Datatilsynet

Justis- og beredskapsdepartementet
Postboks 8005 Dep
0030 OSLO

Deres referanse	Vår referanse (bes oppgitt ved svar)	Dato
	12/00398-2/CBR	4. juli 2012

Høringsuttalelse – EU-kommisjonens forslag til nye personvernregler

Det vises til Justis- og beredskapsdepartementets høringsbrev av 19. april 2012, vedrørende EU-kommisjonens forslag til generell forordning om behandling og overføring av personopplysninger.

Sammendrag

§ Datatilsynet ønsker et nytt, oppdatert personvernregelverk velkommen.
§ Flere av de sentrale bestemmelsene i det fremlagte forslaget er en kodifisering av gjeldende norsk rett.
§ Datatilsynet mener et fullverdig norsk medlemskap i *European Data Protection Board (EDPB)*, må være et ufravikelig krav fra norske myndigheter for å kunne implementere det nye regelverket.

Datatilsynets overordnede kommentarer

Innledningsvis vil Datatilsynet bemerke at det er svært vanskelig å overskue alle konsekvenser av det fremlagte forslaget.

Det skyldes for det første at forordningen åpner for at det kan etableres *nasjonale regelverk* på en rekke områder, og at Kommisjonen gis kompetanse til å etablere utfyllende *europeisk regelverk*[1]. Rettstilstanden vil derved være uavklart på en rekke områder, også dersom forordningen vedtas.

I tillegg kommer at forordningens *virkeområde* er svært omfattende. Datatilsynet forutsetter at sektormyndighetene opplyser mer i detaljer hvilke eventuelle virkninger forordningen vil få innen de ulike sektorene, og gir i det følgende mer generelle og overordnede vurderinger av forslaget.

Datatilsynet legger *det reviderte utkastet* av 22. juni 2012 til grunn for sin uttalelse.

[1] Implementing acts og delegated acts

Postadresse:	Kontoradresse:	Telefon:	Telefaks:	Org.nr:	Hjemmeside:
Postboks 8177 Dep 0034 OSLO	Tollbugt 3	22 39 69 00	22 42 23 50	974 761 467	www.datatilsynet.no

Behov for nytt, harmonisert regelverk
Dagens personverndirektiv (95/46/EF), som den norske personopplysningsloven bygger på, er fra 1995. Regelverket er derved skapt uten tanke på senere teknologiutvikling og internettbruk. Selv om gjeldende regleverk er teknologinøytralt er det allikevel nødvendig å se på reguleringen i lys av denne utviklingen. Datatilsynet ønsker derfor et nytt, oppdatert regelverk på personvernområdet velkommen.

Såfremt beskyttelsesnivået i det nye regelverket generelt sett blir hevet i forhold til i dag, støtter Datatilsynet også det underliggende målet om økt harmonisering mellom landene i Europa. Dagens regulering har resultert i ulikt beskyttelsesnivå i de forskjellige europeiske statene, og et mer harmonisk regelverk vil derfor kunne øke borgernes rettssikkerhet.

Selv om kommisjonen har valgt en forordning som rettslig instrument, er det i det fremlagte forslaget såpass stort nasjonalt handlingsrom at man kan stille spørsmål ved om forslaget vil føre til økt harmonisering i Europa. Blant annet brukes hensynet til "*public interest"* i artiklene 6, 9, 17, 21, 33, 44 og 81 for å beskrive situasjoner hvor nasjonalstatene kan avvike fra forordningens hovedlinjer. Datatilsynet mener det er vanskelig å fullt ut overskue omfanget og innholdet av nasjonale regelverk, og hvilke konsekvenser det får for intensjonen om harmonisering.

Høyere beskyttelsesnivå
Det materielle innholdet i gjeldende forslag til regulering vil kunne gi et høyere beskyttelsesnivå i Europa, enn gjeldende regulering. Tilsynet er imidlertid av den oppfatning at det norske beskyttelsesnivået i det store og hele opprettholdes ved en eventuell innføring av forordningen.

Særegne utfordringer for Norge
Som ikke-medlem av EU gir forordningsutkastet flere særegne utfordringer for Norge. En utfordring gjelder deltagelse i *European Data Protection Board (EDPB)*, et nytt organ som er foreslått opprettet for å sikre en harmonisert regulatorisk praksis i Europa. Selv om det nye personvernregelverket også vil gjelde for Norge, er ikke norske myndigheter tiltenkt medlemskap i EDPB (se mer utfyllende kommentar om EDPB senere i høringsuttalelsen).

En annen utfordring gjelder muligheten for å påvirke utarbeidelsen av delegerende eller implementerende rettsakter. Datatilsynet mener at EFTA/EØS-landene bør gis mulighet til å uttale seg om innholdet i delegerende og implementerende rettsakter før de vedtas, slik EU-landene har tilgang til via Europaparlamentet og Rådet. Dette kan for eksempel spesifiseres i fortalens punkt 130.

Unntak for små og mellomstore bedrifter
I kapittel 4 om behandlingsansvarliges og databehandlers plikter gjøres det en rekke unntak for små og mellomstore bedrifter, det vil si bedrifter med færre enn 250 ansatte.

Dette gjelder bestemmelsene om at behandlingsansvarlige utenfra EU skal utnevne en representant i EU (artikkel 25), dokumentasjonskrav (artikkel 28) og plikten til å oppnevne et personvernombud (artikkel 35). I tillegg åpnes det for særordninger for små og mellomstore bedrifter når det gjelder prosedyrer og mekanismer for utøvelse av den registrertes rettigheter (artikkel 12(6)), informasjonsplikt (artikkel 14(7)), behandlingsansvarliges ansvar (artikkel

22(4)) og konsekvensutredning forut for behandlinger som representerer en viss risiko (artikkel 33(6)).

Datatilsynet mener det bør være behandlingens karakter som avgjør hvilke plikter som påhviler en behandlingsansvarlig, ikke tallet på ansatte i virksomheten. I Norge var det per 1.1.2012 kun 643 av 487 138 bedrifter som hadde flere enn 250 ansatte. Dette utgjør kun 0,13 prosent av virksomhetene. Eventuelle unntak for små- og mellomstore bedrifter vil derfor i praksis omfatte nesten fleste norske bedrifter.

For mye makt til kommisjonen
Datatilsynet mener det på minst to områder gis for mye makt til EU-kommisjonen.

Det første området gjelder kommisjonens mulighet til å overstyre nasjonale personvernmyndigheter i enkeltsaker for å sikre harmonisering og konsistens (jf.artikkel 62). Dette mener Datatilsynet truer personvernmyndighetenes uavhengighet, en rettighet som slås fast i artikkel 47.

Det andre gjelder kommisjonens generelle mulighet til å utarbeide delegerende og implementerende rettsakter (forskriftskompetanse). Mens gjeldende personverndirektiv (95/46/EF) gir kommisjonen forskriftskompetanse på bare ett område, gir det foreslåtte forordningsutkastet kommisjonen forskriftskompetanse på i alt 26 artikler. Datatilsynet mener en del av forskriftskompetansen legges til essensielle deler av forordningens innhold. Blant annet legges det opp til delegerende rettsakter i artikkel 6(5) om sektorspesifikke kriterier for avveining mellom interessene til behandlingsansvarlig og den registrerte. Dette berører et av de vanligste behandlingsgrunnlagene, og innholdet i en slik delegert rettsakt vil derfor ha stor betydning for det materielle innholdet i forordningen. Datatilsynet mener derfor at man bør begrense kommisjonens forskriftskompetanse til bare å gjelde ikke-essensielle deler, slik Artikkel 290 i *Traktaten om Den europeiske unions funksjonsmåte* (EUF-traktaten) krever.

Kommentarer til konkrete bestemmelser i forordningsforslaget

Utvidet geografisk virkeområde (artikkel 3)
Datatilsynet er positivt til at man foreslår å utvide personvernlovgivningens geografiske virkeområde til også å gjelde behandlingsansvarlige som ikke er etablert i EU, også uten at disse benytter hjelpemidler i et EU-land. Utvidelsen har til hensikt å sikre at alle borgere bosatt i Europa vil nyte godt av det vernet som europeisk personvernlovgivning gir, uavhengig av hvilket land den behandlingsansvarlige virksomheten er etablert i.

Det kan stilles spørsmål ved om det er mulig å håndheve den foreslåtte lovgivningen utenfor Europas grenser. Slik forslaget nå foreligger, er det ikke gitt hvordan europeiske tilsynsmyndigheter skal gjennomføre kontroller med, og gi pålegg til, virksomheter som ikke er etablert i EU. Før bestemmelsen trer i kraft bør det avklares hvordan håndhevelsen skal utøves, og etableres eventuelle rettslige instrumenter som er nødvendige (avtaler mellom EU og tredjeland).

Datatilsynet er også bekymret for at bestemmelsen i sin ytterste konsekvens kan fremtvinge et grunnlag for nasjonale myndigheter til å blokkere enkelte tjenestetilbydere fra den "nasjonale" delen av Internett, for å gjennomføre et slags "innførselsforbud". Dette må eventuelt utredes nærmere.

Definisjoner (artikkel 4)
Datatilsynet mener at uttrykket "transfer" (overføring) bør gis en egen definisjon. I norsk rett har det vært tvil om innholdet av dette begrepet. Det gjelder for eksempel spørsmålet om hvorvidt en fjernaksessløsning til data i Norge, for en databehandler i et tredjeland, medfører en overføring av opplysningene. Begrepet er sentralt i en rekke sammenhenger, blant annet for å definere det nærmere innholdet i andre definisjoner (jf artikkelens pkt 17 om binding corporate rules).

Mindreårige (artikkel 8)
Det er foreslått å kodifisere et prinsipp om at personer under 13 år ikke gyldig kan samtykke til deltagelse i et nettsamfunn. Det oppstilles et vilkår om at foreldre eller verge samtykker på vegne av barnet. Dette er gjeldende praksis i Datatilsynet pr i dag.

Sensitive personopplysninger (artikkel 9)
I henhold til norsk personopplysningslov er opplysninger om man er mistenkt, siktet, tiltalt eller dømt for en straffbar handling regnet som sensitive (artikkel 9). Den norske ordlyden går derved lengre enn forslaget til forordning (og gjeldende personverndirektiv), som kun gir anvisning på at det er opplysninger om at man er dømt ("convictions") som er sensitivt. Dersom dette vedtas vil gjeldende norsk rett endres, slik at opplysninger om at man er mistenkt, siktet eller tiltalt ikke lenger er å anse som sensitive.

Dette vil særlig få betydning for de tilfeller hvor slike opplysninger behandles utenfor virkeområdet for et fremtidig direktiv for behandling av personopplysninger i justissektoren, typisk av vektertjenester og arbeidsgivere.

Datatilsynet mener at det et positivt at genetisk data er lagt til listen over sensitive opplysninger.

Retten til å bli glemt (artikkel 17)
Datatilsynet er glad for at man i forslaget til forordning fremhever retten for den enkelte til å slette opplysninger om seg selv. Bestemmelsen gir uttrykk for et viktig prinsipp, ikke minst med tanke på opplysninger som publiseres på Internett. Datatilsynets erfaring er at mange nettbrukere i dag har problemer med å få gehør for ønsket om sletting av personopplysninger når de henvender seg til tjenesteleverandør eller behandlingsansvarlig.

Da Datatilsynet i 2010 og 2011 hadde ansvar for råd- og veiledningstjenesten slettmeg.no, håndterte man nesten 2000 henvendelser fra kvinner og menn i alle aldre som trengte hjelp til å slette egen profil eller konto fra nettet. Det utgjorde 21 prosent av alle henvendelser som denne rådgivningstjenesten fikk om nettkrenkelser disse to årene.

Datatilsynet mener man bør fjerne 17(3)(d). Denne bestemmelsen er unødvendig så lenge artikkel 21 gir så vide unntak som den gjør.

Dataportabilitet (artikkel 18)
Datatilsynet synes forslaget om å gi borgeren rett til å flytte egne personopplysninger fra en behandlingsansvarlig til en annen, såkalt dataportabilitet, er et godt forslag. Prinsippet vil blant annet kunne stimulere til økt konkurranse i et marked hvor det håndteres store mengder personopplysninger, hvilket anses å være positivt i seg selv. Dataportabilitet kan vise seg å bli like viktig for konkurransen blant tjenesteleverandører på Internett som nummerportabilitet var for konkurransen i telemarkedet for over ti år siden. Da Norge innførte nummerportabilitet 1. november 2001 fikk kundene mulighet til å bytte mobilselskap og samtidig beholde nummeret sitt. Ved utgangen av 2002 hadde nærmere 270 000 personer skiftet mobilabonnement og samtidig beholdt nummeret sitt.

Innebygget personvern (artikkel 23)
Datatilsynet er glad for at man fremhever innebygget personvern (”privacy by design”) i forordningsforslaget (artikkel 23). I forslaget forpliktes den behandlingsansvarlige til å iverksette tekniske så vel som organisatoriske tiltak for å sikre et godt beskyttelsesnivå, også før behandlingen finner sted. For å heve statusen til innebygget personvern, er Datatilsynet fornøyd med at manglende etterlevelse av bestemmelsene i denne artikkelen kan føre til det høyeste nivået av økonomiske sanksjoner, slik det er foreslått i artikkel 79 (6) (e).

Selv om den behandlingsansvarlige har ansvar for å velge aktører som følger personvernregelverket, mener Datatilsynet at det burde kommet frem i artikkel 23 at databehandlere, utviklere og leverandører har et selvstendig ansvar for å følge prinsippet om innebygget personvern.

Datatilsynet støtter også forslaget om at standardinnstillinger skal ligge på det mest personvernvennlige nivået (”privacy by default”), og at opplysninger som utgangspunkt ikke skal tilgjengeliggjøres for et ukjent stort publikum (artikkel 23).

Felles behandlingsansvarlig (artikkel 24)
Datatilsynet mener det er positivt at man synliggjør muligheten for å være felles behandlingsansvarlig (”joint controller”), og at man tydeliggjør et krav om at ansvarsfordelingen må reflekteres i en avtale mellom disse.

Tilsynet mener at man burde ha slått fast at prinsippet om solidarisk ansvar gjelder i situasjoner hvor ansvarsfordelingen allikevel ikke er klargjort.

Dokumentasjonskrav (artikkel 28)
Gjeldende meldeplikt erstattes med et krav overfor behandlingsansvarlige og databehandlere om å dokumentere behandlinger som de er ansvarlig for. Dokumentasjonen skal gjøres tilgjengelig for personvernmyndighetene ved forespørsel. Datatilsynet mener dagens meldepliktsystem ikke fungerer tilfredsstillende, og en vridning fra å melde fra til å dokumentere er derfor noe vi ser positivt på.

Datatilsynet mener imidlertid at det ikke bør gjøres unntak for små- og mellomstore bedrifter. Dersom byrden ved dokumentasjonskravet blir for stort for andre enn de aller største virksomhetene, bør man heller justere dokumentasjonskravet slik at det kan gjelde for alle. Dersom dette skal fungere i praksis må det ikke være tvil om bestemmelsens innhold og anvendelse.

Databrudd (artikkel 31 og 32)
Databrudd utgjør en alvorlig trussel for personvernet, og det er trolig langt flere tilfeller av databrudd enn det som kommer frem i offentlighetens lys. Datatilsynet er derfor glad for at den behandlingsansvarlige pålegges en generell plikt til å varsle personvernmyndighetene om databrudd innen 24 timer (artikkel 31), og ved visse tilfeller også å varsle den registrerte (artikkel 32).

Datatilsynet mener det bør utredes hvorvidt plikten til å informere de registrerte bør fastsettes av tilsynsmyndigheten i hvert enkelt tilfelle, slik at tilsynet kan foreta en konkret forholdsmessighetsvurdering.

Konsekvensutredning (artikkel 33)
Behandlingsansvarlig pålegges å gjennomføre en konsekvensutredning forut for behandlinger som representerer en viss risiko. Dette er en ny bestemmelse som Datatilsynet støtter.

Tilsynet tror at slike konsekvensutredninger vil kunne føre til et økt bevissthet rundt innebygget personvern. Datatilsynet er imidlertid ikke enig i at offentlige myndigheter ikke skal pålegges konsekvensutredning, slik man kan få inntrykk av i artikkel 33 (5). Tilsynet er heller ikke enig i åpningen som gis i artikkel 33 (6) om unntak for små og mellomstore bedrifter. Det bør være behandlingens karakter som avgjør om en slik konsekvensutredning er nødvendig, ikke om den behandlingsansvarlige har flere eller færre enn 250 ansatte.

Personvernombud (artikkel 35-37)
Et nytt element i den foreslåtte forordningen er kravet om at offentlige myndigheter og private virksomheter med mer enn 250 ansatte skal utnevne et personvernombud (artikkel 35-37). Ombudet skal, foruten å informere og rådgi den behandlingsansvarlige eller databehandler, også følge med på den interne etterlevelsen av personvernregelverket.

Datatilsynet har gjennom flere år erfart hvilke positivt kraft dedikerte personvernombud kan spille, og er derfor positiv til å gjøre personvernordningen obligatorisk.

Samarbeid og konsistens (artikkel 55-62)
Datatilsynet støtter fullt ut intensjonen om å få på plass et system for økt samarbeid mellom personvernmyndighetene i Europa, og som kan gi en enklere og mer harmonisk regulatorisk praksis.

Tilsynet vil likevel advare mot en utvikling hvor unødvendig mange avgjørelser opp på et felleseuropeisk nivå gjennom den såkalte konsistensmekanismen (”the consistency

mechanism"). I henholdsvis artikkel 58 (3) og 58 (4) åpnes det for at nasjonale personvernmyndigheter og EU-kommisjonen kan kreve at enhver sak blir håndtert i henhold til en konsistensmekanisme. Dersom det ikke trekkes noen grenser for hvilke saker og problemstillinger som kan løftes opp på et europeisk nivå, frykter Datatilsynet at denne mekanismen vil bli overbelastet og dermed ineffektiv.

Datatilsynet er også kritisk til konsistensmekanismens foreslåtte struktur. Slik det legges opp til i forordningsutkastet, gis kommisjonen kompetanse til å uttale seg om enkeltsaker av felleseuropeisk betydning (artikkel 59), gjøre vedtak om utsettelse i slike saker (artikkel 60) og overstyre nasjonale personvernmyndigheter i enkeltsaker ved å vedta implementerende rettsakter (artikkel 62).

Datatilsynet mener kommisjonen har bevilget seg alt for vide fullmakter. Særlig betenkelig er kommisjonens mulighet til å overstyre nasjonale personvernmyndigheter i enkeltsaker. Dette mener Datatilsynet går utover personvernmyndighetenes uavhengighet (jf artikkel 47), og er særlig problematisk for Norge som ikke er et medlemsland.

European Data Protection Board (EDPB) (artikkel 64-72)
Datatilsynet mener kommisjonens forslag om å erstatte Artikkel 29-gruppen med European Data Protection Board (EDPB) – et europeisk organ hvor alle de nasjonale tilsynsmyndighetene er representert – er et riktig grep for å sikre en harmonisert regulatorisk praksis i Europa.

Slik ordlyden i forslaget lyder er det bare tilsynsmyndighetene i medlemslandene som skal være representert i dette organet. Selv om Datatilsynet forutsetter at også norske personvernmyndigheter skal representeres med fulle rettigheter i EDPB, ber vi departementet om snarest å avklare dette.

Administrative sanksjoner (artikkel 79)
Datatilsynet har siden 2009 hatt mulighet til å fastsette overtredelsesgebyr og tvangsmulkt. Dette har vist seg å være et helt nødvendig supplement til vedtakskompetansen, og forslaget i artikkel 79 støttes derfor av tilsynet.

Delegering og implementering (artikkel 86-87)
Forordningsutkastet gir kommisjonen kompetanse til å utarbeide delegerende og/eller implementerende rettsakter (forskriftskompetanse) på en rekke punkter[2].

Datatilsynet stiller spørsmål ved om man her egentlig nøyer seg med å avgi forskriftskompetanse på ikke-essensielle deler av innholdet, slik Artikkel 290 i Traktaten om Den europeiske unions funksjonsmåte (EUF-traktaten) krever.

[2] Artikkel 6, 8, 9, 12, 14, 15, 17, 18, 20, 22, 23, 26, 28, 30, 31, 32, 33, 34, 35, 37, 38, 39, 41, 43, 44, 55, 58, 59, 60, 61, 79, 81, 82, 83

Blant annet legges det i forordningsutkastet opp til delegerende rettsakter i artikkel 6(5) om sektorspesifikke kriterier for avveining mellom interessene til behandlingsansvarlig og den registrerte. Dette berører et av de vanligste behandlingsgrunnlagene, og innholdet i en slik delegert rettsakt vil ha stor betydning for det materielle innholdet i forordningen.

Når det gjelder utformingen av delegerende eller implementerende rettsakter, mener Datatilsynet at også EFTA-landene bør gis formell mulighet til å uttale seg om innholdet i disse før de vedtas. EU-landene har denne påvirkningsmuligheten via Europaparlamentet og Rådet. En oppfordring om å høre EFTA-landene om innholdet i kommisjonens forskriftsforslag kunne for eksempel bli lagt inn i fortalens punkt 130.

Med vennlig hilsen

Bjørn Erik Thon
Direktør

Cecilie L B Rønnevik
seniorrådgiver

Kopi: Fornyings-, administrasjons- og kirkedepartementet,
v/Statsforvaltningsavdelingen,
Pb 8004 Dep, 0030 Oslo