



EUROPA-KOMMISSIONEN

Bruxelles, den 25.1.2012

SEK(2012) 73 final

ARBEJDSDOKUMENT FRA KOMMISSIONENS TJENESTEGRENE

SAMMENDRAG AF KONSEKVENSANALYSEN

Ledsagedokument til

Europa-Parlamentets og Rådets forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (generel forordning om databeskyttelse)

og

Europa-Parlamentets og Rådets direktiv om beskyttelse af fysiske personer i forbindelse med de kompetente myndigheders behandling af personoplysninger med henblik på at forebygge, efterforske, opdage eller retsforfølge straffelovsovertrædelser eller fuldbyrde strafferetlige sanktioner og om fri udveksling af sådanne oplysninger

{COM(2012) 11 final}

{SEC(2012) 72 final}

ARBEJDSDOKUMENT FRA KOMMISSIONENS TJENESTEGRENE

SAMMENDRAG AF KONSEKVENSANALYSEN

Ledsagedokument til

Europa-Parlamentets og Rådets forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (generel forordning om databeskyttelse)

og

Europa-Parlamentets og Rådets direktiv om beskyttelse af fysiske personer i forbindelse med de kompetente myndigheders behandling af personoplysninger med henblik på at forebygge, efterforske, opdage eller retsforfølge straffelovsovertrædelser eller fuldbårde strafferetlige sanktioner og om fri udveksling af sådanne oplysninger

1. INDLEDNING

Siden vedtagelsen af EU's nuværende retlige ramme for databeskyttelse i 1995 har den hastige teknologiske og erhvervsmæssige udvikling bragt nye udfordringer med sig vedrørende beskyttelse af personoplysninger. Omfanget af datadeling og -indsamling er steget dramatisk. Teknologien giver både private virksomheder og offentlige myndigheder mulighed for at udnytte personoplysninger i et hidtil uset omfang, når de udøver deres aktiviteter. Fysiske personer udbreder i stigende grad deres personoplysninger offentligt og globalt uden at være helt klar over de dermed forbundne risici.

Opbygning af tillid i onlinemiljøet er afgørende for den økonomiske udvikling. Manglende tillid får forbrugerne til at være tilbageholdende med at købe varer på internettet og benytte nye tjenester, herunder offentlige e-forvaltningstjenester. Hvis problemet ikke løses, vil den manglende tillid fortsat hæmme den innovative udnyttelse af ny teknologi, bremse den økonomiske vækst og hindre den offentlige sektor i at høste de potentielle frugter af en digitalisering af dens tjenester.

Endvidere har Lissabontraktaten i medfør af artikel 16 i TEUF skabt et nyt retsgrundlag for en moderniseret og global metode til databeskyttelse og fri udveksling af personoplysninger, som også omfatter politisamarbejde og retligt samarbejde i straffesager.

2. PROBLEMFORMULERING

I konsekvensanalysen præsenteres og analyseres tre hovedproblemområder:

2.1. Problem 1: Hindringer for erhvervsliv og offentlige myndigheder på grund af fragmentering, manglende retssikkerhed og uensartet retshåndhævelse

Trods formålet med direktivet, nemlig at sikre et ensartet databeskyttelsesniveau i hele EU, er der stadig store forskelle på reglerne medlemsstaterne imellem. Derfor kan de registeransvarlige være nødt til at henholde sig til 27 forskellige nationale sæt af love og krav inden for EU. Resultatet er et fragmenteret lovgivningsmiljø, som har skabt manglende retssikkerhed og en ulige beskyttelse af fysiske personer. Resultatet er unødige omkostninger og **administrative byrder** (på **ca. 3 mia. EUR om året** i basisscenariet) for erhvervslivet,

hvilket fratager virksomheder, herunder SMV, i det indre marked incitamentet til at ekspandere på tværs af grænserne.

Desuden har de enkelte medlemsstaters nationale databeskyttelsesmyndigheder (DPA'er) meget forskellige ressourcer og beføjelser. I visse tilfælde giver det sig udslag i, at de ikke er i stand til at udøve deres håndhævelsesopgaver tilfredsstillende. Samarbejdet mellem disse myndigheder på EU-plan - via den eksisterende rådgivende gruppe (den såkaldte Artikel 29-gruppe) - er ikke altid nok til at sikre en ensartet håndhævelse og kræver forbedring.

2.2. Problem 2: Fysiske personer har vanskeligt ved at bevare kontrollen over deres personoplysninger

Den manglende harmonisering af nationale databeskyttelseslove og de nationale databeskyttelsesmyndigheders varierende beføjelser betyder, at det i visse medlemsstater er vanskeligere for fysiske personer at udøve deres databeskyttelsesrettigheder end i andre medlemsstater, især i onlinesammenhæng.

Alene mængden af data, der indsamles hver dag, er med til at gøre det vanskeligere for fysiske personer at bevare kontrollen med deres egne personoplysninger, og de er ofte ikke helt klar over, at der indsamles personoplysninger om dem. Selv om mange europæere mener, at videregivelse af personoplysninger i stigende grad er en del af det moderne liv¹, er der stadig 72 % af de europæiske internetbrugere, der er bekymrede over, at de bliver bedt om at udlevere for mange personoplysninger over nettet ofte uden at vide, hvordan de skal udøve deres rettigheder online.

2.3. Problem 3: Mangler og uensartethed i beskyttelsen af personoplysninger inden for politisamarbejde og retligt samarbejde i straffesager

Ifølge direktivet, der byggede på retsgrundlaget for det indre marked, var politisamarbejde og retligt samarbejde i straffesager udtrykkeligt udelukket fra dets anvendelsesområde. Rammeafgårelsen fra 2008 om regulering af databehandling inden for politisamarbejde og retligt samarbejde i straffesager afspejler de særlige træk ved EU's søjlestruktur før Lissabontraktatens vedtagelse og er kendetegnet ved **et begrænset anvendelsesområde og diverse andre mangler**, der ofte medfører manglende retssikkerhed for fysiske personer og retshåndhævende myndigheder samt praktiske vanskeligheder med gennemførelsen. Desuden giver rammeafgårelsen bred mulighed for undtagelser fra de generelle databeskyttelsesprincipper på nationalt plan og modvirker dermed en harmonisering. Dette risikerer ikke alene at udhule selve formålet med disse principper - og dermed at påvirke fysiske personers grundlæggende rettigheder til beskyttelse af deres personoplysninger på dette område negativt - men også at hæmme den smidige udveksling af personoplysninger mellem relevante nationale myndigheder.

3. ANALYSE AF NÆRHEDSPRINCIPPET OG PROPORTIONALITETSPRINCIPPET

I lyset af de ovennævnte problemer giver analysen af nærhedsprincippet følgende begrundelser for nødvendigheden af en indsats på EU-plan:

- Retten til beskyttelse af personoplysninger er udtrykkelig anerkendt i artikel 8 i Den Europæiske Unions charter om grundlæggende rettigheder. Artikel 16 i TEUF er retsgrundlaget for vedtagelsen af EU's databeskyttelsesregler.

¹ Se Special Eurobarometer 359, "Attitudes on Data Protection and Electronic Identity in the European Union", juni 2011, s. 23.

- Det tager kortere og kortere tid at videregive personoplysninger på tværs af nationale grænser både i og uden for EU. Der er desuden en række praktiske udfordringer i forbindelse med håndhævelsen af lovgivningen om databeskyttelse og et behov for samarbejde mellem medlemsstaterne og deres myndigheder, som bør organiseres på EU-plan for at sikre den nødvendige sammenhæng og et højt beskyttelsesniveau inden for Unionen.
- Medlemsstaterne kan ikke selv mindske de aktuelle problemer. Det er navnlig tilfældet med de problemer, der skyldes fragmenteringen af den nationale lovgivning, hvorved EU's retsregler om databeskyttelse skal gennemføres.
- Selv om det ville være muligt for medlemsstaterne at gennemføre en politik, der kan sikre overholdelsen af retten til databeskyttelse, ville det af mangel på EU-regler ikke foregå på en ensartet måde, men i stedet skabe begrænsninger for grænseoverskridende videregivelse af personoplysninger.

De **påtænkte foranstaltninger er proportionale**, idet de falder ind under Unionens kompetence som defineret ved traktaterne og er nødvendige for at sikre en ensartet anvendelse af EU-lovgivningen og dermed en effektiv og lige beskyttelse af fysiske personers grundlæggende rettigheder. En indsats på EU-plan er afgørende for at opretholde både troværdigheden og et højt databeskyttelsesniveau i en globaliseret verden og sikre en fri datastrøm. Et velfungerende indre marked kræver, at bestemmelserne udmøntes i ensartede spilleregler for de erhvervsdrivende.

4. MÅLSÆTNINGER

De tre primære **politiske målsætninger** er:

- **at lægge større vægt på databeskyttelse som led i det indre marked** ved at mindske fragmenteringen, øge ensartetheden og **forenkle** lovgivningen for dermed at fjerne unødige omkostninger og **mindske den administrative byrde**
- **at gøre den grundlæggende ret til databeskyttelse mere effektiv og give fysiske personer kontrol over deres egne personoplysninger**
- **at øge sammenhængen i EU's databeskyttelsesregler**, herunder inden for politisamarbejde og retligt samarbejde i straffesager, idet der tages fuldt hensyn til Lissabontraktatens ikrafttræden.

5. LØSNINGSMODELLER

5.1. Model 1: En blød indsats

Denne løsningsmodel ville primært bestå i **fortolkende meddelelser fra Kommissionen, tekniske værktøjer og finansiering** - samt **incitamenter til standardisering og selvregulering** - for at styrke de registeransvarliges gennemførelse af eksisterende regler i praksis og højne brugernes bevidsthed. Kommissionen ville kun foreslå **lovændringer i meget begrænset omfang** for at præcisere eksisterende begreber i direktivet og kun vedrørende specifikke problemer, der ikke kan løses effektivt på anden måde. Denne løsningsmodel ville kun være relevant for problem 1 og 2.

De begrænsede lovændringer ville indebære en udtrykkelig indførelse af principperne om gennemsigtighed og dataminimering samt "bindende virksomhedsregler" som retsgrundlag for international videregivelse.

5.2. Model 2: Moderniserede retsregler

Kommissionen ville i denne model fremlægge **lovgivningsforslag med henblik på en yderligere harmonisering af materielle regler**, præcisere specifikke bestemmelser og afhjælpe den manglende ensartethed forårsaget af varierende tilgange i de forskellige medlemsstater. Disse forslag ville løse problem 1 og 2, da de på den ene side ville **lette datastrømmen inden for EU og fra EU til tredjelande** og på den anden side **præcisere og styrke fysiske personers rettigheder** (f.eks. ved at styrke retten til indsigt og "retten til at blive glemt" og ved at skabe klarere bestemmelser om samtykke og om anmeldelse af brud på datasikkerheden) og **øge registeransvarliges og registerføreres ansvar - og ansvarlighed** - (f.eks. ved at indføre pligt til at udnævne databeskyttelsesansvarlige eller foretage konsekvensanalyser vedrørende databeskyttelse). Denne model ville navnlig udmønte sig i **en one-stop-shop** for registeransvarlige (dvs. én lov og én ansvarlig DPA). Den generelle anmeldelsespligt ville blive forenklet (dvs. basisregistrering). Modellen ville også **øge DPA'ernes uafhængighed og harmonisere deres beføjelser**. Samarbejdet og den gensidige bistand mellem DPA'erne ville blive udbygget, bl.a. gennem en ny **"sammenhængsmekanisme"** med deltagelse af både en - nyetableret - europæisk databeskyttelsesmyndighed og Kommissionen.

For så vidt angår databeskyttelse inden for politisamarbejde og retligt samarbejde i straffesager (problem 3) ville Kommissionen fremlægge forslag om at erstatte rammeafgørelsen med et **nyt instrument med udvidet anvendelsesområde** og afhjælpe **de største huller og mangler** for både at styrke fysiske personers rettigheder og lette samarbejdet mellem de retshåndhævende myndigheder, samtidig med at der tages hensyn til den retshåndhævende sektors særlige karakter.

5.3. Model 3: Detaljerede retsregler på EU-plan

Denne model ville indeholde de fleste elementer af model 2 samt **meget mere detaljeret EU-lovgivning**, herunder sektorlovgivning (f.eks. i sundheds- og sygehussektoren) og en **centraliseret håndhævelsesstruktur på EU-plan** (dvs. oprettelse af en EU-databeskyttelsesmyndighed). Den ville desuden indebære afskaffelse af den generelle anmeldelsespligt (undtagen vedrørende forudgående kontrol af risikabel behandling), indførelse af en EU-certificeringsordning for processer og produkter, der overholder databeskyttelsesreglerne, og fastlæggelse af EU-harmoniserede strafferetlige sanktioner for brud på databeskyttelsesreglerne. Samtykke ville blive defineret som den "primære begrundelse" for databehandling.

Med hensyn til politisamarbejde og retligt samarbejde i straffesager ville model 1 foruden de materielle foranstaltninger fra model 2 indebære, at der fastlægges detaljerede regler for fysiske personers ret til aktindsigt (altid direkte). Den ville også medføre **ændring af de relevante bestemmelser i alle bestående tidligere tredje søjle-instrumenter**, så de fuldt ud kan tilpasses de nye og udvidede harmoniserede regler.

6. KONSEKVENSANALYSE

6.1. Løsningsmodel 1: En blød indsats

De fortolkende meddelelser fra Kommissionen om direktivets bestemmelser ville ikke være bindende og ville derfor **kun have en begrænset virkning med hensyn til at øge retssikkerheden og mindske omkostningerne**. Mere selvregulering på EU-plan kunne skabe større retlig klarhed for de registeransvarlige i bestemte sektorer, men **ville ikke være tilstrækkeligt** til at sikre effektiv, konsekvent anvendelse af reglerne i mangel af en underliggende klar og harmoniseret EU-lovgivning.

Oplysningskampagner ville hjælpe fysiske personer til at få større kendskab til deres databeskyttelsesrettigheder og give dem en bedre forståelse af praktiske måder at udøve dem på. Det ville imidlertid **ikke være tilstrækkeligt** for disse personer at fastslå deres rettigheder, hvis de ikke er klart definerede i loven. **Præcisering af lovgivningen** med hensyn til principperne om gennemsigtighed, dataminimering, tilstrækkelighed og bindende virksomhedsregler ville øge harmoniseringen og retssikkerheden for fysiske personer og virksomheder.

Angående håndhævelse ville meddelelser fra Kommissionen ikke kunne imødegå medlemsstaternes modvilje mod at ændre nationale regler for at give deres DPA'er større uafhængighed og harmoniserede beføjelser. Øget samordning fra Artikel 29-gruppens side og udvekslinger mellem DPA'erne ville have en positiv indvirkning på en mere ensartet håndhævelse af reglerne, men de **fortsatte forskelle i nationale love og i fortolkningen af dem ville begrænse virkningen af et forbedret samarbejde mellem DPA'erne**.

De forventede **finansielle og økonomiske virkninger af denne løsningsmodel er begrænsede**, og de identificerede problemer ville i store træk bestå.

6.2. Løsningsmodel 2: Moderniserede retsregler

Den manglende retssikkerhed for private selskaber og offentlige myndigheder **ville blive afhjulpet i betydeligt omfang**. Problematiske bestemmelser ville blive præciseret og sammenhængen skærpet takket være den indskrænkede fortolkningsfrihed og de gennemførelsesforanstaltninger og/eller delegerede retsakter, som Kommissionen vedtager.

Hvis den generelle pligt til at anmelde databehandling erstattes af et forenklet, **harmoniseret registreringssystem**, samtidig med at de forudgående kontroller af følsomme data og risikabel behandling opretholdes, ville det fritage de registeransvarlige for en pligt, der i øjeblikket gennemføres forskelligt. Ved at registeransvarlige og registerførere pålægges et større ansvar - i bestemte tilfælde og med klart definerede måltærskler - i form af udpegning af databeskyttelsesansvarlige, udførelse af konsekvensanalyser vedrørende databeskyttelse og indførelse af princippet om indbygget databeskyttelse, ville det blive lettere at sikre og at påvise, at reglerne overholdes.

Præcisering og forenkling af reglerne gennem indførelse af én lov, der gælder i hele EU, og oprettelse af en one-stop-shop for databeskyttelseskontrol ville styrke det indre marked, bl.a. ved at fjerne forskellene i DPA'ernes administrative formaliteter. Det vil kunne give en **samlet besparelse**, blot i administration, på ca. **2,3 mia. EUR** om året.

Det vil også fremme en ensartet håndhævelse, hvis DPA'ernes beføjelser styrkes og harmoniseres, og der skabes en stærk mekanisme til samarbejde og gensidig bistand i sager

med en EU-dimension, og hvis lovovertrædelser, for hvilke der pålægges administrative sanktioner, harmoniseres.

En **harmoniseret pligt i hele EU til at anmelde brud på datasikkerheden** vil skabe en bedre beskyttelse af fysiske personer, sikre ensartethed i alle sektorer og hindre konkurrenceforvridning.

Den registreredes rettigheder og fysiske personers kontrol med egne personoplysninger vil kunne styrkes væsentligt ved at indføre nye rettigheder og ved at styrke og præcisere de eksisterende yderligere. Børn vil blive beskyttet af foranstaltninger, der i særlig grad tager hensyn til deres sårbarhed. Foreningerne vil få større råderum med hensyn til at støtte registrerede i udøvelsen af deres rettigheder, herunder i retssager.

Anvendelse af generelle databeskyttelsesprincipper på området for politisamarbejde og retligt samarbejde i straffesager ville styrke den overordnede sammenhæng i EU's databeskyttelsesregler og samtidig tage hensyn til retshåndhævelsesmyndighedernes særtræk. Fysiske personers rettigheder ville i særdeleshed blive styrket ved at udvide anvendelsesområdet for databeskyttelsesreglerne på dette område til også at omfatte national databehandling med tilhørende fastlæggelse af, hvilke betingelser der kan sikre retten til aktindsigt, og ved at indføre strengere regler for formålsbegrænsning.

Med hensyn til den **finansielle og økonomiske virkning** vil den pligt, der pålægges større erhvervsdrivende (over 250 ansatte) til at udpege databeskyttelsesansvarlige, **ikke medføre uforholdsmæssigt store omkostninger**, idet databeskyttelsesansvarlige allerede er almindelige i disse selskaber. Omkostningerne ved at overholde reglerne ville beløbe sig til 320 mio. EUR om året. Pligten ville omfatte et nødvendigt minimumsudsnit af registeransvarlige, idet SMV'erne som regel ikke vil være omfattet af pligten, medmindre deres databehandling indebærer betydelige databeskyttelsesrisici. Offentlige myndigheder og organer ville få ret til at udpege en enkelt databeskyttelsesansvarlig for flere enheder (som f.eks. dækker flere industrier, afdelinger eller kontorer) på baggrund af deres organisatoriske struktur.

En forenkling af reglerne om international videregivelse (f.eks. ved at udvide anvendelsesområdet for bindende virksomhedsregler) ville også have en positiv virkning for det europæiske erhvervslivs konkurrenceevne på internationalt plan.

En styrkelse af DPA'ernes uafhængighed og beføjelser ville sammen med medlemsstaternes pligt til at give dem de nødvendige ressourcer betyde ekstra udgifter for de offentlige myndigheder, som i øjeblikket ikke har de rette beføjelser og tilstrækkelige ressourcer.

Den nye mekanisme for samarbejde og gensidig bistand mellem DPA'erne ville også medføre ekstra omkostninger for nationale DPA'er og for Den Europæiske Tilsynsførende for Databeskyttelse (EDPS). Således vil de ekstra opgaver, som EDPS får ved at skulle varetage sekretariatsfunktionen for Det Europæiske Databeskyttelsesråd, der erstatter Artikel 29-gruppen, og især ved at blive inddraget i sammenhængsmekanismen, sandsynligvis kræve en forøgelse af den tilsynsførendes aktuelle ressourcer med yderligere 3 mio. EUR om året i gennemsnit for de første seks år, herunder bevillinger til flere menneskelige ressourcer i størrelsesordenen 10 årsværk.

6.3. Løsningsmodel 3: Detaljerede retsregler på EU-plan

Yderligere detaljerede lovbestemmelser, herunder sektorlovgivning, ud over de foranstaltninger, der er nævnt i model 2, vil mindske **forskellene mellem medlemsstaterne mest muligt**. Imidlertid er der måske ikke tilstrækkelig fleksibilitet til, at medlemsstaterne kan tage hensyn til nationale særtræk.

En fuldstændig afskaffelse af anmeldelser - undtagen i forbindelse med forudgående kontrol - ville i høj grad forenkle lovgivningen og mindske den administrative byrde.

Oprettelsen af et EU-Databeskyttelsesagentur ville gøre **håndhævelsen meget mere ensartet** og løse problemet med uensartethed i sager med en klar EU-dimension, men et sådant europæisk agents beføjelser kunne være for vidtgående i henhold til EU-retten. Det ville imidlertid være meget bekosteligt for EU's budget. Harmoniserede strafferetlige sanktioner ville også styrke en ensartet håndhævelse, men ville ligeledes blive mødt med stærk modvilje fra medlemsstaterne.

Registreredes rettigheder, inklusive børns, ville blive yderligere styrket, f.eks. ved at udvide definitionen af følsomme data til også at dække personoplysninger om børn, biometriske data og finansielle oplysninger. Indførelsen af en ret til kollektive søgsmål kunne sikre en maksimering af rettighederne gennem retssager. En harmonisering af sanktionsniveauet, herunder strafferetlige sanktioner, på EU-plan forventes at styrke fysiske personers rettigheder yderligere.

Udtrykkelige ændringer af alle instrumenter med henblik på at udvide de generelle databeskyttelsesregler til området for politisamarbejde og retligt samarbejde i straffesager ville have en positiv virkning med hensyn til at sikre ensartethed og sammenhæng mellem reglerne på området og til at styrke fysiske personers rettigheder. Men en så radikal strategi ville møde modstand fra medlemsstaterne og være politisk vanskelig at gennemføre.

7. SAMMENLIGNING AF LØSNINGSMODELLER

Løsningsmodel 1 ville medføre en lav grad af regeloverholdelse og beskedne administrative omkostninger, især for private registeransvarlige, idet det er de nationale og europæiske offentlige myndigheder, der vil få de fleste ekstraomkostninger. Samtidig ville modellen kun have en **begrænset positiv indvirkning på de identificerede problemer og på opfyldelsen af de politiske målsætninger**.

Med hensyn til politisk gennemførlighed vil denne løsningsmodel, om end forslagene ikke er kontroversielle, sandsynligvis blive mødt med modstand fra interessenterne, fordi den kun i begrænset omfang løser problemerne og derfor vil blive betragtet som uambitiøs.

Løsningsmodel 2 vil **mindske fragmenteringen og øge retssikkerheden i betydeligt omfang**. Den forventes i langt højere grad at kunne løse de identificerede problemer og opfylde de politiske målsætninger. De omkostninger, **der er forbundet med denne løsningsmodel til overholdelse og administration, forventes at være rimelige set i lyset af fordelene og besparelserne på omkring 2,3 mia. EUR i administrative byrder om året - noget, der vil være meget vigtigt for virksomhederne**. Denne model vil samlet set give en bedre og mere ensartet håndhævelse. Afskaffelsen af anmeldelsespligten til fordel for et meget enklere basisregistreringssystem ville også forenkle lovgivningen og mindske den administrative byrde.

For så vidt angår interessenternes accept ville denne løsningsmodel generelt blive modtaget positivt af de erhvervsdrivende og de offentlige myndigheder, fordi den samlet set ville reducere deres omkostninger til overholdelse af reglerne, navnlig de omkostninger, der er forbundet med det nuværende fragmenterede regelmiljø. Styrkelsen af databeskyttelsesrettighederne ville blive hilst velkommen af databeskyttelsesaktørerne og især DPA'erne. Vedrørende den tredje generelle målsætning ville denne løsningsmodel bidrage til at opfylde målene om **mere ensartethed og sammenhæng i databeskyttelsesreglerne på området for politisamarbejde og retligt samarbejde i straffesager**, idet rammeafgørelsen ophæves og ajourføres i overensstemmelse med Lissabontraktaten, således at dens mangler afhjælpes, især ved at udvide afgørelsens anvendelsesområde til også at omfatte national behandling.

Løsningsmodel 3 indeholder de fleste af foranstaltningerne i løsningsmodel 2, men er på flere punkter mere vidtrækkende. Den ville derfor have en **stor og positiv indvirkning, både med hensyn til nedbringelse af de omkostninger, der er forbundet med den fragmenterede lovgivning, og styrkelsen af fysiske personers rettigheder**. Desuden ville den maksimere ensartetheden og sammenhængen i databeskyttelsesreglerne i den tidligere tredje søjle og hæve databeskyttelsesstandarderne på det område. Nogle af foranstaltningerne i denne model vil imidlertid enten udløse **uforholdsmæssigt store omkostninger ved regeloveryholdelsen eller møde stærk modstand fra interessenterne**. Desuden ville den samtidige ændring af alle tidligere tredje søjle-instrumenter blive meget kompliceret og politisk kontroversiel.

Foretrukne løsningsmodel:

Den **foretrukne løsningsmodel** er model 2 i kombination med:

- afskaffelse af anmeldelsespligten fra model 3 og
- visse "bløde foranstaltninger" fra model 1, nemlig tilskyndelse til brug af teknologier og certificeringsordninger, der kan forbedre beskyttelsen af privatlivets fred, samt oplysningskampagner.

Den foretrukne løsningsmodel er den, der mest sandsynligt sikrer opfyldelsen af de politiske målsætninger uden uforholdsmæssigt store omkostninger ved regeloveryholdelsen og med en betydelig reduktion af den administrative byrde.

De styrkede databeskyttelsesregler forventes at give anledning til visse ekstra regeloveryholdelsesomkostninger, især for registeransvarlige, der behandler følsomme data. Et stærkt databeskyttelsessystem kan imidlertid give EU's erhvervsliv en konkurrencemæssig fordel, da et højere beskyttelsesniveau og et forventet fald i antallet af databeskyttelseshændelser og -overtrædelser kan øge forbrugernes tillid. Hvis der stilles krav til selskaberne om at indføre høje standarder for databeskyttelse, kan det også give forbedringer på langt sigt for europæiske virksomheder, som kunne blive førende på verdensplan inden for teknologier, der kan forbedre beskyttelsen af privatlivets fred, eller løsninger af typen "Privacy by Design" og derved tiltrække forretninger, job og kapital til Den Europæiske Union.

Endvidere vil den øgede harmonisering gøre grænseoverskridende behandling af personoplysninger enklere og billigere for virksomheder, der driver forretning i EU's indre marked. Dette forventes at give disse virksomheder et væsentligt incitament til at ekspandere over grænserne og høste frugten af det indre marked med deraf følgende gavnlige virkninger for både forbrugerne og den europæiske økonomi som helhed.

Den foretrukne løsningsmodel indeholder også en afbalanceret løsning på problem 3, da den styrker fysiske personers rettigheder, afhjælper mangler og mindsker uensartetheden, for så vidt angår databeskyttelse på området for politisamarbejde og retligt samarbejde i straffesager, samtidig med at den letter samarbejdet om retshåndhævelsen og respekterer sektorens særtræk og operative behov.

8. OVERVÅGNING OG EVALUERING

Overvågningen og evalueringen af virkningen af den foretrukne løsningsmodel vil være rettet mod elementer som f.eks. anvendelsen af de nye instrumenter, der er indført med reformen; de nationale DPA'ers beføjelser og ressourcer; sanktioner, der pålægges for brud på databeskyttelseslovene; registeransvarliges tidsforbrug og omkostninger ved regeloverholdelsen samt udviklingen af fysiske personers tillid til beskyttelsen af deres personoplysninger i onlinemiljøet