen bevoegde nationale instanties gehinderd.

---

[1] Zie speciale Eurobarometer 359 – *Attitudes on Data Protection and Electronic Identity in the European Union*, juni 2011, blz. 23.

3. SUBSIDIARITEITS- EN EVENREDIGHEIDSANALYSE

Uit de subsidiariteitsanalyse komt naar voren dat, gezien de hierboven aangekaarte problemen, actie op EU-niveau vereist is om de volgende redenen:

- bescherming van persoonsgegevens is een recht dat is vastgelegd in artikel 8 van het Handvest van de grondrechten van de EU. Artikel 16 VWEU is de rechtsgrondslag voor de vaststelling van EU-voorschriften inzake gegevensbescherming;
- persoonsgegevens kunnen steeds vaker en sneller worden doorgegeven over landsgrenzen heen, zowel over de binnengrenzen van de EU als de buitengrenzen met derde landen. Er doen zich bovendien praktische problemen voor bij de handhaving van de wetgeving inzake gegevensbescherming en de samenwerking tussen de lidstaten en hun autoriteiten. Een en ander moet op EU-niveau worden geregeld om de nodige samenhang en een hoog beschermingsniveau in de hele Unie te waarborgen;
- de problemen met de huidige regeling kunnen niet door de lidstaten afzonderlijk worden verholpen. Dat geldt vooral voor problemen die ontstaan door de fragmentatie van de nationale wetgevingen ter uitvoering van het EU-regelgevingskader voor gegevensbescherming;
- de lidstaten kunnen weliswaar een beleid voeren dat waarborgt dat het recht op de bescherming van persoonsgegevens wordt gehandhaafd, maar zonder gemeenschappelijke regels op EU-niveau zal dat niet op eenvormige wijze gebeuren, waardoor belemmeringen voor het grensoverschrijdende verkeer van persoonsgegevens ontstaan.

De **voorgenomen maatregelen voldoen aan het evenredigheidsbeginsel**, omdat zij onder de bevoegdheden van de Unie vallen, zoals die bij het Verdrag zijn vastgesteld, en noodzakelijk zijn om eenvormige toepassing van de EU-wetgeving te waarborgen en de grondrechten van personen doeltreffend en in gelijke mate te beschermen. Er moeten op EU-niveau maatregelen worden genomen met het oog op geloofwaardigheid en om een hoog niveau van bescherming van persoonsgegevens in deze wereld van mondialisering te waarborgen, zonder afbreuk te doen aan het vrije verkeer van dergelijke gegevens. Voor de goede werking van de interne markt moeten de bepalingen voor alle marktdeelnemers gelijke voorwaarden tot stand brengen.

4. DOELSTELLINGEN

De drie **voornaamste beleidsdoelen** zijn:

- **de internemarktdimensie van gegevensbescherming versterken** door de fragmentatie te bestrijden, de onderlinge samenhang te verbeteren en de regels te **vereenvoudigen** en daardoor onnodige kosten te vermijden en de **administratieve lasten te verminderen**;
- **het grondrecht op bescherming van persoonsgegevens effectiever maken en personen de controle geven over hun eigen gegevens**;
- **de samenhang van het EU-kader voor gegevensbescherming vergroten**, ook wat betreft politiële en justitiële samenwerking in strafzaken, zoals bepaald in het Verdrag van Lissabon.

5. BELEIDSOPTIES

5.1. Optie 1: Zachte acties

Deze optie omvat met name **interpretatieve mededelingen van de Commissie, hulpmiddelen voor technische ondersteuning en financiering**, maar ook **aanmoediging van normalisatie en zelfregulering**. Het doel daarvan is versterking van de praktische tenuitvoerlegging van de bestaande regels door voor de verwerking verantwoordelijken en bewustmaking van de betrokkenen. Bij deze optie stelt de Commissie **slechts zeer beperkte wijzigingen van de wetgeving** voor, namelijk om reeds bestaande begrippen in de richtlijn te verduidelijken en specifieke vraagstukken aan te pakken die niet doeltreffend anders kunnen worden geregeld. Deze beleidsoptie is slechts relevant voor de problemen 1 en 2.

De beperkte wetswijzigingen zouden inhouden dat de beginselen van transparantie en minimale gegevensverwerking expliciet worden gemaakt en een rechtsgrondslag wordt ingevoerd voor bindende bedrijfsvoorschriften met betrekking tot internationale gegevensdoorgifte.

5.2. Optie 2: Modernisering van het rechtskader

Deze optie houdt in dat de Commissie **wetgevingsvoorstellen doet om de materiële regels verder te harmoniseren**, specifieke bepalingen te verduidelijken en inconsequenties weg te werken die door de verschillende benaderingen in de lidstaten zijn ontstaan. Met deze voorstellen zouden de problemen 1 en 2 worden aangepakt door enerzijds **gegevensstromen binnen de EU en van de EU naar derde landen te vergemakkelijken** en anderzijds de **rechten van personen** (zoals het recht van toegang, het "recht om te worden vergeten", duidelijker procedures voor toestemmingverlening en voor melding van gegevenslekken) **te verduidelijken en te versterken** en de **verantwoordelijkheid – en de verantwoordingsplicht – van voor de verwerking verantwoordelijken en van gegevensverwerkers te versterken** (bijvoorbeeld door, waar relevant, de benoeming van functionarissen voor gegevensbescherming verplicht te stellen en een privacyeffectbeoordeling uit te voeren). Deze optie omvat met name een **éénloketsysteem** voor voor de verwerking verantwoordelijken (d.w.z. één wet en één gegevensbeschermingsautoriteit). De algemene kennisgevingsvereisten zouden in het kader van optie 2 worden vereenvoudigd (basisregistratie). Deze optie **vergroot de onafhankelijkheid van de gegevensbeschermingsautoriteiten en harmoniseert hun bevoegdheden.** Samenwerking en wederzijdse bijstand tussen de gegevensbeschermingsautoriteiten worden bevorderd, onder meer met een nieuwe "**conformiteitstoetsing**" waarbij een nieuw op te richten "Europees comité voor gegevensbescherming" en de Europese Commissie betrokken zijn.

Ten aanzien van de gegevensbescherming in het kader van politiële samenwerking en justitiële samenwerking in strafzaken (probleem 3) doet de Commissie bij deze optie voorstellen om het kaderbesluit te vervangen door een **nieuw instrument met een uitgebreider toepassingsgebied** en pakt zij de **ernstigste lacunes en tekortkomingen** aan, om zowel de rechten van personen te versterken als de samenwerking tussen rechtshandhavingsautoriteiten te faciliteren, met inachtneming van de specifieke kenmerken van de sector rechtshandhaving.

5.3. Optie 3: Gedetailleerde rechtsvoorschriften op EU-niveau

Deze optie omvat de meeste onderdelen van optie 2, met daarnaast **veel uitgebreidere EU-rechtsvoorschriften**, inclusief sectorale wetgeving (bijvoorbeeld voor de medische sector en de zorgsector) en een **gecentraliseerde handhavingsstructuur op EU-niveau** (bijvoorbeeld een EU-gegevensbeschermingsautoriteit). Deze optie omvat tevens afschaffing van de vereisten inzake algemene kennisgeving (behalve controle vooraf bij verwerking van gevoelige gegevens), opzetten van een EU-certificeringsregeling voor privacyconforme processen en producten en vaststelling van geharmoniseerde strafrechtelijke sancties op EU-niveau voor inbreuk op de privacyvoorschriften. De hoofdregel wordt dus: geen verwerking zonder toestemming.

Wat betreft de politiële en justitiële samenwerking in strafzaken worden, naast de inhoudelijke maatregelen van optie 2, nadere voorschriften vastgesteld inzake het toegangsrecht van personen (dat altijd direct moet zijn). Ook worden de **relevante bepalingen van alle bestaande instrumenten die tot de derde pijler behoorden**, gewijzigd en aangepast aan de nieuwe, uitgebreide geharmoniseerde voorschriften.

6. EFFECTBEOORDELING

6.1. Beleidsoptie 1: Zachte acties

Interpretatieve mededelingen van de Commissie over richtlijnbepalingen zijn niet bindend en **bestrijden rechtsonzekerheid en kosten dus slechts in beperkte mate**. Meer zelfregulering op EU-niveau kan in specifieke sectoren tot een grotere rechtszekerheid voor voor verwerking verantwoordelijken leiden, maar is **niet voldoende** om doeltreffende en consequente toepassing van de regels te waarborgen, als er niet ook een duidelijk en geharmoniseerd rechtskader op EU-niveau aan ten grondslag ligt.

Voorlichting kan ertoe bijdragen dat mensen hun privacyrechten beter kennen en begrijpen hoe ze die praktisch kunnen uitoefenen. Het **volstaat echter niet** dat personen hun rechten kennen, als die rechten in de wet niet duidelijk zijn gedefinieerd. **Verduidelijking van de wetgeving** wat de beginselen van transparantie, minimale gegevensverwerking, toereikendheid en bindende bedrijfsvoorschriften betreft, versterkt de harmonisatie en de rechtszekerheid voor personen en bedrijven.

Wat de **handhaving** betreft, veranderen mededelingen van de Commissie weinig aan de geringe bereidheid van de lidstaten om hun nationale rechtsvoorschriften te wijzigen en de gegevensbeschermingsautoriteiten onafhankelijker te maken en hun bevoegdheden te harmoniseren. Betere coördinatie door de Groep artikel 29 en uitwisseling tussen de gegevensbeschermingsautoriteiten bevorderen een consequente handhaving van de regels, maar **als de nationale wetgevingen en de interpretatie ervan blijven uiteenlopen, blijft het effect van betere coördinatie tussen de gegevensbeschermingsautoriteiten beperkt**.

De te verwachten **financiële en economische impact van deze beleidsoptie zijn beperkt**, en de geconstateerde problemen worden erdoor voor het merendeel niet verholpen.

6.2. Beleidsoptie 2: Modernisering van het rechtskader

De **rechtsonzekerheid** voor particuliere bedrijven en overheden **wordt aanzienlijk verminderd**. Bepalingen die problemen opleveren, worden verduidelijkt en de onderlinge

samenhang wordt verbeterd door inperking van de interpretatiemarge en door uitvoeringsmaatregelen en/of gedelegeerde handelingen van de Commissie.

Als de verplichting om kennis te geven van elke verwerking van gegevens wordt vervangen door een vereenvoudigd **geharmoniseerd registratiesysteem**, blijft de voorafgaande controle in geval van gevoelige gegevens en de verwerking daarvan bestaan, maar verdwijnt voor de verwerking verantwoordelijken een verplichting die momenteel op uiteenlopende wijze is geïmplementeerd. Als de verantwoordelijkheid van de voor de verwerking verantwoordelijken en verwerkers wordt uitgebreid door de invoering van functionarissen voor gegevensbescherming en privacyeffectbeoordelingen (in bepaalde gevallen, en vanaf welbepaalde drempels) en van het beginsel "privacy by design", kan conformiteit gemakkelijker aantoonbaar worden gewaarborgd.

Verduidelijking en vereenvoudiging van de voorschriften door voor de hele EU één toepasselijke wet vast te stellen en een éénloketsysteem voor privacytoezicht in te voeren, versterkt de interne markt, ook doordat de verschillen tussen de administratieve formaliteiten van de gegevensbeschermingsautoriteiten worden weggenomen. Hiermee kan op jaarbasis, aan administratieve formaliteiten alleen, **in totaal circa 2,3 miljard euro worden bespaard**.

Een **consequente handhaving wordt ook bevorderd** door de bevoegdheden van de gegevensbeschermingsautoriteiten uit te breiden en te harmoniseren, krachtige mechanismen voor samenwerking en wederzijdse bijstand op te zetten voor zaken met een EU-dimensie en te harmoniseren welke feiten aanleiding geven tot administratieve sancties.

Met een **voor de EU geharmoniseerde verplichting om gegevenslekken te melden**, worden personen beter beschermd, wordt de onderlinge samenhang voor alle sectoren bevorderd en worden concurrentienadelen vermeden.

De rechten van betrokkenen en hun controle over de henzelf betreffende gegevens worden aanzienlijk versterkt door de invoering van nieuwe rechten en de verbetering en verduidelijking van de bestaande rechten. Ten behoeve van kinderen komen er maatregelen die specifiek rekening houden met hun kwetsbaarheid. Verenigingen krijgen meer mogelijkheden om betrokkenen de helpen hun rechten uit te oefenen, ook in rechtszaken.

Toepassing van de algemene beginselen inzake gegevensbescherming op politiële en justitiële samenwerking in strafzaken komt de algehele samenhang van het EU-kader voor gegevensbescherming ten goede en is ook in overeenstemming met de specifieke vereisten van de rechtshandhaving. De rechten van personen worden met name beter gewaarborgd als het toepassingsgebied van de gegevensbeschermingsregels op dit gebied wordt uitgebreid tot de binnenlandse verwerking, regels voor de uitoefening van het toegangsrecht worden vastgesteld en strengere regels inzake doelbinding worden opgesteld.

Wat de **financiële en economische impact** betreft, leidt de verplichting om in grotere ondernemingen (meer dan 250 werknemers) een functionaris voor gegevensbescherming te benoemen niet tot **onevenredige kosten**, aangezien die functie in zulke bedrijven meestal al bestaat. De kosten om aan dit voorschift te voldoen, bedragen 320 miljoen euro per jaar. Deze verplichting zou niet meer voor de verwerking verantwoordelijken treffen dan struikt genomen noodzakelijk, want kleine en middelgrote ondernemingen zijn in de regel vrijgesteld, tenzij hun gegevensverwerkingsactiviteiten een aanzienlijk privacyrisico inhouden. Overheidsinstanties mogen één gegevensverwerkingsfunctionaris voor

verschillende onderdelen (bijvoorbeeld bureaus of afdelingen) benoemen, rekening houdend met hun organisatiestructuur.

Vereenvoudiging van de voorschriften voor internationale doorgiften (bijvoorbeeld door de reikwijdte van de bindende bedrijfsvoorschriften uit te breiden) heeft eveneens een gunstige invloed op de internationale concurrentiepositie van het EU-bedrijfsleven.

Het versterken van de onafhankelijkheid en de bevoegdheden van de gegevensbeschermingsautoriteiten en de verplichting voor de lidstaten om voldoende middelen ter beschikking te stellen, brengen extra kosten met zich mee voor overheidsinstanties die nog niet over de juiste bevoegdheden en adequate middelen beschikken.

Ook het nieuwe mechanisme voor samenwerking en wederzijdse bijstand tussen gegevensbeschermingsautoriteiten brengt extra kosten met zich mee voor die autoriteiten en voor de Europese Toezichthouder voor gegevensbescherming. Voor de aanvullende taken waarmee de Europese Toezichthouder wordt belast in verband met de secretariaatswerkzaamheden voor het EU-comité voor gegevensbescherming (dat in de plaats komt van de Groep artikel 29) en vooral zijn rol bij de conformiteitstoetsing, moeten de huidige middelen van de toezichthouder waarschijnlijk met gemiddeld 3 miljoen euro per jaar worden verhoogd gedurende de eerste zes jaar, waarbij kredieten voor tien extra personeelsposten zijn inbegrepen.

6.3. Beleidsoptie 3: Gedetailleerde rechtsvoorschriften op EU-niveau

Door nader gedetailleerde (o.a. sectorale) rechtsvoorschriften vast te stellen die verder gaan dan de maatregelen van optie 2, kunnen de **discrepanties tussen de lidstaten maximaal worden teruggedrongen**. Het kan echter zijn dat de lidstaten niet voldoende flexibel kunnen optreden om met alle nationale bijzonderheden rekening te houden.

Door de kennisgevingen volledig af te schaffen (behalve wat voorafgaande controles betreft), kan de regelgeving aanzienlijk worden vereenvoudigd en de administratieve belasting verminderd.

Door oprichting van een EU-agentschap voor gegevensbescherming kan de wetgeving **consequenter worden gehandhaafd** en wordt een einde gemaakt aan de inconsistenties bij gevallen met een duidelijke EU-dimensie. Het kan echter zijn dat de EU-wetgeving dergelijke bevoegdheden voor een EU-agentschap niet toelaat. De kosten van zo'n agentschap zouden voor de begroting van de EU zeer hoog zijn. Ook harmonisering van de strafrechtelijke sancties bevordert consequente handhaving, maar zal anderzijds wellicht op sterk verzet van de lidstaten stuiten.

De rechten van de betrokkenen, onder wie kinderen, worden bij deze optie verder versterkt, bijvoorbeeld doordat de definitie van gevoelige gegevens wordt uitgebreid tot gegevens betreffende kinderen, biometrische gegevens en financiële gegevens. Ook door ter beslechting van geschillen collectieve vorderingen mogelijk te maken, kunnen rechten worden gemaximaliseerd. Individuele rechten zouden nog verder kunnen worden versterkt door op EU-niveau sancties (ook strafrechtelijke) te harmoniseren.

Een uitdrukkelijke wijziging van alle rechtsinstrumenten waarbij de algemene voorschriften inzake gegevensbescherming van toepassing worden op de politiële en justitiële samenwerking in strafzaken, zou de effectiviteit en de samenhang van de voorschriften op dit

gebied, maar ook de rechten van personen, positief beïnvloeden. Zo'n radicale aanpak zou echter stuiten op verzet van de lidstaten en politiek moeilijk haalbaar zijn.

7. VERGELIJKING VAN DE OPTIES

Bij beleidsoptie 1 zijn de nalevingskosten en administratieve kosten beperkt, vooral voor particuliere voor verwerking verantwoordelijken, aangezien de meeste bijkomende kosten voor rekening komen van de nationale overheden en EU-instanties. De optie zou echter slechts een **gering positief effect hebben op de geconstateerde problematiek en de verwezenlijking van de beleidsdoelen**.

Wat de politieke haalbaarheid van deze optie betreft: de voorstellen zijn niet controversieel, maar zullen waarschijnlijk op verzet van de belanghebbenden stuiten omdat zij niet ver genoeg gaan en een geringe impact hebben en dus onvoldoende ambitieus worden bevonden.

Beleidsoptie 2 leidt tot een **aanzienlijke vermindering van fragmentatie en rechtsonzekerheid**. Deze optie is naar verwachting veel effectiever om de geconstateerde problemen op te lossen en de beleidsdoelen te verwezenlijken. De verhouding tussen de nalevingskosten en administratieve **kosten bij deze optie en de voordelen en de besparingen van circa 2,3 miljard euro per jaar aan administratieve lasten zal naar verwachting redelijk zijn, wat van groot belang is voor het bedrijfsleven**. Deze optie zorgt over het algemeen voor betere en consequentere handhaving. Door de kennisgevingen af te schaffen en te vervangen door een veel eenvoudiger systeem van basisregistraties kan de regelgeving worden vereenvoudigd en de administratieve belasting verminderd.

Wat het draagvlak voor deze optie betreft: zij zal waarschijnlijk positief worden ontvangen door bedrijven en overheden, omdat de nalevingskosten erdoor over het algemeen worden verlaagd, met name de kosten die samenhangen met de huidige gefragmenteerde regeling. De versterking van de privacyrechten zal gunstig worden ontvangen door degenen die bij gegevensbescherming betrokken zijn, met name de gegevensbeschermingsautoriteiten. Wat de derde algemene doelstelling betreft: deze optie draagt bij tot de **samenhang en de effectiviteit van de voorschriften inzake gegevensbescherming op het gebied van politiële en justitiële samenwerking in strafzaken** door het kaderbesluit in te trekken en te vervangen door een tekst die met het Verdrag van Lissabon verenigbaar is. Daarmee wordt een aantal lacunes aangepakt, met name door het toepassingsgebied uit te breiden tot verwerking in het binnenland.

Beleidsoptie 3 omvat de meeste van de maatregelen van beleidsoptie 2, maar gaat in een aantal opzichten verder. Deze optie heeft daardoor een **grote positieve impact: zij bestrijdt de kosten die met juridische fragmentatie gepaard gaan en versterkt de rechten van personen**. Bovendien maximaliseert beleidsoptie 3 de effectiviteit en de samenhang van de privacyregels die voorheen in de derde pijler waren opgenomen en zorgt zij in die context voor strengere privacynormen. Enkele van de maatregelen van deze optie leiden echter tot **buitensporig hoge nalevingskosten of grote weerstand bij de belanghebbenden**. Daarnaast is een gelijktijdige wijziging van alle voormalige derdepijlerinstrumenten zeer complex en politiek controversieel.

Voorkeursoptie:

De ***voorkeur wordt gegeven aan optie 2***, in combinatie met:

– afschaffing van de kennisgevingsplicht, zoals in optie 3, en

– enkele "zachte maatregelen" zoals in optie 1: aanmoediging van privacyversterkende technologieën en certificeringsregelingen en voorlichtingscampagnes.

De kans dat de beleidsdoelstellingen worden bereikt zonder buitensporige nalevingskosten en met een aanzienlijke verlichting van de administratieve lasten, is bij de voorkeursoptie het grootst.

De strengere gegevensbeschermingsregels zullen naar verwachting leiden tot iets hogere nalevingskosten, met name voor voor verwerking verantwoordelijken die met gevoelige gegevens werken. Een robuuste regeling voor gegevensbescherming kan voor de economie van de EU een concurrentievoordeel opleveren, doordat de betere bescherming en de verwachte daling van privacyincidenten en -lekken het vertrouwen van de consument kunnen versterken. Als bedrijven aan strenge privacynormen moeten voldoen, kan dat leiden tot duurzame verbeteringen voor het Europese bedrijfsleven, dat een koppositie kan innemen voor privacybevorderende technologieën of privacy by design-oplossingen. Daarmee kan de Europese Unie bedrijven, banen en kapitaal aantrekken.

Voor bedrijven die op de interne markt van de EU opereren, kan de grotere harmonisatie het grensoverschrijdend verwerken van persoonsgegevens eenvoudiger en goedkoper maken. Dit kan voor die bedrijven een aanzienlijke stimulans betekenen om hun activiteiten naar het buitenland uit te breiden, waardoor zij kunnen profiteren van de voordelen van de interne markt. Dat is zowel voor consumenten als voor de hele Europese economie voordelig.

De voorkeursoptie omvat tevens een evenwichtige oplossing voor probleem 3: zij versterkt de rechten van natuurlijke personen, biedt oplossingen voor lacunes en inconsistenties in de gegevensbescherming op het gebied van politiële en justitiële samenwerking in strafzaken, terwijl zij de samenwerking bij de rechtshandhaving vergemakkelijkt en rekening houdt met de specifieke kenmerken van de sector en de operationele behoeften.

8. TOEZICHT EN EVALUATIE

Het toezicht op en de evaluatie van het effect van de voorkeursoptie zullen worden toegespitst op de volgende aspecten: de wijze waarop de nieuwe instrumenten worden gebruikt, de bevoegdheden en middelen van de nationale gegevensbeschermingsautoriteiten, de tijd en de middelen die de voor de verwerking verantwoordelijken moeten spenderen om aan de voorschriften te voldoen en de ontwikkeling van het vertrouwen dat betrokkenen hebben in de bescherming van hun persoonsgegevens op internet.