KOMMISSIONEN FOR DE EUROPÆISKE FÆLLESSKABER

Bruxelles, den 2.5.2007
KOM(2007) 228 endelig

MEDDELELSE FRA KOMMISSIONEN TIL EUROPA-PARLAMENTET OG RÅDET

om bedre databeskyttelse med teknologier til beskyttelse af privatlivet

MEDDELELSE FRA KOMMISSIONEN TIL EUROPA-PARLAMENTET OG RÅDET

om bedre databeskyttelse med teknologier til beskyttelse af privatlivet

(EØS-relevant tekst)

1. INDLEDNING

Med den intensive og vedvarende udvikling af informations- og kommunikationsteknologier (IKT) opstår der hele tiden nye tjenesteydelser, som forbedrer folks liv. Interaktionen i cyberspace er i vid udstrækning baseret på personlige oplysninger om personer, der færdes i cyberspace, når de køber varer og tjenesteydelser, opretter eller vedligeholder kontakter med andre eller formidler deres ideer til world wide web. Ud over de fordele, som denne udvikling giver borgerne, opstår der også nye risici for dem, for eksempel identitetstyveri, diskriminerende profilering, løbende overvågning eller svig.

Artikel 8 i Den Europæiske Unions charter om grundlæggende rettigheder omhandler retten til beskyttelse af personoplysninger. Denne grundlæggende rettighed er fastlagt i de europæiske regler om beskyttelse af personoplysninger, som især omfatter af databeskyttelsesdirektivet 95/46/EF[1] og e-direktivet om privatlivets fred 2002/58/EF[2] samt databeskyttelsesforordningen (EF) 45/2001[3] om behandlingen af data i fællesskabsinstitutionerne og –organerne. Lovgivningen indeholder mange væsentlige bestemmelser om forpligtelser for den registeransvarlige og om rettigheder for den registrerede. Den fastsætter også sanktioner og passende retsmidler til brug i tilfælde af krænkelser og indfører mekanismer til håndhævelse af reglerne.

Dette system kan måske vise sig ikke at være tilstrækkeligt, når personoplysninger formidles over hele verden gennem IKT-netværk, og behandlingen af data foregår i flere retsområder, ofte uden for EU. I sådanne situationer kan de nuværende regler anses for gældende, og de kan give et klart juridisk svar. Endvidere kan det fastslås, hvilken myndighed der har kompetence til at håndhæve dem. Men der kan være store praktiske forhindringer på grund af vanskeligheder med selve den anvendte teknologi, som indebærer, at data behandles af forskellige aktører forskellige steder, og problemer med at håndhæve nationale administrative og retlige regler i et andet retsområde, især i lande uden for EU.

Det er strengt taget de registeransvarlige, der har det juridiske ansvar for, at reglerne om databeskyttelse overholdes, men andre har også et vist ansvar for databeskyttelse ud fra et

---

1 Europa-Parlamentets og Rådets direktiv 95/46/EF af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger, EFT L 281 af 23.11.1995, s. 31.

2 Europa-Parlamentets og Rådets direktiv 2002/58/EF af 12. juli 2002 om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor (direktivet om databeskyttelse inden for elektronisk kommunikation), EFT L 201 af 31.7.2002, s. 37.

3 Europa-Parlamentets og Rådets forordning (EF) nr. 45/2001 af 18. december 2000 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger i fællesskabsinstitutionerne og -organerne og om fri udveksling af sådanne oplysninger, EFT L 8 af 12.1.2001, s. 1-22.

samfundsmæssigt og et etisk synspunkt. Der er tale om dem, som udformer tekniske specifikationer, og dem, som rent faktisk opbygger eller implementerer applikationer eller operativsystemer.

Ifølge artikel 17 i databeskyttelsesdirektivet har den registeransvarlige en forpligtelse til at gennemføre passende tekniske og organisatoriske foranstaltninger og at tilvejebringe et tilstrækkeligt sikkerhedsniveau i forhold til oplysningernes art og risiciene ved at behandle dem. Brug af teknologi til at støtte overholdelse af lovgivningen, især reglerne om databeskyttelse, er allerede i et vist omfang forudset i direktivet om privatlivets fred[4].

En anden mulighed for at fremme formålet med reglerne, som er at indskrænke behandling af personoplysninger og, hvor det er muligt, benytte anonyme eller pseudonyme oplysninger, kan være at benytte de såkaldte teknologier til beskyttelse af privatlivet. Det vil gøre det lettere at sikre, at krænkelser af databeskyttelsesreglerne og af individets rettigheder ikke blot er forbudt og giver anledning til sanktioner, men at det også teknisk set bliver mere vanskeligt.

Hensigten med denne meddelelse, som er omhandlet i den første beretning om gennemførelsen af databeskyttelsesdirektivet[5], er at se på, hvilke fordele der er ved disse teknologier, at fastlægge Kommissionens målsætninger på dette område for at fremme teknologierne og at foreslå, hvad der skal gøres for at nå dette mål om at støtte udviklingen af disse teknologier og de registeransvarliges og forbrugernes anvendelse heraf.

2. HVAD ER TEKNOLOGIER TIL BESKYTTELSE AF PRIVATLIVET?

Der er en række definitioner på disse teknologier, som anvendes på universiteter og i pilotprojekter om dette emne. Ifølge for eksempel det EF-finansierede PISA-projekt står disse teknologier for et sammenhængende system af IKT-foranstaltninger, der beskytter privatlivet ved at fjerne eller reducere personoplysninger eller forhindre unødvendig og/eller uønsket behandling af personoplysninger, uden at det på nogen måde går ud over informationssystemets funktionalitet. Ved hjælp af teknologierne kan der udformes informations- og kommunikationssystemer og tjenesteydelser, hvor indsamling og anvendelse af personoplysninger kan indskrænkes, og hvor det er lettere at overholde databeskyttelsesreglerne. Kommissionen sagde i den første beretning om gennemførelse af databeskyttelsesdirektivet, at "*…anvendelsen af passende teknologiske foranstaltninger er et vigtigt supplerende element til de retlige foranstaltninger, og at de skal være en integreret del af enhver bestræbelse på at opnå et tilstrækkeligt niveau af privatlivsbeskyttelse*…". Takket være teknologier til beskyttelse af privatlivet skulle det blive vanskeligere at krænke visse databeskyttelsesregler, og/eller det skulle blive lettere at opspore krænkelser.

Med den dynamik, der er på IKT-området, er der forskel på, hvor effektive de forskellige teknologier til beskyttelse af privatlivet er til at sikre beskyttelse af privatlivet, herunder aspekter vedrørende overholdelse af databeskyttelsesloven, og de ændrer sig hele tiden. Der er også forskellige typer. De kan være stand alone-værktøjer, hvor forbrugerne selv må gøre noget (de skal købe og installere dem på deres PC), eller de kan være indbygget i selve informationssystemernes arkitektur. Der kan gives mange eksempler på teknologier til beskyttelse af privatlivet:

---

4 Betragtning 46 og artikel 14, stk. 3, i direktiv 2002/58/EF.

5 KOM(2003) 265(01) af 15.5.2003, se http://eurlex.europa.eu/LexUriServ/site/da/com/2003/com2003_0265da01.pdf

- Automatisk anonymisering af data efter en vis tid underbygger princippet om, at behandlede data ikke bør opbevares på en måde, der gør det muligt at identificere personer i et længere tidsrum, end hvad der er nødvendigt for de formål, dataene oprindeligt blev indsamlet til.

- Krypteringsværktøjer, der kan forhindre hacking, når der sendes oplysninger over internettet, er en støtte for den registeransvarliges forpligtelse til at træffe passende foranstaltninger til at beskytte personoplysninger mod ulovlig behandling.

- Med cookie-cutters, der blokerer cookies, som er placeret på brugerens PC, for at den kan udføre visse instruktioner, uden at brugeren kender til dem, er det lettere at overholde princippet om, at data skal behandles ordentligt og efter reglerne, og at en person skal underrettes om den behandling, der foregår.

- Med P3P (Platform for Privacy Preferences – indstillinger til beskyttelse af personlige oplysninger) er det muligt for en internetbruger at se, hvilken politik netsteder har til beskyttelse af personlige oplysninger, og sammenligne det med, hvilke oplysninger brugeren ønsker at frigive. Det er med til at sikre, at den registreredes samtykke til behandling af personlige oplysninger er et informeret samtykke.

3. KOMMISSIONEN STØTTER TEKNOLOGIER TIL BESKYTTELSE AF PRIVATLIVET

Kommissionen mener, at teknologier til beskyttelse af privatlivet bør udvikles og anvendes mere bredt, end tilfældet er, især når personoplysninger behandles gennem IKT-net. Kommissionen mener, at større brug af disse teknologier vil kunne forbedre beskyttelsen af privatlivet, og at databeskyttelsesreglerne hermed vil være lettere at opfylde. Anvendelsen af teknologierne vil kunne komplementere de nuværende regler og håndhævelsesmekanismer.

I meddelelsen om en strategi for et sikkert informationssamfund (KOM(2006) 251 af 31. maj 2006) opfordrede Kommissionen især den private sektor til at "*stimulere indførelse af sikkerhedsfremmende produkter, processer og tjenester for at forebygge og bekæmpe id-tyveri og andre angreb på privatlivets fred*". Endvidere er et af hovedprincipperne for elektronisk identitetsstyring i Kommissionens køreplan for indførelse af paneuropæiske regler for eIDM inden 2010[6], at systemet skal være sikkert, have de fornødne elementer til at beskytte brugerens privatliv, og brugen heraf skal kunne passe ind i lokale interesser og indstillinger.

Da der medvirker forskellige aktører ved databehandlingen og er forskellige nationale retsområder, kan det være vanskeligt at håndhæve reglerne. På den anden side kan teknologierne i et vist omfang sikre, at visse krænkelser af databeskyttelsesregler, som resulterer i indtrængen i grundlæggende rettigheder som blandt andet privatlivet, kan undgås, fordi det teknologisk set vil blive vanskeligere. Kommissionen er klar over, at teknologi ikke i sig selv er nok til at sikre beskyttelse af privatlivet, selv om det spiller en væsentlig rolle i beskyttelsen heraf. Det er nødvendigt, at teknologierne anvendes efter en reguleringsramme med databeskyttelsesregler, som det er muligt at håndhæve, og som har et vist antal mulige niveauer for beskyttelse af privatlivet for hver især. Brugen af teknologierne betyder ikke, at operatørerne dermed fritages for alle juridiske forpligtelser (f.eks. til at give individuelle brugere ret til at få adgang til deres oplysninger).

[6] http://ec.europa.eu/information_society/activities/egovernment_research/doc/eidm_roadmap_paper.pdf

Vigtige samfundsinteresser vil også bedre kunne tilgodeses. Den juridiske ramme for databeskyttelse indeholder bestemmelser om begrænsninger i de generelle principper og om indgreb i personers rettigheder for at beskytte vigtige samfundsinteresser som offentlig sikkerhed, bekæmpelse af kriminalitet eller folkesundhed. Betingelserne for sådanne begrænsninger er fastlagt i artikel 13 i databeskyttelsesdirektivet og artikel 15 i direktivet om privatlivets fred. De svarer stort set til dem, der er fastlagt i artikel 8 i den europæiske menneskerettighedskonvention (EMRK), nemlig at et sådant indgreb sker i overensstemmelse med loven, og at det ikke er et uforholdsmæssigt indgreb og er nødvendigt i et demokratisk samfund af hensyn til vigtige samfundsinteresser[7]. Brugen af teknologierne må ikke forhindre lovhåndhævelsesorganer eller andre kompetente myndigheder i at gribe ind under en lovmæssig udøvelse af deres funktioner, der skal beskytte vigtige samfundsinteresser, f.eks. bekæmpelse af cyberkriminalitet og af terrorisme eller forebyggelse af spredning af smitsomme sygdomme. De ansvarlige myndigheder bør kunne få adgang til personlige oplysninger, når det er nødvendigt for at nå disse mål, og det bør ske efter de procedurer, betingelser og garantier, der er fastsat i loven.

En bedre overholdelse af databeskyttelsesregler vil også kunne have en positiv indvirkning på forbrugernes tillid, især i cyberspace. For en række lovende, nyttige tjenesteydelser, der beror på overførsel af personoplysninger i it-net, som for eksempel e-læring, e-forvaltning, e-sundhed, e-banking, e-handel eller "intelligente bilsystemer", vil det helt sikkert være en fordel. Folk kan være sikre på, at de oplysninger, de giver for at identificere sig selv, modtage ydelser eller foretage betalinger, kun bliver brugt til legitime formål, og at deres deltagelse i det digitale samfund ikke sker på bekostning af deres rettigheder.

4. FÆRDIGGJORT ARBEJDE OG VEJEN FREM

For at sikre privatlivet endnu bedre og øge databeskyttelsen i Fællesskabet ved blandt andet at udvikle og øge brugen af teknologier til beskyttelse af privatlivet har Kommissionen til hensigt at foretage følgende, hvor en bred vifte af aktører inddrages, herunder egne tjenestegrene, nationale myndigheder, erhvervsliv og forbrugere.

Under drøftelserne vil der blive taget hensyn til den specielle situation, som små og mellemstore virksomheder (SMV'er) er i, og til deres muligheder for at bruge disse teknologier samt incitamenter hertil. Kommissionen vil også se på spørgsmål om blandt andet tillid og kendskab, som har særlig stor betydning for SMV'er.

4.1. Første målsætning: at støtte udviklingen af teknologier til beskyttelse af privatlivet

Hvis disse teknologier skal finde bred anvendelse, må der ske en yderligere udformning, udvikling og fremstilling heraf. Det sker allerede i et vist omfang inden for den offentlige og den private sektor, men Kommissionen mener, at dette arbejde bør optrappes. For at det kan ske, må teknologierne og de hertil knyttede teknologiske krav identificeres, og der må udvikles værktøjer i forbindelse med FTU-aktiviteter.

---

[7] Dom afsagt af Domstolen den 20.5.2003 i de forenede sager C-465/00, C-138/01 og C-139/01 "Österreichischer Rundfunk m.fl." ("Rechnungshof") Sml. [2003] I-04989, præmis 71 og 72.

4.1.1. Aktion 1.1.: At identificere behovet for og teknologiske krav til teknologier til beskyttelse af privatlivet

Teknologierne er meget afhængige af udviklingen inden for IKT. Når det er blevet fastslået, hvilke farer den teknologiske udvikling medfører, må der stilles passende krav til en teknologisk løsning.

Kommissionen vil opfordre forskellige interessegrupper til at samles og debattere teknologier til beskyttelse af privatlivet. Disse grupper kan omfatte repræsentanter fra IKT-sektoren, udviklere af sådanne teknologier, databeskyttelsesmyndigheder, lovhåndhævelsesorganer, teknologipartnere (herunder eksperter på relevante områder som e-sundhed eller informationssikkerhed), og forbruger- og borgerretssammenslutninger. De bør løbende følge med i, hvordan teknologien udvikler sig, hvilke farer det indebærer for grundlæggende rettigheder og databeskyttelse, og hvilke tekniske krav der kan stilles til disse teknologier. Der kan være tale om finjustering af de teknologiske foranstaltninger efter de forskellige risici og de forskellige data og hensyntagen til beskyttelse af samfundsinteresser som for eksempel offentlig sikkerhed.

4.1.2. Aktion 1.2.: At udvikle teknologier til beskyttelse af privatlivet

Efterhånden som det bliver fastslået, hvordan behovet er for disse teknologier, og hvilke teknologiske krav der skal stilles hertil, må der arbejdes på at nå frem til et slutprodukt, der er klar til brug.

Kommissionen har allerede set på hvordan behovet er. Inden for rammerne af 6. rammeprogram sponsoreres PRIME-projektet[8], der behandler spørgsmål om digital identitetsstyring og beskyttelse af privatlivet i informationssamfundet. OPEN-TC-projektet[9] giver mulighed for at opnå et sikkert computersystem, og DISCREET-projektet[10] udvikler middleware, der kan håndhæve beskyttelse af privatlivet i avancerede nettjenester. Senere hen vil Kommissionen under 7. rammeprogram støtte andre FTU-projekter og omfattende pilotprojekter, som kan udvikle og stimulere overtagelsen af teknologier til beskyttelse af privatlivet. Hensigten er at skabe et grundlag for tjenesteydelser til beskyttelse af privatlivet, som styres af brugerne selv, og som forener de lovmæssige og tekniske forskelle, der er i Europa, gennem offentligt-private partnerskaber.

Kommissionen opfordrer også nationale myndigheder og den private sektor til at investere i udvikling af disse teknologier. Det er afgørende for at få europæisk erhvervsliv placeret forrest i en sektor, som vil vokse, efterhånden som de teknologiske standarder mere og mere kræver brug af disse teknologier, og forbrugerne også vil kræve det, når de bliver klar over, at det er nødvendigt at beskytte deres rettigheder i cyberspace.

4.2. Anden målsætning: at støtte de registeransvarliges brug af teknologier til beskyttelse af privatlivet

Der vil kun kunne drages fordel af disse teknologier, hvis de indsættes i og benyttes i det tekniske udstyr og software-værktøjer, der bruges til behandling af personoplysninger. Det er derfor af afgørende betydning, at virksomheder, der fremstiller sådant udstyr, og registeransvarlige, som anvender det til databehandling, deltager heri.

---

8 https://www.prime-project.eu/

9 http://www.opentc.net/

10 http://www.ist-discreet.org/

4.2.1. Aktion 2.1.: At fremme erhvervslivets brug af teknologier til beskyttelse af privatlivet

Kommissionen er overbevist om, at alle, der har at gøre med behandling af personoplysninger, vil have fordel af at benytte disse teknologier i højere grad. IKT-virksomheder, der er de primære udviklere og udbydere af teknologierne, har en særlig vigtig rolle at spille, når det gælder om at fremme brugen af dem. Kommissionen opfordrer alle registeransvarlige til at inddrage og gøre intensiv brug af teknologierne i deres arbejde. Med henblik herpå vil Kommissionen afholde seminarer, hvor der skal deltage nøgleaktører fra IKT-virksomheder, navnlig dem, der udvikler teknologierne, for at få undersøgt, hvordan de vil kunne bidrage til at fremme brugen heraf blandt registeransvarlige.

Kommissionen vil også foretage en undersøgelse af, hvilke økonomiske fordele der er ved teknologierne, og formidle resultaterne heraf for at opfordre virksomheder, især SMV'er, til at anvende dem.

4.2.2. Aktion 2.2.: At sikre respekt for passende standarder til beskyttelse af personoplysninger gennem teknologier til beskyttelse af privatlivet

Hvis der skal gøres vidtrækkende fremstød, kræver det en aktiv indsats fra de IKT-virksomheder, der fremstiller teknologierne, men respekt for passende standarder kræver en indsats, som ligger ud over selvregulering eller goodwill fra de involverede aktørers side. Kommissionen vil vurdere behovet for at udvikle standarder for lovlig behandling af personoplysninger med disse teknologier gennem konsekvensanalyser. Der kan blive tale om to slags instrumenter, afhængigt af resultatet af disse analyser:

- *Aktion 2.2.a) Standardisering*

Kommissionen mener, at der ved standardisering skal tages hensyn til overholdelse af databeskyttelsesreglerne. Kommissionen vil bestræbe sig på at inddrage indlæggene fra interessegrupperne i debatten om teknologier til beskyttelse af privatlivet under forberedelserne af sine egne tiltag og det arbejde, der gøres i de europæiske standardiseringsorganer. Det er især vigtigt, hvis det under debatten viser sig, at det ved visse databeskyttelsesregler er nødvendigt at inddrage og gøre brug af nogle af disse teknologier.

Kommissionen kan bede de europæiske standardiseringsorganisationer (CEN, CENELEC, ETSI) om at se på, om der er specifikke europæiske behov, og om efterfølgende at bringe dem op på internationalt niveau ved at anvende eksisterende aftaler mellem europæiske og internationale standardiseringsorganer. I givet fald bør de europæiske standardiseringsorganer fastlægge et specifikt standardiseringsprogram, der dækker de europæiske behov og således supplerer det igangværende arbejde på internationalt niveau.

- *Aktion 2.2.b) Koordinering af nationale tekniske regler om sikkerhedsforanstaltninger ved databehandling.*

National lovgivning, der vedtages i medfør af databeskyttelsesdirektivet[11], giver databeskyttelsesmyndighederne en vis indflydelse på at fastsætte de tekniske krav mere præcist og for eksempel udarbejde en vejledning for registeransvarlige, undersøge de systemer, der indføres, eller udstede tekniske instruktioner. De nationale databeskyttelsesmyndigheder kan også stille krav om, at der skal inddrages og anvendes visse teknologier til beskyttelse af privatlivet, når

[11] F.eks. artikel 17.

behandlingen af personoplysninger gør det nødvendigt. Kommissionen mener, at dette er et område, hvor en koordinering af national praksis vil kunne bidrage positivt til at fremme brugen af teknologierne. Især Artikel 29-Gruppen[12] vil kunne bidrage, da den har til opgave at sørge for en ensartet anvendelse af nationale foranstaltninger, der vedtages i henhold til direktivet. Kommissionen opfordrer derfor Artikel 29-Gruppen til under sit arbejde på området at medtage et fast punkt i sit program, hvor behovet for at inddrage teknologierne i databehandlingsopgaver analyseres, hvilket er en effektiv måde at sikre overholdelse af databeskyttelsesreglerne på. Der kan så udarbejdes retningslinjer for databeskyttelsesmyndighederne, som skal implementere dem på nationalt plan, gennem en koordineret vedtagelse af passende instrumenter.

4.2.3. Aktion 2.3.: At fremme offentlige myndigheders brug af teknologier til beskyttelse af privatlivet

Offentlige myndigheder gennemfører et stort antal behandlinger, hvori der indgår personoplysninger, når de udøver deres beføjelser både på nationalt plan og på fællesskabsplan. Offentlige organer er selv bundet af respekten for grundlæggende rettigheder, herunder retten til beskyttelse af personoplysninger, og de skal sikre, at de respekteres af andre, hvorfor de bør foregå med et godt eksempel.

For de nationale myndigheders vedkommende har Kommissionen bemærket en mere og mere udbredt anvendelse af applikationer til e-forvaltning, der har til formål at øge effektiviteten af den offentlige service. Som det fremgår af *Kommissionens meddelelse om e-forvaltningens betydning for Europas fremtid*[13], er det nødvendigt at anvende teknologier til beskyttelse af privatlivet, hvis der skal opbygges tillid til, at systemet fungerer. Kommissionen opfordrer regeringerne til at sørge for, at der indgår databeskyttelsesforanstaltninger i applikationer til e-forvaltning, og at der gøres bredest mulig brug af disse teknologier ved udformningen og gennemførelsen af sådanne applikationer.

For fællesskabsinstitutionernes og –organernes vedkommende vil Kommissionen sørge for, at kravene i forordning (EF) nr. 45/2001 overholdes, navnlig ved en større brug af teknologierne i forbindelse med IKT-applikationer, der indebærer behandling af personoplysninger. Samtidig opfordrer Kommissionen andre EU-institutioner til at gøre det samme. Den Europæiske Tilsynsførende for Databeskyttelse kan være med til at rådgive fællesskabsinstitutionerne og -organerne og at opstille interne regler for behandling af personoplysninger. Når Kommissionen udvælger nye IKT-applikationer til eget brug eller videreudvikler eksisterende applikationer, vil det blive set på, om der er mulighed for at indføre teknologier til beskyttelse af privatlivet. Betydningen af disse teknologier vil fremgå af Kommissionens overordnede it-forvaltningsstrategi. Kommissionen vil også hele tiden sørge for at informere sit eget personale herom. For at kunne implementere teknologierne i Kommissionens IKT-applikationer må der dog være relevante produkter tilgængelige, og de må evalueres hver for sig og ses i lyset af, hvordan den enkelte applikation udvikler sig.

---

[12] Gruppe vedrørende Beskyttelse af Fysiske Personer i forbindelse med Behandling af Personoplysninger, nedsat ved artikel 29 i direktiv 95/46/EF.

[13] KOM(2003) 567 endelig af 26.9.2003.

4.3. Tredje målsætning: at opfordre forbrugerne til at benytte teknologier til beskyttelse af privatlivet

Forbrugerne vil fortsat være den part, for hvem det er mest relevant, at personoplysninger bliver anvendt ordentligt, at databeskyttelsesreglerne håndhæves ordentligt, og at teknologierne til at sikre dette er effektive.

Det bør derfor gøres helt klart for forbrugerne, hvilke fordele brugen af teknologierne giver med hensyn til at mindske risiciene ved transaktioner, der indebærer behandling af deres personlige data. De bør også kunne træffe et informeret valg, når de køber it-udstyr og software eller benytter e-tjenesteydelser. Det bør ske ud fra et kendskab til de risici, der er forbundet hermed, navnlig om teknologierne tilbyder en passende beskyttelse Brugerne må derfor have adgang til enkle, forståelige oplysninger om teknologiske værktøjer, der kan beskytte privatlivet. Øget brug af teknologier til beskyttelse af privatlivet og af e-tjenesteydelser, hvor disse teknologier er indført, vil kunne give økonomisk gevinst til de virksomheder, der bruger dem, og det kan give en sneboldeffekt, som får andre virksomheder til at lægge større vægt på at overholde databeskyttelsesreglerne. Det kræver, at der iværksættes en række tiltag.

4.3.1. Aktion 3.1.: At gøre forbrugerne mere bevidste

Der bør vedtages en passende strategi, som kan gøre forbrugerne mere bevidste om, hvilke risici der er forbundet med behandling af deres data, og hvilke løsninger teknologierne kan tilbyde som et supplement til de eksisterende systemer i lovgivningen om databeskyttelse. Kommissionen vil lancere en række informationskampagner i hele EU om disse teknologier.

Hovedansvaret herfor ligger hos de nationale databeskyttelsesmyndigheder, som allerede har relevant erfaring på området. Kommissionen opfordrer dem til at udvide deres forbrugeroplysning til også at omfatte oplysninger om teknologier til beskyttelse af privatlivet med alle til rådighed stående midler. Kommissionen opfordrer også Artikel 29-Gruppen til at koordinere national praksis og sætte det ind i en sammenhængende arbejdsplan, der kan øge bevidstheden om teknologierne, og til at fungere som kontaktsted for udveksling af god praksis, som allerede er indført på nationalt plan. Det er navnlig forbrugersammenslutninger og andre aktører, for eksempel Det Europæiske Netværk af Forbrugercentre, som er et netværk for hele EU og har til opgave at rådgive borgerne om deres rettigheder som forbrugere, der kan blive partnere i forsøget på at opdrage forbrugerne.

4.3.2. Aktion 3.2.: At gøre det lettere for forbrugerne at træffe et informeret valg: Datasikkerhedsmærkning

Det vil være lettere at få folk til at forstå og bruge teknologierne, hvis det er let at se, at de er tilstede i et bestemt produkt, og hvad de grundlæggende går ud på. Med henblik herpå vil Kommissionen undersøge, om det er muligt at indføre et system for hele EU med datasikkerhedsmærkning, blandt andet ved at foretage en analyse af økonomiske og samfundsmæssige konsekvenser. Formålet med sådanne datasikkerhedsmærkninger er at gøre det let for forbrugerne at se, om der ved et bestemt produkt er sikkerhed for, at databeskyttelsesreglerne overholdes ved behandlingen af data, især om der er indført passende teknologier til beskyttelse af privatlivet.

For at datasikkerhedsmærkningerne kan opfylde deres mål, mener Kommissionen, at følgende principper må respekteres:

– Antallet af systemer til datasikkerhedsmærkning bør holdes på et minimum. Hvis der er alt for mange datasikkerhedsmærkninger, kan det skabe mere forvirring hos forbrugerne og undergrave tilliden til alle mærkninger. Derfor bør der foretages en vurdering af, om og i hvilket omfang det vil være passende at indføre en europæisk datasikkerhedsmærkning i en mere generel ordning for sikkerhedscertificering[14].

– Datasikkerhedsmærkninger bør kun tildeles et produkt, som overholder en række standarder svarende til databeskyttelsesreglerne. Standarderne bør være så ensartede som muligt i hele EU.

– De offentlige myndigheder, herunder navnlig databeskyttelsesmyndighederne, bør spille en vigtig rolle og deltage i fastsættelse af relevante standarder og procedurer samt overvåge, at systemet med datasikkerhedsmærkning fungerer.

På baggrund heraf og under hensyntagen til de erfaringer, der er gjort i forbindelse med datasikkerhedsmærkningsprogrammer på andre områder (f.eks. miljø, landbrug, sikkerhedscertificering for varer og tjenesteydelser), vil Kommissionen indgå en dialog med alle berørte parter, herunder nationale databeskyttelsesmyndigheder, erhvervs- og forbrugersammenslutninger og standardiseringsorganer.

[14] I en meddelelse fra 31. maj 2006 om en strategi for et sikkert informationssamfund – "Dialog, partnerskab og myndiggørelse" (KOM(2006) 251 endelig), opfordrede Kommissionen allerede den private sektor til at "arbejde hen imod prismæssigt overkommelige sikkerhedscertificeringsordninger, der omfatter produkter, processer og tjenester, og som opfylder EU-specifikke behov (navnlig hvad angår beskyttelse af privatlivets fred)".