HENSTILLINGER

KOMMISSIONENS HENSTILLING

af 1. marts 2011

om retningslinjer for gennemførelsen af databeskyttelsesbestemmelserne i forbrugerbeskyttelsessamarbejdssystemet CPSC (Consumer Protection Cooperation System)

(2011/136/EU)

EUROPA-KOMMISSIONEN HAR —

som henviser til traktaten om Den Europæiske Unions funktionsmåde, særlig artikel 292, og

som tager følgende i betragtning:

(1) Målet med Europa-Parlamentets og Rådets forordning (EF) nr. 2006/2004 af 27. oktober 2004 om samarbejde mellem nationale myndigheder med ansvar for håndhævelse af lovgivning om forbrugerbeskyttelse (»forordningen om forbrugerbeskyttelsessamarbejde«) ([1]) (»CPC-forordningen«) er at styrke samarbejdet om håndhævelse af forbrugerbeskyttelseslovgivningen i det indre marked. Ved denne forordning er der oprettet et EU-netværk af offentlige myndigheder med ansvar for håndhævelse af forbrugerbeskyttelseslovgivning i medlemsstaterne (»CPC-netværket«). I forordningen opstilles desuden de generelle rammer og betingelser for, hvordan medlemsstaternes myndigheder kan samarbejde om at beskytte forbrugernes økonomiske interesser.

(2) Samarbejdet mellem nationale håndhævelsesmyndigheder er afgørende for, at det indre marked kan fungere effektivt, og i CPC-netværket kan den enkelte myndighed anmode de andre myndigheder om bistand til at undersøge eventuelle overtrædelser af EU's forbrugerbeskyttelseslovgivning.

(3) Målet med forbrugerbeskyttelsessamarbejdssystemet (»CPCS«) er at gøre det muligt for offentlige håndhævelsesmyndigheder i et sikkert miljø at udveksle oplysninger om eventuelle overtrædelser af forbrugerbeskyttelseslovgivningen.

(4) Den elektroniske informationsudveksling mellem medlemsstaterne skal overholde bestemmelserne om beskyttelse af personoplysninger i 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 ([2]) (»direktivet om databeskyttelse«) og i 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 ([3]) (»forordningen om databeskyttelse«).

(5) I artikel 8 i EU's charter om grundlæggende rettigheder anerkendes retten til databeskyttelse. CPCS skal sikre en klar fordeling af de forskellige forpligtelser og ansvar på databeskyttelsesområdet mellem Kommissionen og medlemsstaterne, og at de registrerede bliver informeret og får let adgang til mekanismer, der gør det muligt for dem at udøve deres rettigheder.

(6) Det er hensigtsmæssigt at opstille retningslinjer for gennemførelsen af databeskyttelsesbestemmelserne i CPSC (»retningslinjer«) for at sikre, at databeskyttelsesbestemmelserne overholdes, når oplysninger behandles i CPCS.

(7) Håndhævelsestjenestemænd bør opfordres til at kontakte deres nationale databeskyttelsesmyndigheder for at få vejledning i, hvordan retningslinjerne bedst kan gennemføres i overensstemmelse med national lovgivning, og om nødvendigt for at sikre, at der på nationalt plan gennemføres procedurer for anmeldelse og forudgående kontrol i relation til behandling af data under CPCS.

(8) De kompetente myndigheder bør opfordres kraftigt til at deltage i kurser afholdt af Kommissionen for at bistå dem med gennemførelsen af retningslinjerne.

(9) Tilbagemeldinger til Kommissionen om gennemførelsen af retningslinjerne skal være Kommissionen i hænde senest to år efter henstillingens vedtagelse. Derefter bør Kommissionen foretage en ny evaluering af databeskyttelsesniveauet i CPCS og vurdere, om der er behov for yderligere instrumenter, herunder lovgivningsmæssige foranstaltninger.

([1]) EUT L 364 af 9.12.2004, s. 1.

([2]) EFT L 281 af 23.11.1995, s. 31.

([3]) EFT L 8 af 12.1.2001, s. 1.

(10) Der bør træffes de nødvendige foranstaltninger for at fremme, at aktører og brugere af CPCS gennemfører retningslinjerne. De nationale databeskyttelsesmyndigheder og Den Europæiske Tilsynsførende for Databeskyttelse bør nøje overvåge udviklingen og gennemførelsen af databeskyttelsesbestemmelserne, for så vidt angår CPCS.

(11) Retningslinjerne supplerer Kommissionens beslutning 2007/76/EF [1] og tager hensyn til udtalelsen fra gruppen vedrørende beskyttelse af personer i forbindelse med behandling af personoplysninger nedsat ved artikel 29 [2] i direktivet om databeskyttelse og udtalelsen fra Den Europæiske Tilsynsførende for Databeskyttelse (»den tilsynsførende«) [3], der blev indført ved artikel 41 i forordningen om databeskyttelse —

VEDTAGET DENNE HENSTILLING:

Medlemsstaterne følger retningslinjerne i bilaget til henstillingen.

Udfærdiget i Bruxelles, den 1. marts 2011.

På Kommissionens vegne
John DALLI
Medlem af Kommissionen

[1] EUT L 32 af 6.2.2007, s. 192.
[2] Udtalelse 6/2007 om databeskyttelsesspørgsmål i forbindelse med forbrugerbeskyttelsessamarbejdssystemet (CPCS) — 01910/2007/DA — WP 130 — vedtaget den 21. september 2007.
[3] EDPS Opinion Ref. 2010-0692.

BILAG

Retningslinjer for gennemførelsen af databeskyttelsesbestemmelserne i CPCS (Consumer Protection Cooperation System)

1. INDLEDNING

Samarbejde mellem nationale forbrugerbeskyttelsesmyndigheder er afgørende for det indre markeds funktion. Uden en effektiv håndhævelse på tværs af grænserne undermineres forbrugernes tillid til at benytte sig af grænseoverskridende tilbud og dermed også til det indre marked, samtidig med at der opstår konkurrenceforvridning.

It-værktøjet CPCS, der er oprettet ved CPC-forordningen, er en struktureret mekanisme til informationsudveksling mellem nationale forbrugerbeskyttelsesmyndigheder, der er med i CPC-netværket. Med dette værktøj kan en offentlig myndighed anmode andre offentlige myndigheder i CPC-netværket om bistand til at efterforske og håndtere eventuelle overtrædelser af EU's forbrugerbeskyttelseslovgivning og til at træffe retshåndhævende foranstaltninger for at stoppe sælgeres og leverandørers ulovlige handelspraksis over for forbrugere, der bor i andre EU-lande. Informationsanmodninger og al kommunikation mellem kompetente offentlige myndigheder om anvendelsen af CPC-forordningen sker gennem CPCS.

Målet med CPC-forordningen er at forbedre håndhævelsen af forbrugerbeskyttelseslovgivningen i det indre marked gennem oprettelsen af et netværk af nationale håndhævelsesmyndigheder i hele EU og at fastlægge betingelserne for medlemsstaternes samarbejde. Ifølge CPC-forordningen skal informationsudvekslinger og anmodninger om gensidig bistand mellem nationale håndhævelsesmyndigheder ske via en dertil oprettet database. CPCS skulle derfor lette det administrative samarbejde og informationsudvekslingen og dermed styrke EU's forbrugerbeskyttelseslovgivning.

Samarbejdet er begrænset til overtrædelser inden for Fællesskabet af de retsakter, der er opført i bilaget til CPC-forordningen, og som beskytter forbrugernes kollektive økonomiske interesser.

2. RETNINGSLINJERNES ANVENDELSESOMRÅDE OG MÅL

Retningslinjerne sigter mod at skabe ligevægt mellem på den ene side et effektivt, målrettet håndhævelsessamarbejde mellem de kompetente myndigheder i medlemsstaterne og på den anden side respekt for den grundlæggende ret til privatlivets fred og beskyttelse af personoplysninger.

Personoplysninger defineres i direktivet om databeskyttelse [1] som enhver oplysning om en identificeret eller identificerbar fysisk person. Ved identificerbar person forstås en person, der direkte eller indirekte kan identificeres, f.eks. ved et identifikationsnummer eller et eller flere elementer, som er særlige for denne persons fysiske, fysiologiske, psykiske, økonomiske, kulturelle eller sociale identitet.

Eftersom nationale håndhævelsestjenestemænd (sagsbehandlere), der er brugere af CPCS, ikke nødvendigvis er databeskyttelseseksperter og måske ikke altid er tilstrækkeligt bekendte med databeskyttelseskravene i deres egen nationale databeskyttelseslovgivning, tilrådes det at give CPCS-brugere retningslinjer og en beskrivelse af, hvordan CPCS fungerer i praksis rent databeskyttelsesmæssigt, samt en detaljeret beskrivelse af de sikkerhedsforanstaltninger, der er indbygget i systemet, og eventuelle risici i forbindelse med brugen af det.

Formålet med retningslinjerne er at dække de vigtigste databeskyttelsesspørgsmål i tilknytning til CPCS og give en brugervenlig forklaring, som alle CPCS-brugere kan henvises til. De giver imidlertid ikke en udtømmende analyse af CPCS' konsekvenser for databeskyttelsen.

Det henstilles indtrængende, at medlemsstaternes databeskyttelsesmyndigheder høres for at sikre, at retningslinjerne suppleres med særlige forpligtelser i de nationale databeskyttelseslove. CPCS-brugere kan også få yderligere hjælp og vejledning fra de nationale databeskyttelsesmyndigheder, så man sikrer, at databeskyttelseskravene opfyldes. En liste over disse myndigheder samt kontaktoplysninger og websteder findes på:

http://ec.europa.eu/justice_home/fsj/privacy/nationalcomm/#eu

Det bør understreges, at behandling af personoplysninger bør ske i overensstemmelse med de særlige principper og betingelser i direktivet om databeskyttelse. Sagsbehandlere har inden for rammerne af forordningen ret til at udveksle data, herunder personoplysninger, via CPCS, hvis formålet med behandlingen er at stoppe overtrædelser af EU's forbrugerlove som opført i CPC-forordningens bilag. Men før sådanne oplysninger behandles, skal der foretages en omhyggelig vurdering for at sikre, at databeskyttelsesprincipperne er overholdt, og at databehandlingen er strengt nødvendig for at nå målene i CPC-forordningen.

[1] Artikel 2, litra a).

Sagsbehandlere med adgang til CPCS skal således foretage en vurdering fra sag til sag, før personoplysninger kan behandles ([1]). Formålet med disse retningslinjer er at bistå sagsbehandlerne med denne vurdering, således at de databeskyttelsesprincipper, der beskrives i retningslinjerne, kommer til at indgå i betragtningerne.

Målet er også at afklare nogle af de mere komplekse aspekter af CPCS-strukturen vedrørende fælles behandlingsaktiviteter og fælles kontroludøvelse, idet de indeholder en beskrivelse af Kommissionens og medlemsstaternes kompetente myndigheders rolle som »fælles registeransvarlige« for CPCS-dataudvekslinger.

3. CPCS — ET IT-VÆRKTØJ TIL HÅNDHÆVELSESSAMARBEJDE

CPCS er et it-værktøj, der er udviklet og administreres af Kommissionen i samarbejde med medlemsstaterne. CPCS er tænkt som en hjælp til medlemsstaterne til den praktiske gennemførelse af EU's forbrugerbeskyttelseslovgivning. Systemet bruges af CPC-netværket, der består af offentlige myndigheder udpeget af medlemsstaterne og EØS-landene, og som skal samarbejde og udveksle oplysninger med hinanden i håndhævelsen af forbrugerbeskyttelseslove som omhandlet i CPC-forordningen.

Det hedder i artikel 10 i CPC-forordningen, at:

»Kommissionen opretholder en elektronisk database, hvor den lagrer og behandler de oplysninger, den modtager i henhold til artikel 7, 8 og 9. Kun de kompetente myndigheder har mulighed for at konsultere databasen.«

Og i artikel 12, stk. 3, i CPC-forordningen tilføjes følgende:

»Anmodninger om bistand og enhver formidling af oplysninger fremsættes skriftligt under anvendelse af en standardformular og fremsendes elektronisk via den i artikel 10 omhandlede database.«

CPCS letter samarbejde om og udveksling af oplysninger vedrørende overtrædelser inden for Fællesskabet af de direktiver og forordninger, der er opført i bilaget til CPC-forordningen, og som behandler en bred vifte af emner såsom urimelig handelspraksis, fjernsalg, forbrugerkredit, pakkerejser, urimelige kontraktbetingelser, timeshare, e-handel og andet. CPCS kan ikke bruges til informationsudveksling på lovgivningsområder, der ikke er specifikt opført i bilaget.

Eksempler:

I. En handlende, der er etableret i Belgien, benytter sig af urimelige vilkår over for forbrugere bosiddende i Frankrig, hvilket er en overtrædelse af direktivet om urimelige kontraktvilkår. Forbrugermyndigheden i Frankrig kan bruge CPCS til at fremsætte en anmodning til forbrugermyndigheden i Belgien om at træffe de nødvendige håndhævelsesforanstaltninger, der er til rådighed i Belgien, over for den handlende, således at der bliver sat en øjeblikkelig stopper for overtrædelsen inden for Fællesskabet.

II. Forbrugermyndigheden i Danmark modtager klager over, at der på et bestemt websted bruges svigagtig og vildledende handelspraksis til skade for forbrugerne. Webstedets vært befinder sig i Sverige. Den danske forbrugermyndighed har brug for oplysninger om webstedet. Den kan derfor bruge CPCS til at fremsende en informationsanmodning til den svenske forbrugermyndighed, som har pligt til at tilvejebringe oplysningerne.

Oplysninger uploades af medlemsstaterne, opbevares i CPCS, er tilgængelige for de medlemsstater, som oplysningerne er stilet til, og slettes af Kommissionen ([2]). CPCS bruges som informationsbank og som middel til at udveksle oplysninger i et effektivt, sikkert kommunikationssystem.

Ud fra et databeskyttelsesperspektiv medfører oprettelsen af en sådan database altid visse risici for den grundlæggende ret til beskyttelse af personoplysninger, f.eks. udveksling af flere oplysninger end strengt nødvendigt for at sikre et effektivt samarbejde, opbevaring af oplysninger, der skulle have været slettet, opbevaring af oplysninger, der ikke længere er nøjagtige eller er ukorrekte, eller manglende sikring af, at registreredes rettigheder og registeransvarliges forpligtelser overholdes. Sådanne risici skal derfor håndteres ved at sikre, at brugerne af CPCS er velinformerede om og veluddannede i databeskyttelsesbestemmelser og kan sikre overholdelse af gældende databeskyttelseslovgivning.

4. LOVGIVNINGS- OG TILSYNSRAMMER FOR DATABESKYTTELSE

EU har haft et etableret retsgrundlag for databeskyttelse siden 1995, såsom direktivet om databeskyttelse ([3]) vedrørende medlemsstaternes behandling af personoplysninger og forordningen om databeskyttelse ([4]) vedrørende EU's institutioners og organers behandling af personoplysninger. Hvilken databeskyttelseslov der anvendes, afhænger i øjeblikket af, hvem CPCS-aktøren eller -brugeren er.

([1]) Det skal bemærkes, at databeskyttelsesprincipper finder anvendelse både på data, der opbevares elektronisk og som papirkopi.
([2]) De præcise bestemmelser for sletning findes bl.a. i beslutning 2007/76/EF og i »The Consumer Protection Cooperation Network: Operating Guidelines«.
([3]) Direktiv 95/46/EF.
([4]) Forordning (EF) nr. 45/2001.

Kommissionens behandlingsaktiviteter er omfattet af forordningen om databeskyttelse, mens behandlingsaktiviteter foretaget af sagsbehandlere i de kompetente nationale håndhævelsesmyndigheder henhører under den nationale lovgivning, der omsætter direktivet om databeskyttelse.

Kommissionen og de udpegede kompetente myndigheder spiller begge en specifik rolle i CPCS, fordi de sammen fungerer som registeransvarlige. De har derfor pligt til at anmelde og fremsende deres respektive behandlingsaktiviteter til forudgående kontrol hos de relevante tilsynsmyndigheder og sikre overholdelse af databeskyttelsesbestemmelserne. Når det er sagt, kan nationale love, der gennemfører direktivet om databeskyttelse, indeholde undtagelser både fra kravet om anmeldelse og kravet om forudgående kontrol.

Målet med at harmonisere databeskyttelseslovene var at sikre både et højt databeskyttelsesniveau og den enkeltes grundlæggende rettigheder, samtidig med at det blev muligt frit at overføre personoplysninger mellem medlemsstaterne. De nationale gennemførelsesforanstaltninger kan give anledning til forskelligartede bestemmelser, og brugerne af CPCS rådes for at sikre overholdelse af databeskyttelsesbestemmelserne kraftigt til at drøfte de foreliggende retningslinjer med deres nationale databeskyttelsesmyndigheder, da der f.eks. kan være forskellige regler for, hvilke oplysninger enkeltpersoner skal have, eller pligten til at indberette bestemte behandlingsaktiviteter til databeskyttelsesmyndighederne.

Et centralt træk ved de retlige rammer for EU's databeskyttelse er de uvildige databeskyttelsesmyndigheders kontrol. Borgerne har ret til at indgive klager til disse myndigheder og få en hurtig, udenretlig løsning på deres databeskyttelsesbekymringer. Behandling af personoplysninger på nationalt plan overvåges af de nationale databeskyttelsesmyndigheder, mens EU's institutioners behandling af personoplysninger overvåges af Den Europæiske Tilsynsførende for Databeskyttelse ([1]). Kommissionen er følgelig underlagt den tilsynsførendes kontrol, mens andre CPCS-brugere er underlagt kontrol af de nationale databeskyttelsesmyndigheder.

5. HVEM ER HVEM I CPCS? — SPØRGSMÅLET OM FÆLLES KONTROLUDØVELSE

CPCS er et klart eksempel på fælles behandlingsaktiviteter og fælles kontroludøvelse. Mens det kun er de kompetente myndigheder i medlemsstaterne, der kan indsamle, registrere, videregive og udveksle personoplysninger, er opbevaring og sletning af disse oplysninger Kommissionens ansvar. Kommissionen har ikke adgang til disse personoplysninger, men betragtes som systemadministrator og -operatør.

Fordelingen af de forskellige opgaver og ansvar mellem Kommissionen og medlemsstaterne kan opsummeres som følger:

— Hver kompetent myndighed er registeransvarlig for sine egne databehandlingsaktiviteter.

— Kommissionen er ikke bruger, men operatør af systemet, og primært ansvarlig for systemarkitekturens vedligeholdelse og sikkerhed. Kommissionen har dog også adgang til varslinger, feedbackinformation og andre sagsrelaterede oplysninger ([2]). Formålet med Kommissionens adgang er at overvåge anvendelsen af CPC-forordningen og forbrugerbeskyttelseslovgivningen i bilaget til CPC-forordningen og samle statistiske oplysninger i forbindelse med varetagelsen af disse opgaver. Kommissionen har dog ikke adgang til oplysningerne i anmodninger om gensidig bistand og håndhævelse, da disse kun sendes til de kompetente myndigheder i medlemsstaterne, der behandler de pågældende specifikke spørgsmål. Når det er sagt, giver CPC-forordningen Kommissionen mulighed for at bistå kompetente myndigheder i tilfælde af visse tvister ([3]) og blive opfordret til at deltage i en koordineret undersøgelse, der omfatter mere end to medlemsstater ([4]).

— CPCS-aktørerne deler ansvaret for behandlingens lovlighed, oplysningspligten og retten til indsigt, indsigelse og berigtigelse.

— Både Kommissionen og de kompetente myndigheder er i deres egenskab af registeransvarlige individuelt ansvarlige for, at bestemmelserne i relation til deres databehandlinger stemmer overens med databeskyttelsesreglerne.

6. AKTØRER OG BRUGERE I CPCS

Der findes forskellige adgangsprofiler i CPCS: Adgang til databasen er begrænset, tildeles kun en navngiven tjenestemand hos en kompetent myndighed (autentificeret bruger) og kan ikke overdrages til andre. Adgang til CPCS kan kun gives til tjenestemænd, som de kompetente myndigheder i medlemsstaterne har udnævnt og oplyst til Kommissionen. Det log-in/den adgangskode, der skal bruges for at komme ind i systemet, kan tildeles det centrale forbindelseskontor.

Kun brugere hos de bistandssøgte og bistandssøgende kompetente myndigheder har fuld adgang til alle de oplysninger, der udveksles i en bestemt sag, hvilket omfatter alle bilag i CPCS' sagsakter. De centrale forbindelseskontorer har kun adgang til de oplysninger om en sag, der sætter dem i stand til at identificere den kompetente myndighed, som en anmodning skal overføres til. De har ikke adgang til fortrolige dokumenter, der er vedlagt en anmodning eller en varsling som bilag.

([1]) http://www.edps.europa.eu/EDPSWEB/edps/EDPS.
([2]) Artikel 8, 9 og 15 i CPC-forordning (EF) nr. 2006/2004.
([3]) Artikel 8, stk. 5, i CPC-forordning (EF) nr. 2006/2004.
([4]) Artikel 9 i CPC-forordning (EF) nr. 2006/2004.

I håndhævelsessager kan brugere hos alle de kompetente myndigheder, som er anmeldt som ansvarlige for de retsakter, der er overtrådt, udveksle generelle oplysninger. Det sker gennem anmeldelser. Disse anmeldelser bør give en bred beskrivelse af en sag og undgå at inddrage personoplysninger. Der findes dog undtagelser som f.eks. sælgers eller leverandørs navn (hvis det er en fysisk person).

Kommissionen har ikke adgang til anmodninger om oplysninger og håndhævelser eller fortrolige dokumenter, men modtager anmeldelser og varslinger.

7. DATABESKYTTELSESPRINCIPPER FOR INFORMATIONSUDVEKSLING

Personoplysninger kan kun behandles af CPCS-brugerne i medlemsstaterne på bestemte betingelser og i overensstemmelse med de principper, som direktivet om databeskyttelse opstiller. Den registeransvarlige er ansvarlig for at sikre, at databeskyttelsesprincipperne overholdes i forbindelse med behandling af personoplysninger i CPCS.

Det skal også bemærkes, at både bestemmelserne om fortrolighed og bestemmelserne om databeskyttelse finder anvendelse på CPCS. Fortrolighedsbestemmelserne og bestemmelserne om tavshedspligt kan finde anvendelse på oplysninger generelt, mens bestemmelserne om databeskyttelse er begrænset til personoplysninger.

Det er vigtigt at huske, at CPCS-brugerne i medlemsstaterne er ansvarlige for mange andre behandlingsaktiviteter, og at de ikke nødvendigvis er databeskyttelseseksperter. Overholdelse af databeskyttelsesreglerne i CPCS behøver ikke være unødigt kompliceret eller medføre en uforholdsmæssigt stor administrativ byrde. Systemet skal heller ikke nødvendigvis være et universalsystem, der passer til alle. Disse retningslinjer er henstillinger vedrørende behandling af personoplysninger, og der skal gøres opmærksom på, at det ikke er alle oplysninger, som udveksles inden for rammerne af CPCS, der er personoplysninger.

Før hver uploading af oplysninger til CPCS skal håndhævelsesmyndighederne vurdere, om de personoplysninger, der skal fremsendes, er strengt nødvendige for at opnå et effektivt samarbejde, og overveje, hvem de sender personoplysningerne til. Håndhævelsestjenestemanden skal spørge sig selv, om modtageren virkelig har brug for de pågældende oplysninger til varslingen eller anmodningen om gensidig bistand.

Nedenstående liste over grundlæggende databeskyttelsesprincipper er tænkt som en hjælp til håndhævelsestjenestemænd med adgang til CPCS til at foretage en vurdering fra sag til sag af, om databeskyttelsesbestemmelserne for behandling af personoplysninger bliver overholdt, hver gang de behandler personoplysninger i systemet. Håndhævelsestjenestemænd bør også holde sig for øje, at der på nationalt plan kan være undtagelser fra og begrænsninger for anvendelsen af nedenstående databeskyttelsesprincipper, og de rådes til at konsultere deres nationale databeskyttelsesmyndigheder ([1]).

Databeskyttelsesprincipper, der skal overholdes

De generelle principper for databeskyttelse, der skal tages hensyn til, før man går i gang med at behandle personoplysninger, er fastlagt i direktivet om databeskyttelse. Eftersom dette direktiv er omsat til national lovgivning, anmodes sagsbehandlere om at konsultere deres nationale databeskyttelsestilsynsmyndigheder vedrørende anvendelsen af nedenstående principper, og de rådes til at undersøge, om der findes undtagelser fra eller begrænsninger for anvendelsen af disse principper.

Princippet vedrørende gennemsigtighed

I henhold til direktivet om databeskyttelse har den registrerede ret til at blive orienteret, når den pågældendes personoplysninger behandles. Den registeransvarlige skal oplyse sit navn og sin adresse, formålet med behandlingen, modtagerne af oplysningerne og alle andre fornødne oplysninger for at sikre, at behandlingen er rimelig ([2]).

Oplysninger må kun behandles i følgende tilfælde ([3]):

— Når den registrerede har givet sit samtykke.

— Når behandlingen er nødvendig i forbindelse med udformning eller indgåelse af en kontrakt.

— Når behandling er nødvendig for at overholde en retlig forpligtelse.

— Når behandling er nødvendig for at beskytte den registreredes vitale interesser.

([1]) Artikel 11, stk. 2, og artikel 13 i direktiv 95/46/EF.
([2]) Artikel 10 og 11 i direktiv 95/46/EF.
([3]) Artikel 7 i direktiv 95/46/EF.

— Når behandlingen er nødvendig af hensyn til udførelsen af en opgave i samfundets interesse eller henhørende under offentlig myndighedsudøvelse, som den registeransvarlige eller en tredjemand, til hvem oplysningerne videregives, har fået pålagt.

— Når behandlingen er nødvendig, for at den registeransvarlige eller den tredjemand eller de tredjemænd, til hvem oplysningerne videregives, kan forfølge en legitim interesse.

Princippet vedrørende lovlighed og rimelighed

Personoplysninger må ikke indsamles eller behandles på ulovlige eller urimelige måder, og de må ikke bruges til formål, der ikke er forenelige med målene i CPC-forordningen. For at behandlingen skal være lovlig, skal sagsbehandlerne sikre sig, at de har klare grunde, der berettiger behandlingen. Behandlingen skal foretages til udtrykkeligt angivne og legitime formål, og senere behandling må ikke være uforenelig med disse formål ([1]). Dette kan alene være baseret på CPC-forordningen.

For at behandlingen skal være rimelig, skal de registrerede informeres om formålet med behandlingen af den pågældendes personoplysninger og deres ret til indsigt, berigtigelser og indvendinger.

Princippet vedrørende proportionalitet, korrekthed og opbevaringsperioder

Personoplysningerne skal være proportionelle, tilstrækkelige, relevante og ikke omfatte mere end det, der er nødvendigt i forhold til de formål, hvortil de er indsamlet og/eller efterfølgende behandlet. Oplysningerne skal være korrekte og om nødvendigt ajourført. Der skal tages ethvert rimeligt skridt til at sikre, at oplysninger, der er ukorrekte eller ufuldstændige i forhold til de formål, hvortil de indsamles, eller i forbindelse med hvilke de behandles på et senere tidspunkt, slettes eller berigtiges. Personoplysninger må ikke opbevares på en måde, der giver mulighed for at identificere de registrerede i et længere tidsrum end det, der er nødvendigt af hensyn til de formål, hvortil de indsamles, eller i forbindelse med hvilke de behandles. Der skal fastsættes relevante garantier for personoplysninger, der i historisk, statistisk eller videnskabeligt øjemed opbevares længere end i ovennævnte periode.

Sagsbehandlerne skal vurdere, om de oplysninger, de behandler, er strengt nødvendige i forhold til de formål, der ønskes opfyldt.

Princippet vedrørende formålsbegrænsning

Personoplysninger skal indsamles til udtrykkeligt angivne og legitime formål, og senere behandling heraf må ikke være uforenelig med disse formål og skal bringes til den registreredes kendskab. Sagsbehandlerne må kun behandle personoplysninger, når det har et klart formål, dvs. når der er et retsgrundlag i CPC-forordningen, som begrunder overførslen.

Ret til indsigt

Registrerede har i henhold til direktivet om databeskyttelse ([2]) ret til at få oplyst, at deres personoplysninger behandles, formålene med behandlingen, modtagerne af oplysningerne, og at de har bestemte rettigheder, f.eks. retten til information og berigtigelser. Den registrerede har ret til indsigt i alle oplysninger, der behandles om vedkommende. Den registrerede har også ret til at anmode om berigtigelse, sletning eller blokering af oplysninger, der er ufuldstændige, ukorrekte eller ikke behandles i overensstemmelse med databeskyttelsesbestemmelserne ([3]).

Følsomme data

Behandling af personoplysninger om racemæssig eller etnisk baggrund, politisk, religiøs eller filosofisk overbevisning, fagforeningsmæssigt tilhørsforhold og oplysninger om helbredsforhold og seksuelle forhold er forbudt. Databeskyttelsesdirektivet ([4]) omfatter dog visse undtagelser fra denne bestemmelse, hvor følsomme oplysninger kan behandles på visse betingelser ([5]). Da CPCS-brugere kan komme i en situation, hvor de behandler følsomme oplysninger ([6]), tilrådes det at nærme sig dem med forsigtighed. CPCS-brugere anbefales at konsultere deres nationale databeskyttelsesmyndighed med hensyn til, om der gælder undtagelser for behandlingen af følsomme oplysninger.

Undtagelser

I forbindelse med forebyggelse, efterforskning, afsløring og retsforfølgning i straffesager omfatter direktivet om databeskyttelse nogle undtagelser. Sagsbehandlerne rådes til at konsultere national lovgivning for at vurdere, om der er mulighed for sådanne undtagelser og i bekræftende fald i hvilket omfang ([7]). Hvis der indføres sådanne undtagelser, henstilles det, at de anføres klart i den enkelte kompetente myndigheds fortrolighedserklæringer.

([1]) Artikel 6, stk. 1, litra b), i direktiv 95/46/EF.
([2]) Artikel 10, 11 og 12 i direktiv 95/46/EF.
([3]) Artikel 12 i direktiv 95/46/EF.
([4]) Artikel 8, stk. 2, i direktiv 95/46/EF.
([5]) Artikel 8 i direktiv 95/46/EF.
([6]) Kapitel 4 i bilaget til beslutning 2007/76/EF.
([7]) Udtalelse 6/2007 om databeskyttelsesspørgsmål i forbindelse med forbrugerbeskyttelsessamarbejdssystemet (CPCS) — 01910/2007/DA — WP 130 — vedtaget den 21. september 2007, s. 24.

Anvendelse af databeskyttelsesprincipperne

Anvendelse af disse databeskyttelsesprincipper på CPCS fører til følgende henstillinger:

1) Brug af CPCS bør være strengt begrænset til de formål, der er anført i CPC-forordningen. Det hedder i artikel 13, stk. 1, i CPC-forordningen, at udleverede oplysninger kun kan anvendes til at sikre overholdelse af lovgivning, som beskytter forbrugernes interesser. Disse love er opført i bilaget til CPC-forordningen.

2) Håndhævelsestjenestemænd rådes til kun at bruge oplysninger, der stammer fra en anmodning om gensidig bistand eller varsling til formål, der vedrører den specifikke sag, under nøje overholdelse af lovbestemmelserne om databeskyttelse, og forudgående vurdere nødvendigheden af behandlingen i forbindelse med undersøgelser foretaget ud fra en bredere samfundsinteresse.

3) Håndhævelsestjenestemænd bør i forbindelse med overførsel af oplysninger foretage en vurdering fra sag til sag af, hvem der skal modtage de oplysninger, som skal behandles.

4) CPCS-brugerne bør omhyggeligt udvælge de spørgsmål, de stiller i anmodningen om gensidig bistand, og ikke bede om flere oplysninger end nødvendigt. Det handler ikke kun om at overholde principperne om oplysningernes pålidelighed, men også om at mindske den administrative byrde.

5) Direktivet om databeskyttelse [1] indeholder krav om, at personoplysninger skal være korrekte og ajourførte. Det henstilles, at den kompetente myndighed, som leverede oplysningerne, bidrager til at sikre, at oplysninger, der opbevares i CPCS, er korrekte. Pop up-beskeder i CPCS minder regelmæssigt sagsbehandlerne om at kontrollere, om personoplysningerne er korrekte og ajourførte.

6) En praktisk måde at informere de registrerede om deres rettigheder er ved hjælp af en omfattende meddelelse om beskyttelse af privatlivets fred på webstedet. Det henstilles, at alle kompetente myndigheder anbringer en meddelelse om beskyttelse af privatlivets fred på deres websteder. Denne meddelelse bør være i overensstemmelse med alle oplysningsforpligtelserne i direktivet om databeskyttelse og indeholde et link til Kommissionens websted om disse meddelelser og om andre oplysninger såsom kontaktoplysninger for den pågældende kompetente myndighed og eventuelle nationale begrænsninger i retten til indsigt eller oplysninger. Alle involverede registeransvarlige er ansvarlige for offentliggørelse af meddelelser om beskyttelse af privatlivets fred.

7) De registrerede kan anmode om indsigt i, berigtigelse og sletning af personoplysninger fra mere end én kilde. Selv om hver kompetent myndighed i sin egenskab af registeransvarlig er ansvarlig for sine egne behandlingsaktiviteter, bør der opnås en koordineret tilgang til anmodninger i relation til grænseoverskridende sager. Det henstilles, at de kompetente myndigheder i sådanne tilfælde meddeler andre kompetente myndigheder, at de har modtaget anmodningen.

   Hvis en kompetent myndighed mener, at imødekommelse af en anmodning kan påvirke en efterforsknings- eller håndhævelsesprocedure, der udføres af andre kompetente myndigheder, bør førstnævnte høre sidstnævnte, før anmodningen imødekommes.

   Den registrerede kan også henvende sig til Kommissionen med sin anmodning. Kommissionen kan kun imødekomme en anmodning om oplysninger, som den har adgang til. Når Kommissionen modtager en anmodning, bør den konsultere den kompetente myndighed, der har fremsendt oplysningerne. Hvis der ikke gøres indsigelser, eller den kompetente myndighed ikke besvarer henvendelsen inden for en rimelig frist, kan Kommissionen beslutte, om anmodningen skal imødekommes på grundlag af forordningen om databeskyttelse. Kommissionen bør også høre de kompetente myndigheder, hvis efterforsknings- eller håndhævelsesaktiviteter kan blive påvirket som et resultat af, at anmodningen imødekommes. Kommissionen bør undersøge, om yderligere tekniske funktioner i CPCS ville fremme sådanne udvekslinger.

8) I henhold til CPC-beslutning 2007/76/EF om gennemførelse kan der oprettes oplysningsfelter i CPCS til navne på virksomhedsledere. Håndhævelsestjenestemændene skal vurdere, om det er nødvendigt at medtage den type personoplysninger for at løse sagen. Der skal foretages en vurdering fra sag til sag af, om det er nødvendigt at indsætte navnet på en virksomhedsleder i det relevante felt, før hver uploading af oplysninger til CPCS og før der sendes en varsling eller en anmodning om gensidig bistand til en anden kompetent myndighed.

9) CPC-beslutning 2007/76/EF om gennemførelse indeholder et krav om, at den kompetente myndighed, der uploader oplysninger, håndhævelsesanmodninger eller varslinger, skal angive, om oplysningerne skal behandles som fortrolige. Dette afgøres fra sag til sag. På samme måde skal den bistandssøgte myndighed, når den leverer oplysninger, anføre, om oplysningerne skal behandles som fortrolige. CPCS indeholder en standardværdifunktion, hvor CPCS-brugere udtrykkeligt skal give adgang til dokumenter ved at slå fortrolighedsmarkøren fra.

[1] Artikel 6, stk. 1, litra d), i direktiv 95/46/EF.

8. CPCS OG DATABESKYTTELSE

Databeskyttelsesvenligt miljø

CPCS er udformet på grundlag af krav i databeskyttelseslovgivningen:

— CPCS bruger s-TESTA (secured Trans European Services for Telematics between Administrations), som udgør en styret, pålidelig og sikker transeuropæisk kommunikationsplatform for europæiske og nationale myndigheder. s-TESTA-netværket bygger på en dedikeret privat infrastruktur, der er fuldstændig adskilt fra internettet. Systemets udformning omfatter passende sikkerhedsforanstaltninger, der sikrer den bedst mulige beskyttelse af netværket. Netværket er sikkerhedsgodkendt for at gøre det egnet til at sende oplysninger, der klassificeres som »EU RESTRICTED«.

— Der findes en række tekniske funktioner: anmeldelse af sikre og personlige adgangskoder til kompetente tjenestemænd hos de udpegede myndigheder, brug af et sikkert netværk (s-TESTA), pop up-beskeder, der minder sagsbehandlerne om, at de skal indtænke databeskyttelsesbestemmelser i behandlingen af personoplysninger, oprettelse af forskellige brugerprofiler, der gør adgang til oplysninger afhængig af brugerens rolle (den kompetente myndighed, det centrale forbindelseskontor eller Kommissionen), mulighed for at begrænse adgang til dokumenter ved at markere dem som fortrolige og beskeden på CPCS-hjemmesiden, der henviser til databeskyttelsesbestemmelserne.

— Gennemførelsesbestemmelser ([1]), der dækker centrale aspekter for at sikre overholdelse af databeskyttelsesbestemmelserne: klare regler for sletning (hvilke oplysninger, hvor og hvornår oplysninger skal slettes o.l.), principper vedrørende fastlæggelse af de forskellige former for adgang til oplysninger (kun direkte berørte kompetente myndigheder har fuld adgang, mens andre kun har adgang til generelle oplysninger).

— Praktiske retningslinjer ([2]), som yderligere præciserer, hvad der skal tages i betragtning i forbindelse med udfyldelsen af de forskellige oplysningsfelter, og integration af disse retningslinjer ([3]).

— Årlige revisioner til sikring af, at de kompetente myndigheder kontrollerer, om personoplysningerne er korrekte (mærkning er planlagt, men endnu ikke gennemført), og også, at sager er afsluttet og/eller slettet og dermed ikke glemmes. Kommissionen arrangerer jævnligt sammen med medlemsstaterne en systematisk gennemgang af de sager, der har været åbne i en væsentlig længere periode end den gennemsnitlige sagsbehandlingsperiode.

— Automatisk sletning af sager om gensidig bistand fem år efter en sags afslutning som krævet i CPC-forordningen.

— CPCS er et it-værktøj under udvikling, som skal være databeskyttelsesvenligt Der er allerede nu indbygget mange garantifunktioner i systemarkitekturen, som er beskrevet ovenfor. Kommissionen agter at videreudvikle og forbedre systemet efter behov.

Yderligere hjælp

Hvor længe bør en sag opbevares, og hvornår skal den afsluttes og slettes?

Kun Kommissionen kan slette oplysninger fra CPCS ([4]) og gør det normalt efter anmodning fra en kompetent myndighed. Når en kompetent myndighed fremsender en sådan anmodning, skal den indeholde en begrundelse for anmodningen om sletning. Den eneste undtagelse er anmodninger om håndhævelse. Dem sletter Kommissionen automatisk, fem år efter at den bistandssøgende myndighed har afsluttet sagen.

Bestemmelserne med faste tidsfrister er indført for at sikre sletning af data, der ikke længere er nødvendige, er ukorrekte, viser sig at være ubegrundede og/eller har været opbevaret i det maksimale tidsrum.

Hvorfor er opbevaringsperioden for oplysninger fastsat til fem år?

Formålet med opbevaringsperioden er at lette samarbejdet mellem offentlige myndigheder med ansvar for håndhævelsen af de love, der beskytter forbrugernes interesser i forbindelse med overtrædelser inden for Fællesskabet, at bidrage til at sikre det indre markeds gnidningsfrie funktion, kvaliteten af og konsekvensen i håndhævelsen af love, der beskytter forbrugernes interesser, tilsynet med beskyttelsen af forbrugernes økonomiske interesser og at hæve standarden for og konsekvensen i håndhævelsen. I løbet af opbevaringsperioden kan autoriserede håndhævelsestjenestemænd, der arbejder for en kompetent myndighed, som oprindelig behandlede en sag, have adgang til sagen for at konstatere forbindelser til eventuelle gentagne overtrædelser, hvilket bidrager til en bedre og mere effektiv håndhævelse.

([1]) Beslutning 2007/76/EF.
([2]) The Consumer Protection Cooperation Network: Operating Guidelines — godkendt af CPC-udvalget den 8. juni 2010.
([3]) Retningslinjernes indhold vil indgå i fremtidige kurser i CPCS.
([4]) Artikel 10 i CPC-forordning (EF) nr. 2006/2004 og kapitel 2 i bilaget til CPC-beslutning 2007/76/EF om gennemførelse.

Hvilke oplysninger kan indgå i diskussionsforummet?

Diskussionsforummet er en funktion under CPCS og er et værktøj til udveksling af oplysninger om f.eks. nye håndhævelsesbeføjelser og bedste praksis. Generelt bør diskussionsforummet, der dog ikke bruges så ofte af håndhævelsestjenestemænd, ikke bruges til udveksling af sagsrelaterede oplysninger og ikke henvise til personoplysninger.

Hvilken type oplysninger kan medtages i korte resuméer og bilag?

I overensstemmelse med CPC-beslutning 2007/76/EF om gennemførelse er der et felt med betegnelsen »bilag« i varslinger og anmodninger om oplysninger og håndhævelse. De korte resuméer er felter, hvor overtrædelsen beskrives. Det henstilles, at personoplysninger ikke medtages i de korte resuméer, da formålet med dette felt er at give en generel beskrivelse af overtrædelsen. Personoplysninger i bilag, der ikke er strengt nødvendige, skal skjules eller slettes.

Hvad betyder en »rimelig formodning« om, at der er sket en overtrædelse?

Rimelig formodning skal fortolkes i henhold til national lovgivning. Det henstilles dog, at formodninger om overtrædelser kun medtages i CPCS, hvis der er beviser for, at der er sket eller sandsynligvis vil ske en overtrædelse.

Hvad med overførsler til tredjelande?

Det hedder i CPC-forordningen [1], at oplysninger, som videregives i henhold til CPC-forordningen, også kan videregives til en myndighed i et tredjeland af en medlemsstat i henhold til en bilateral bistandsaftale med tredjelandet, såfremt der er indhentet samtykke fra den kompetente myndighed, som oprindelig videregav oplysningerne, og såfremt videregivelsen er i overensstemmelse med databeskyttelsesbestemmelserne.

Det henstilles, at bilaterale aftaler om bistand med et givet tredjeland, så længe EU ikke har indgået en international aftale om samarbejdsordninger vedrørende gensidig bistand [2], bør indeholde passende databeskyttelsesbestemmelser og anmeldes til de relevante databeskyttelsestilsynsmyndigheder, således at der kan foretages forudgående kontrol, medmindre Kommissionen har konstateret, at tredjelandet sikrer et passende beskyttelsesniveau for personoplysninger, der videregives fra EU i henhold til artikel 25 i direktivet om databeskyttelse.

---

[1] Artikel 14, stk. 2, i CPC-forordning (EF) nr. 2006/2004.
[2] Artikel 18 i CPC-forordning (EF) nr. 2006/2004.