

Justisdepartementet,
Lovavdelingen,
Postboks 8005 Dep,
0030 Oslo.

lovavdelingen@jd.dep.no



Saksbehandler:	Vår dato:	Vår referanse:	Deres dato:	Deres referanse:
TN	26.07.2012	12/2060	19.04.2012	201201634 ES LLE/AHI/mk

Høring - EU-kommisjonens forslag til nye personvernregler.

Vi viser til brev fra Justis- og beredskapsdepartementet av 19. april 2012. Forbrukerrådet har valgt å gi en utførlig gjennomgang av enkelte av forordningens forslag, all den tid EU-Kommisjonens forslag kommer i form av en forordning og ikke et direktiv.

Forbrukerrådet ønsker også å klargjøre at vårt svar er i overensstemmelse med den Europeisk forbrukerorganisasjonen BEUCs¹ respons til EU-kommisjonen, og at deler av vårt hørings svar er basert på tidlige utkast av BEUC sitt hørings svar.

KAPITTEL I - Alminnelige bestemmelser

Artikkel 2 – Saklig virkeområde

Artikkel 2 i forslaget definerer den saklige rekkevidden av reguleringen på samme vilkår som direktiv 95/46: behandling av personopplysninger gjennom helt eller delvis automatiserte metoder eller til behandling av ikke-automatiske hjelp av personopplysninger som inngår, eller er ment å danne en del av et register.

Unntakene fra det generelle virkeområdet i forslaget er i midlertidig utvidet i forhold til dagens direktiv. Forbrukerrådet er ikke uenige i unntakene, men mener at de bør defineres klarere.

Når det gjelder unntaket relatert til "nasjonal sikkerhet", ønsker vi å peke på at det vil kunne være nasjonale forskjeller i forståelsen av begrepet, noe som vil undergrave en ensartet anvendelse. Vi mener derfor at forordningen bør vise til egne kriterier som bedre definerer omfanget av unntaket til nasjonal sikkerhet.

Når det gjelder unntak for "personal and household activities", støtter vi næringsvirksomhet som det viktigste kriterium for anvendelsen av unntaket. Spørsmålet er spesielt viktig innenfor en teknologisk kontekst der enkeltpersoner f. eks publiserer gjennom nettsamfunn, blogger, nettsteder osv.

¹ www.beuc.org

Utkastet avklarer imidlertid ikke anvendelsen av unntaket i de tilfeller data blir gjort tilgjengelig for et ubestemt antall individer. Ifølge rettspraksis fra EU-domstolen², bør unntak bare gjelde når dataene er gjort tilgjengelig for et begrenset antall individer. Vi vil derfor foreslå at unntaket fra artikkel 2.2.d suppleres med et kriterium om ubestemt antall personer, og med det klargjøre at et ubestemt antall kontakter i prinsippet betyr at unntaket ikke lenger kommer til anvendelse.

Artikkel 3 – Geografisk virkeområde

Artikkel 3 omhandler det geografiske virkeområdet for forslaget, og adresserer tilfellene der behandlingsansvarlige er etablert innenfor og utenfor EU.

Artikkel 3.1 introduserer et etableringskriterium i EU for å avgjøre om forordningen kommer til anvendelse. Samtidig anser vi at definisjonen av etableringen som stedet der de viktigste beslutningene blir tatt i relasjon til de formål, forutsetninger og metoder for databehandlingen (artikkel 4.13), ikke nødvendigvis er egnet for foretak med en desentralisert beslutningsstruktur.

Videre angir artikkel 3.1 kun anvendelsen av EU-retten, uten kriterier for å avgjøre hvilken nasjonal lov som skal gjelde. Dette er i prinsippet logisk all den tid forordningen er ment å være et selvstendig instrument. Det er likevel slik at forordningen åpner for anvendelsen av nasjonal lovgivning i enkelte bestemmelser, og landene opprettholder dermed friheten til å vedta spesifikk lovgivning på et begrenset antall områder. Forordningsutkastet angir kun kriterier for å definere den ledende Data Protection Authority (artikkel 51) der flere medlemsstater kan være relevante, men løser ikke spørsmålet om nasjonal lov.

Artikkel 3.2 viser til tilfeller hvor behandlingsansvarlige ikke er etablert i EU, men prosesseringen er knyttet til tilbud av varer og tjenester til registrerte personer bosatt i EU, eller som får sine handlinger registrert. Sammenlignet med artikkel 3 i gjeldende direktiv, fjerner den nye bestemmelsen kriteriet "bruk av utstyr".

Selv om Forbrukerrådet ønsker de nye vilkårene velkommen, ber vi om en avklaring/presisering som sikrer at begrepet varer og tjenester også omfatter "gratis tjenester", der ikke den registrerte bærer noen direkte økonomisk kostnad³.

Artikkel 4 - Definisjoner

Artikkel 4.1-Definisjon av "data" (personlige data)

Sammenlignet med dagens direktiv, overføres definisjonen av "personopplysninger" til definisjonen av "data". Forbrukerrådet er fornøyd med at de viktigste elementene i definisjonene videreføres. Forbrukerrådet anser at den vide definisjonen i forslaget tar høyde for fortsatt rask teknologisk utvikling i relasjon til personvernsutfordringer.

Forbrukerrådet ønsker spesielt velkommen at det nye forslaget utvider definisjonen ved å inkludere begrepene "online identifiere" og lokaliseringsdata. Det er et sterkt behov for å dekke og adressere mulighetene for å identifisere, spore og lage profiler av mennesker i nettbaserte økosystemer. Dette vil også kunne avklare usikkerheten rundt IP-adressers rettslige status. Den

² See ECJ 6 November 2003, Lindquist and Satamedia, C-101/0

³ Opinion 01/2012 on the data protection reform proposals by Article 29 Data Protection Working Party

europæiske domstolen har nylig tatt til ordet for at IP-adresser skal anses som personopplysninger; "*because they allow those users to be precisely identified*"⁴.

Undertiden synes den foreslåtte definisjonen å stå i kontrast med den siste setningen i recital 24⁵. Denne setningen undergraver formålet i den nye definisjonen, som skal være å dekke enhver opplysning eller middel som åpner for identifisering av en registrert. Er informasjonen egnet for den behandlingsansvarlige til å identifisere en enkeltperson, bør informasjonen anses som personopplysninger. Forbrukerrådet mener derfor at siste setning i recital 24 må slettes, alternativt skrives om slik at det så snart det er en nær nok relasjon mellom det identifiserbare og et individ, vil det medføre at inneværende regler kommer til anvendelse.

Artikkel 4.8-Registrertes samtykke

Utkastet etablerer et enkelt regime for at samtykke kan benyttes som et mulig rettslig grunnlag for databehandling, hva gjelder både personlige og sensitive personopplysninger. Artikkel 4.8 krever at samtykket skal være frivillig, spesifikt, informert og uttrykkelig, mens artikkel 7 fastsetter en rekke vilkår for samtykket, herunder å legge bevisbyrden på den behandlingsansvarlige for å godtgjøre at vilkårene er oppfylt.

Forbrukerrådet bifaller presiseringen i recital 25 om at samtykke kan gis på hensiktsmessig måte. Dette åpner for en viss grad av fleksibilitet, samt bestemmelsen om at anmodningen om å gi samtykke i en onlinesituasjon ikke bør være unødvendig forstyrrende for bruk av tjenesten.

Forbrukerrådet erkjenner at det ikke nødvendigvis finnes noen "one size fits all" løsning på spørsmålet om samtykke, men anser samtidig at bestemmelsene om samtykke fra forbrukere må være fleksible og brukervennlige. Vi mener at praksis fremover bør vurderes opp mot følgende to kriterier:

- En analyse av skadepotensialet for forbrukeren knyttet til en bestemt praksis/fremgangsmåte.
- En evaluering av om en praksis/fremgangsmåte oppfyller 'rimelige forventninger' av bruk av informasjonen vurdert fra en
 - o gjennomsnittlig eller typisk forbruker, eller
 - o et gjennomsnittlig medlem av en gruppe
 når praksisen/fremgangsmåten er rettet mot en bestemt gruppe forbrukere.

Forbrukerrådet vil derfor rette fokuset mot at kravet om samtykke må være meningsfullt, samtidig som det må fremgå tydelig at samtykke kun er ett av flere mulige juridiske grunnlag, og ikke nødvendigvis det mest passende i alle situasjoner. For eksempel kan samtykke ikke være gyldig grunnlag dersom vilkårene om åpenhet og informasjon ikke er oppfylt, eller når den registrerte ikke har et reelt valg, men befinner seg i en "take it or leave it" situasjon.

Artikkel 4.13- Main establishment

"Main establishment" er definert som det stedet der en virksomhets viktigste beslutninger knyttet til formål, betingelser og metoder for behandling tas. Denne definisjonen fremstår som mindre egnet for foretak med desentralisert struktur, der f. eks. sentraladministrasjonen og forvaltningsadministrasjonen av databehandlingen er forskjellig steder.

⁴ ECJ c- 70/10 Scarlet v. SABAM.

⁵ Recital 24: "...identification numbers, location data, on line identifiers...need not necessarily be considered as personal data in all circumstances".

I slike tilfeller vil "main establishment" etter reguleringen avgjøres av hva konsernet anser er "main", alternativt den "avdelingen" som utøver makt over andre.

Artikkel 4.20 (ny) - Overføring av personopplysninger

Forbrukerrådet etterlyser en definisjon av hva som anses som en overføring av personopplysninger. The European Court of Justice har avklart at

*"there is no 'transfer [of data] to a third country' where an individual in a Member State loads personal data onto an internet page which is stored on an internet site on which the page can be consulted and which is hosted by a natural or legal person who is established in that State or in another Member State, thereby making those data accessible to anyone who connects to the internet, including people in a third country"*⁶.

Selv om dette ville bety at publisering/opplasting av materiale på et nettsted ikke er en internasjonal overføring, gjenstår spørsmålet for andre typer utvekslinger på nettverk, som for eksempel selskapsservere.

KAPITTEL II - Prinsipper og lovligheten for bearbeiding

Kapittel II omhandler prinsippene for databehandling og stiller konkrete krav til innsamling og prosessering av data relatert til mindreårige og av sensitive data. Forbrukerrådet er positive til at de generelle prinsippene for databearbeiding er opprettholdt i forslaget, samtidig som betydelige forbedringer er foreslått, særlig i relasjon til prinsippet om åpenhet (transparency).

Artikkel 5 - Prinsipper for behandling av personopplysninger

Forbrukerrådet ønsker velkommen innføring av **prinsippet om åpenhet** i forhold til innsamling og prosessering av data. Innføringen innebærer en styrking av de forpliktelser som den behandlingsansvarlige har til å gi de som er registrert (artikkel 14 i forslaget) relevant informasjonen om databehandlingen. Dette gjelder eksempelvis kontaktdetaljene til kontrolleren, formålet med behandling, oppbevaringsperiode og eksistensen av rettigheter og nærmere regler for å utøve dem, jf. artikkel 14. Mangel på åpenhet og informasjon kan virke sterkt avskrekkende for brukere, og der de ikke vet hvordan deres data blir brukt, til hvilket formål og av hvem, vil de vanskelig være i stand til å utøve og håndheve sine rettigheter.

Forslaget styrker også prinsippet om **dataminimalisering** ved å gi prinsippet større synlighet i et nytt avsnitt (e). Styrkingen av dette prinsippet er helt nødvendig for å møte dagens realiteter som f. eks. datahøsting og "data mining", som blant annet kan benyttes til profilering av forbrukere. Disse modellene involverer store mengder personlige data, og det er grunn til å tro at den behandlingsansvarlige av og til beholder data utover tiden som er nødvendig for å utføre tjenesten. Hva søkemotorer angår, har The article 29 Working Party⁷ helt konkret krevd av slike tjenester:

"to delete or irreversibly anonymise personal data once they no longer serve the specified and legitimate purpose they were collected for and be capable of justifying retention and the longevity of cookies deployed at all times".

⁶ ECJ 6 November 2003 Lindqvist C-101/01.

⁷ Article 29 Working Party opinion 1/2008 on search engines (April 2008).

Prinsippet om dataminimalisering speiler etter vår mening også de nye prinsippene for innebygget personvern (privacy by design) og personvern som standard ligger på høyeste beskyttelsesnivå (privacy by default), som skal være forankret i personvernsensitive teknologier og tjenester helt fra oppstarten.

Prinsippet om **formålsbegrensning av databehandling** er av stor betydning når det kommer til utbredelsen av forretningsmodeller grunnet på datadeling med tredjeparter. Forretningsmodellene som mange internettelskaper (som for eksempel enkelte søkemotorer og nettsamfunn) er tuftet på, kan være uforenlig med prinsippet om formålsbegrensning og spesifisering av bruken av personopplysninger. Det er tilsynelatende flere selskaper som samler inn personopplysninger og/eller overfører data til tredjeparter, som igjen behandler dataene med andre formål enn for den opprinnelige databehandlingsansvarliges formål.

Forbrukerrådet beklager at prinsippet om formålsbegrensning svekkes gjennom det faktum at det ikke finnes noen definisjon av hva som anses for uforenlig bruk ("incompatible use"). Videre har kriteriene for "kompatibel bruk" (ingen spesifisering av hva som er kompatibel eller inkompatibel), ført til divergerende forståelse på nasjonalt nivå. Forbrukerrådet mener derfor at den nye forordningen bør inneholde kriterier for hva som regnes som "kompatibel bruk" på bakgrunn av beste praksis for hvordan "kompatibilitet" har blitt tolket på nasjonalt nivå⁸.

Videre åpner artikkel 6.4 for at formålsbegrensningsprinsippet kan innskrenkes i visse tilfeller når videre behandling ikke er kompatibel med det opprinnelige formålet med behandlingen, men kan forsvares av andre rettsgrunnlag. Dette tillegget svekker etter vårt syn autonomien som ligger i prinsippet. Vi er særlig bekymret for utvanning av prinsippet der behandlingen er basert på en kontrakt (artikkel 6.1 (b)). Det er en kjensgjerning at forbrukerne har liten eller ingen anledning til å forhandle om innholdet av avtalene. Vi mener derfor at artikkel 6.4 bør slettes. Den samme bekymringen gjør seg gjeldende når unntak er basert på "offentlig interesse", ref litra e. Dette begrepet kan variere fra land til land, og uten videre forklaring risikerer man en divergerende oppfatning av regelen fra land til land.

Artikkel 6 - lovligheten av behandling

Artikkel 6 i forslaget gjengir stort sett grunnlag for samme behandling som dagens direktiv er bygget på. Behandling av personopplysninger er lovlig når minst ett av følgende gjelder:

- a) the data subject has given its consent to the processing,
- b) processing is necessary for the performance of a contract,
- c) processing is necessary for compliance with a legal obligation,
- d) processing is necessary to protect the vital interests of the data subject,
- e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of a public authority vested on the controller,
- f) processing is necessary for the purposes of the legitimate interest of the data controller unless such interest contrast with the fundamental rights and freedoms of the data subject.

Sammenlignet med eksisterende direktiv inneholder forslaget noen få, men svært viktig nyheter. De mest velkomne endringer finner vi i definisjonen og betingelsene for "samtykke" (artikkel 7), samt bestemmelsen om behandling av personopplysninger av barn (artikkel 8).

⁸ The Article 29 Working Party har annonsert at de vil ta opp disse spørsmålene i sine fremtidige handlingsplaner.

Når behandlingen enten er basert på den behandlingsansvarliges juridiske forpliktelse eller på offentlighetens interesse, vil grunnlaget for behandlingen enten måtte gis i EU-retten eller i nasjonal lovgivning i en medlemsstat (artikkel 6.3). Denne bestemmelsen er svært viktig all den tid den utelukker lovgivningen i et ikke-EU land som rettslige grunnlag for behandlingen.

Artikkel 7 - Betingelser for samtykke

Forskriftsutkastet etablerer et enkelt regime for at samtykke kan benyttes som grunnlag for behandlingen av både sensitive og ikke-sensitive personopplysninger. Artikkel 7 fastsetter en rekke vilkår for samtykke, herunder databehandlerens bevisbyrde om at vilkårene for samtykket som grunnlag er oppfylt.

Forbrukerrådet viser til kommentarene til recital 25 i avsnittet ovenfor. Forbrukerrådet er tilfreds med at artikkel 7 legger bevisbyrden for samtykke på behandlingsansvarlige. Behandlingsansvarlige har dermed en oppfordring til å være særlig oppmerksom på påliteligheten av de verktøyene som benyttes til å innhente samtykke fra den registrerte i samsvar med recital 25.

Forbrukerrådet ønsker også å peke på at den foreslåtte retten til når som helst å trekke tilbake eget samtykke fremstår som et bedre og mer anvendelig verktøy enn retten til å protestere, som er å finne i gjeldende direktiv.

For at samtykket skal være gyldig som rettslig grunnlag, må vilkårene om at samtykket er informert, spesifikt og fritt avgitt være oppfylt. Utkastet gir eksempler på tilfeller hvor samtykke må anses ugyldig på grunn av manglende balanse mellom partene, for eksempel i arbeidslivet. Når det gjelder "informert" samtykke, bør den registrerte ha blitt presentert for klar og forståelig informasjon om viktige elementer, slik disse er definert i artikkel 14.

Artikkel 8 - Behandling av barns personopplysninger

Forbrukerrådet anser det som fornuftig å kreve foreldrenes samtykke til behandling av personopplysninger for barn under 13 år. Terskelen på 13 år synes i utgangspunktet som hensiktsmessig.

Forbrukerrådet anser at en plikt til å innhente foreldrenes samtykke bør kombineres med en plikt til å implementere mekanismer for aldersbekreftelse. Samtidig mener vi at det ville være en fordel om den foreslåtte reguleringen inneholdt nærmere kriterier og vilkår i tilknytning til foreldresamtykke, og ikke kun delegerer den videre utforming av bestemmelsen til Kommisjonen. All den tid personopplysninger benyttes til markedsføring, er det særlig viktig at bestemmelsene i markedsføringslovens kapittel 4 blir håndhevet.

Artikkel 9 - Behandling av spesielle kategorier av personopplysninger

Forbrukerrådet støtter forslaget om forbud mot innsamling/behandling av sensitive personopplysninger som nevnt i artikkel 9.1. Forbrukerrådet mener imidlertid at også finansielle data bør anses som sensitive personopplysninger når de avsløre personlig betalingsevne⁹.

⁹ En undersøkelse gjennomført av the Office of the Information Commissioner i Storbritannia i 2006, viste at 70.5% av respondentene anså finansielle data som særlig sensitive personopplysninger.

Andre finansielle data som f. eks. ubetalt gjeld til selskapet som den registrerte er, eller har vært i et kontraktsforhold med, vil falle utenfor denne kategorien.

I tillegg, gitt en stadig skiftende teknologisk utvikling, mener vi at forslaget bør inneholde en ikke-uttømmende liste over sensitive personopplysninger.

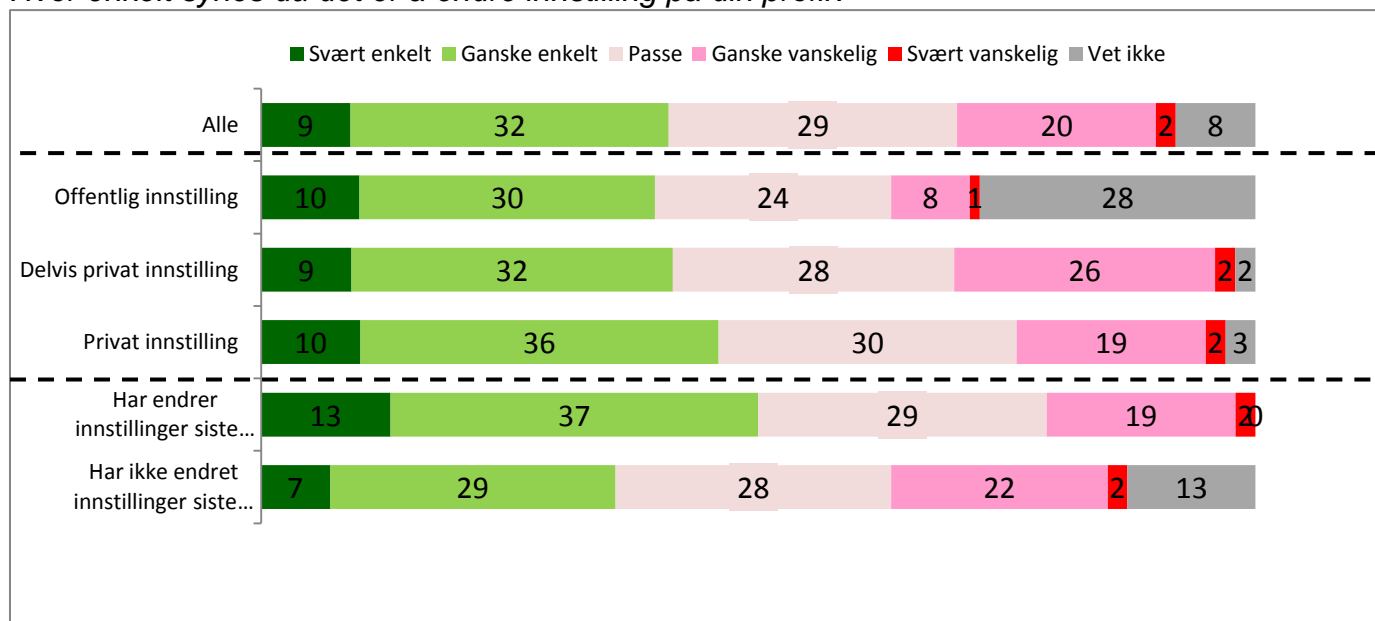
KAPITTEL III - Rettigheter til den registrerte

Artikkel 11 - Transparent informasjon og kommunikasjon

Mangel på åpenhet og mangel på klar og tydelig informasjon har en betydelig avskrekkende effekt for brukere som ønsker å håndheve sine rettigheter. Forbrukerne forstår sjelden personvernsvilkår, som generelt er utilgjengelig i form og innhold for den gjengse forbruker.

Undersøkelser viser også at på tross av at forbrukere er bekymret for eget personvern, anser de ikke at personvernsvilkår er en egnet måte å formidle vilkårene på, eller til dempe deres bekymringer for eget personvern¹⁰. Disse funnene bekreftes av atferdsøkonomiske teorier som viser at forbrukerne ikke leser personvernsvilkår, og ofte godtar standardinnstillingene. TNS Gallup gjennomført en undersøkelse¹¹ for Forbrukerrådet i februar/mars 2012, og stilte der blant annet følgende spørsmål til de som hadde svart ja til at de hadde en profil på Facebook:

”Hvor enkelt synes du det er å endre innstilling på din profil?”



¹⁰ I følge Eurobarometer mener 64% av brukerne at informasjonen om bruk av deres personlige informasjon ikke er tilfredsstillende. I følge Forbrukerrådets egen undersøkelse utført i forkant av vår klage til datatilsynet mot Facebook og Zynga, svarte hele 73% av brukerne i alderen 15-30 år at de sjeldent leste brukervilkår. Den engelske forbrukerorganisasjonen Which? fant i sin undersøkelse fra mars 2010 at kun 6% av de over 16 år (med internettilgang) hadde lest personvernsregler på nettsteder.

¹¹ Undersøkelsen ble gjennomført online og deltakere ble rekruttert via TNS Gallup sitt internettpanel. Målgruppen var et landsrepresentativt utvalg over 15 år, og alle 1050 intervjuene ble gjennomført i uke 8, 2012.

Som det fremgår av resultatene ovenfor, er det de som har størst problemer med å endre innstillinger, som innehar de mest åpne profilene på Facebook. Denne delen av undersøkelsen vil også være relevant i tilbakemeldingene fra Forbrukerrådet under artikkel 23, som omhandler reguleringen av "Privacy by default".

Forslaget innebærer en betydelig styrking av informasjonskravet fra den behandlingsansvarlige til den registrerte (11 artikler, 12 og 13). Vi ønsker spesielt velkommen det nye kravet om at informasjon skal gis i en forståelig form gjennom bruk av klart og enkelt språk. Vi støtter også regulering av prosedyrene for informasjonsoverføringen til de registrerte, all den tid vi anser at dette vil styrke behandlingsansvarliges ansvar vis-à-vis den registrerte.

Artikkel 12 - Prosedyrer og mekanismer for å utøve rettighetene til den registrerte

Forbrukerrådet støtter også innføring av spesifikke regler for utøvelsen av rettighetene til den registrerte. Behandlingsansvarlige skal svare på den registrertes forespørselen uten ugrunnet opphold og senest innen en måned. Videre bør behandlingsansvarlige ikke kunne ta betalt for å gi en registrert tilgang til egne personopplysninger, så lenge denne rett ikke misbrukes. Når det gjelder retten til å korrigere, fjerne og slette data, bør den alltid være gratis, da det er i alle parter interesse at data er korrekte og oppdaterte.

Artikkel 13 - Rettigheter i forhold til mottakere

Forbrukerrådet støtter innføringen av en plikt for den behandlingsansvarlige til å varsle hver mottaker hvis data har blitt videresendt/overført, i tilfelle retting eller sletting, så lenge dette er mulig uten uforholdsmessig ressursbruk. Bestemmelsen er særlig viktig i digitale miljøer, der informasjon enkelt deles med tredjeparter, og det kan være et særlig behov for å korrigere unøyaktigheter.

Artikkel 14 - Informasjon til den registrerte

Artikkel 14 lister opp all informasjon den behandlingsansvarlige er forpliktet til å gi den registrerte ved innsamling/behandling av dennes personlige data. Bestemmelsen er omfattende, og inneholder det meste av hva som må anses for relevant informasjon den registrerte skal gis. Samtidig savner vi at listen inneholder informasjon om hvilken type personopplysninger som samles inn og behandles, og foreslår at listen utvides tilsvarende.

Vi støtter også den nye plikten behandlingsansvarlige har til å informere den registrerte om retten til å klage til tilsynsmyndigheten og til å oppgi relevant kontaktinformasjon. Bestemmelsen underbygger på en god måte den registrertes rett til å rette direkte klage til tilsynsmyndigheten, slik denne er formulert i artikkel 15.1 (f).

Når det gjelder unntak fra krav til informasjon nevnt i artikkel 14.5, mener vi at unntaket i artikkel 14.5 b) (når informasjon til de registrerte personene viser seg umulig eller bærer en uforholdsmessig stor anstrengelse) bør defineres bedre i reguleringen, heller enn å la Kommisjonen vedta spesifiserte slikt unntak.

Det er viktig å informere den registrerte om innsamlingen av personopplysninger er obligatorisk eller frivillig. I tilfeller der den registrerte velger ikke å oppgi personlige data, bør han ikke nektes adgang til en bestemt tjeneste, slik tilfellet er for de fleste online-tjenester, hvor forretningsmodell

er basert på innsamling av data i bytte mot såkalte "gratis tjenester". Tvert imot bør tilgangen til tjenesten være gjenstand for ulike betingelser.

Vi støtter forslaget henvisning til en standardisering av måten informasjonen gis til den registrerte. Vi anser det likevel som formålstjenelig om dette settes som en forutsetning, heller enn et frivillig alternativ. Standardiserte informasjonsformater gir erfaringsmessig bedre og mer strukturert informasjon til forbruker. Vi mener også at det nye European Data Protection Board (EDPB) bør ta ledelsen i å utvikle slike standardiserte personvernerklæringer med deltakelse fra både forbrukerorganisasjoner og næringsinteresser.

Avslutningsvis mener vi at den behandlingsansvarliges mulighet til å presentere informasjonen ved hjelp av lagdelt oppsett (multilayered) bør uttrykkelig tillates.

Artikkel 15 - Rett til innsyn for den registrerte

Artikkel 15 inneholder en liste over opplysningsplikter knyttet til den registrertes tilgangsrett til informasjon. I forhold til gjeldende direktivet, er tillegg av plikten til å informere om retten til å klage til tilsynsmyndigheten (15.1 (f)) avgjørende, og dermed særlig velkommen.

Artikkel 17 - Rett til å bli glemt og til å bli slettet

Forbrukerrådet støtter innføring av retten til å bli glemt (artikkel 17 i forslaget). Denne retten styrker den eksisterende retten til å slette egne data i tilfelle dataene ikke lenger er nødvendige for spesifikke formål, eller når den registrerte har trukket sitt samtykke. Den enkeltes digitale fotavtrykk kan bli mange og omfattende, og en rett til å begrense disse, er på sin plass. Som nevnt er rett til sletting allerede inkludert i gjeldende direktivet, men bestemmelsen er lite anvendt online. Ulike studier og undersøkelser understreker hvilke utfordringer enkeltpersoner har ved utøvelsen av denne retten i dag¹².

Forbrukerrådet ser samtidig at en for utstrakt og ubetinget rett til å bli glemt kan være inkompatibel med f. eks. yttringsfriheten. Samtidig er det viktig å påse at ikke gjennomføring og håndheving av bestemmelsen medfører tekniske tiltak som resulterer i filtrering av online kommunikasjon. Forbrukerrådet oppfordrer sterkt til at bestemmelsene om ansvarsfrihet for tjenesteleverandører i e-handelsdirektivet vurderes nøye i det videre arbeidet med reguleringen. For Forbrukerrådet er de nevnte bestemmelsene i e-handelsdirektivet en viktig bestanddel for å nå mål om nøytral og ubehandlet informasjonsflyt.

Artikkel 17.2 bør dermed klargjøre at den behandlingsansvarliges ansvar vurderes ut fra tiltak, og ikke nødvendigvis resultat. I noen tilfeller vil det være umulig å informere alle parter der data er distribuert og/eller å spore opp alle mulige lenker og kopier.

¹² Som et eksempel viser vi til undersøkelsen som ble publisert av den franske forbrukerorganisasjonen UFC Que choisir i 2009, som viser at majoriteten av internettsselskapene er tilbakeholdne med å trekke tilbake personopplysninger de sitter på. Samtidig viser Forbrukerrådets egen undersøkelse om sosiale medier fra (Sintef, 2009) at brukere av sosiale medier har få, om noen mulighet til å håndheve egne rettigheter når det gjelder endring/sletting av egne data når de første er delt med tredjeparter.

Artikkel 18 - Rett til dataportabilitet

Forbrukerrådet bifaller sterkt forslaget i forordningen om å innføre en rett til dataportabilitet.

Gjennom bruk av heldigitale internettjenester, produserer og lagrer forbrukere enorme mengder informasjon. Det er Forbrukerrådets erfaring at alt for mange av disse tjenestene per i dag låser forbrukerne til tjenester og plattformer, blant annet gjennom å vanskeliggjøre/ikke legge til rette for flytting av data, eksempelvis til konkurrerende tjenester.

En slik situasjon er uforenlig med en brukers rett til å ha kontroll over egne data, samtidig som det hindrer konkurranse blant tjenesteleverandører. Gjennom å innføre en rett til dataportabilitet legger man til rette for at forbrukeren beholder eierskapet til, og har kontroll over egne data. Dermed legges det også til rette for at markedsaktørene er i bedre stand til å utnytte konkurransemekanismene i markedet, noe som f. eks. var tilfellet med nummerportabilitet i telemarkedet.

Forholdet mellom retten til dataportabilitet og retten til sletting bør klargjøres i forslaget. Etter vår mening må en rett til dataportabilitet innebærer en krav om umiddelbar og uoppfordret sletting av data hos den opprinnelige tjenesteleverandøren. Bruken av ordet "kopi" i artikkel 18.1 synes å innebære at den opprinnelige tjenesteleverandøren kan beholde data. Uansett vil den behandlingsansvarlige ha plikt til å slette dataene etter artikkelartikkel 5 e.

Artikkelen 18.2 kan forstås slik at den begrenser omfanget av portabilitet til data som har blitt publisert av den registrerte på grunnlag av samtykke eller av kontrakt. Etter vår mening bør denne retten også gjelde i de tilfeller der dataene er samlet inn på andre grunnlag, all den tid formålet for innsamling/behandling ikke lenger eksisterer.

Forbrukerrådet ønsker avslutningsvis å peke på at en effektiv implementering av en rett til dataportabilitet nødvendiggjør tilgang til interoperable, eller kompatible standarder som kanskje ikke finnes i dag, og som derfor må utvikles.

Artikkel 19 - Rett til å protestere

Artikkel 19 i forslaget etablerer en rett for den registrerte til å protestere over behandling av egne data som er samlet inn på visse grunnlag, med mindre den behandlingsansvarlige kan vise til klare, legitime grunner for behandlingen. Dette medfører en betydelig forbedring fra dagens situasjon, der den registrerte kun har en rett til å motsette seg behandling hvor han/hun kan vise til konkret skade. Ifølge artikkel 19 vil den registrerte i utgangspunktet ha rett til å motsette seg behandling og det vil være opp til den behandlingsansvarlige å anskueliggjøre både at innvendingen ikke er gyldig og at behandling er lovmessig.

Bestemmelsen klargjør dessverre ikke konsekvensene av nevnte rett i forhold til de angjeldende data, og Forbrukerrådet mener bestemmelsen bør klargjøre at dersom retten til å protestere stadfestes, bør behandlingsansvarlige forpliktes til umiddelbart å slette relevante data.

Begrepet "compelling legitimate grounds" som på tross av innvendingen skal kunne legitimere videre behandlingen av personopplysningene, bør utvikles og presiseres mer i reguleringen.

Artikkel 20 - Tiltak basert på profilering

Artikkel 20 tar for seg behandling av personopplysninger der formålet er å profilere enkeltpersoner i henhold til deres personlige preferanser og adferd¹³. Vi ser en stadig fremvekst av forretningsmodeller der profilering av enkeltpersoner er sentralt, og forbrukerne er ofte verken klar over hvilken praksis de er utsatt for, eller hvilke konsekvenser de kan ha. Per i dag har forbrukere liten kontroll over de mange, komplekse media -, og markedsføringsøkosystemer¹⁴.

Det er viktig å understreke at Forbrukerrådet både erkjenner og anerkjenner nye og innovative forretningsmodeller. Dette utgangspunktet forutsetter imidlertid at forbrukerne er oppmerksomme på teknologier og andre tiltak som benyttes i reklamebaserte forretningsmodeller. Forbrukerrådet slutter seg etter dette til forslaget om å inkludere profileringspraksiser i reguleringen. Vi registrerer at utkastet ikke forbyr profilering i seg selv, men tilgodeser en rett til å motsette seg profilering når denne er skadelig. For å sikre den enkeltes rettsikkerhet, må det avklares hvordan begrepene “legal effects” og “significantly affects” skal forstås.

Artikkel 21 - Begrensninger

Artikkel 21 i forslaget introduserer en rekke mulige restriksjoner til de registrertes rettigheter. Vi merker oss at denne artikkelen er mer omfattende enn den tilsvarende artikkel i dagens direktiv (artikkel 13). I motsetning til gjeldende direktiv, kan den nye artikkelen 21 brukes til å begrense nesten alle rettighetene til den registrerte (herunder prinsipper for behandling, retten til å protestere, tiltak basert på profilering og rett til å bli varslet om datainnbrudd).

Vi anser at artikkel 21 bør formuleres mer presist når det gjelder formål, proporsjonalitet og nødvendighet av behandlingen, hvilke kategorier av data som innhentes og hvilke personer som er autorisert til å behandle dataene.

KAPITTEL IV - behandlingsansvarlige og databehandler

Artikkel 22 – Behandlingsansvarliges ansvar

Reguleringsutkastet introduserer ansvarlighetsprinsippet, hvor den behandlingsansvarlige må etablere tiltak og kontrollsystemer som sikrer etterlevelse, og som gir eksterne interessenter, inkludert tilsynsmyndighetene, grunnlag for å etterprøve etterlevelsen.

Artikkel 22 introduserer en generell plikt for den behandlingsansvarlige til riktig implementering og etterlevelse av bestemmelsene i kapittel IV, inkludert innføring av en såkalt “Data Protection Impact Assessment”, oppnevning av en “Data Protection Officer”, samt gjennomføring av databeskyttelse både ved design og som standard.

Forbrukerrådet støtter de foreslåtte tiltakene, som fremstår som godt egnet til både å forbedre behandlingsansvarliges ansvar og til å legge til rette for at personvern blir en naturlig del av bedriftskulturen. Slik reguleringen er utformet på dette punktet, anser Forbrukerrådet at den er godt egnet til å gi en høy grad av fleksibilitet for bedriftene. Dette er avgjørende for regulering av et område preget av rask, teknologisk utvikling.

¹³ Såkalte “Behavioural targeting techniques” omfatter f. eks. neuromarketing, interaktiv video , målretting gjennom sosiale nettverk, “retargeting” og lokasjonsbasert målretting for mobile enheter.

¹⁴ Se som eksempel <http://ecpmblog.wordpress.com/2010/05/03/image-online-advertising-value-chain/>

I tillegg til kravet om å kunne godtgjøre regleoverholdelse ovenfor relevant tilsynsmyndighet, er det viktig at behandlingsansvarlige plikter og evner å godtgjøre det samme ovenfor publikum generelt.

Artikkel 23 - Personvern ved design og standard

De to prinsippene "Privacy by design" og "privacy by default" har lenge vært viktige for forbrukernes representanter i Europa. Forbrukerrådet anser reguleringen i artikkel 23 som et skritt i riktig retning. Det er likevel slik at det i et europeisk perspektiv er forskjeller mellom begrepene personvern og "privacy", og vi ser derfor at bestemmelsen dekker områdene der de ikke overlapper hverandre. Retten til privatliv og til beskyttelse av personopplysninger kan reise forskjellige spørsmål, og derfor både bør være likt ivaretatt i reguleringen.

Forbrukerrådet støtter den teknologinøytrale utformingen av bestemmelsen, og vi mener dette vil gi relevante aktører en nødvendig fleksibilitet for å kunne overholde bestemmelsen.

Når det gjelder prinsippet om personvern som standard, mener Forbrukerrådet at artikkel 23.2 bør endres. Det bør være et eksplisitt krav om at personverninnstillingene som standard skal settes til et nivå som sikrer personopplysningene, men uten at noen konkret handling er påkrevd av den registrerte. Den registrerte skal ha muligheten til å endre innstillingene for personvern og selv avgjøre om, og eventuelt hvordan han ønsker å dele sine personlige data.

Forbrukerne skal kunne forvente at tjenestetilbyderne også setter opp personlige innstillinger på en måte som gir oversikt og kontroll over hvordan personlige informasjonen blir innhentet, brukt og lagret. I Forbrukerrådets undersøkelse, som er nevnt ovenfor, svarer 30 % av de spurte som har en offentlig Facebook-profil at de ikke vet hvordan man endrer innstillingene på kontoen sin. For de som har en privat innstilling på profilen sin, svarer kun 3 % at de ikke vet. Dette underbygger den store praktiske betydningen innføringen av et prinsipp om personvern som standard vil medføre.

Forbrukerrådet merker seg at artikkel 23 kun omhandler den behandlingsansvarlige, men kan ikke se noen gode grunner til ikke å la prinsippene også gjelde for databehandleren. Et slikt krav bør legges til i artikkel 26, som også definerer databehandleres forpliktelser.

Artikkel 24-Joint kontrollere

Forbrukerrådet støtter forlaget om "Joint controllers" i artikkel 24 og med den innføringen av en plikt til å definere den enkeltes respektive forpliktelser, samtidig som manglende overholdelse av bestemmelsene vil kunne innebære administrative sanksjoner i henhold til artikkel 79 (5) litra e.

I praksis kan skillet mellom behandlingsansvarliges, databehandleres og tredjeparters rettslige ansvar og struktur være vanskelig å trekke. Selv om artikkel 26 krever at den behandlingsansvarlige definerer ansvarsområdene, vil Forbrukerrådet anbefale å inkludere en spesifikk bestemmelse om felles ansvar mellom behandlingsansvarlige og databehandleren, slik at en registrert kan søke oppreisning/erstatning fra hver enkelt av dem.

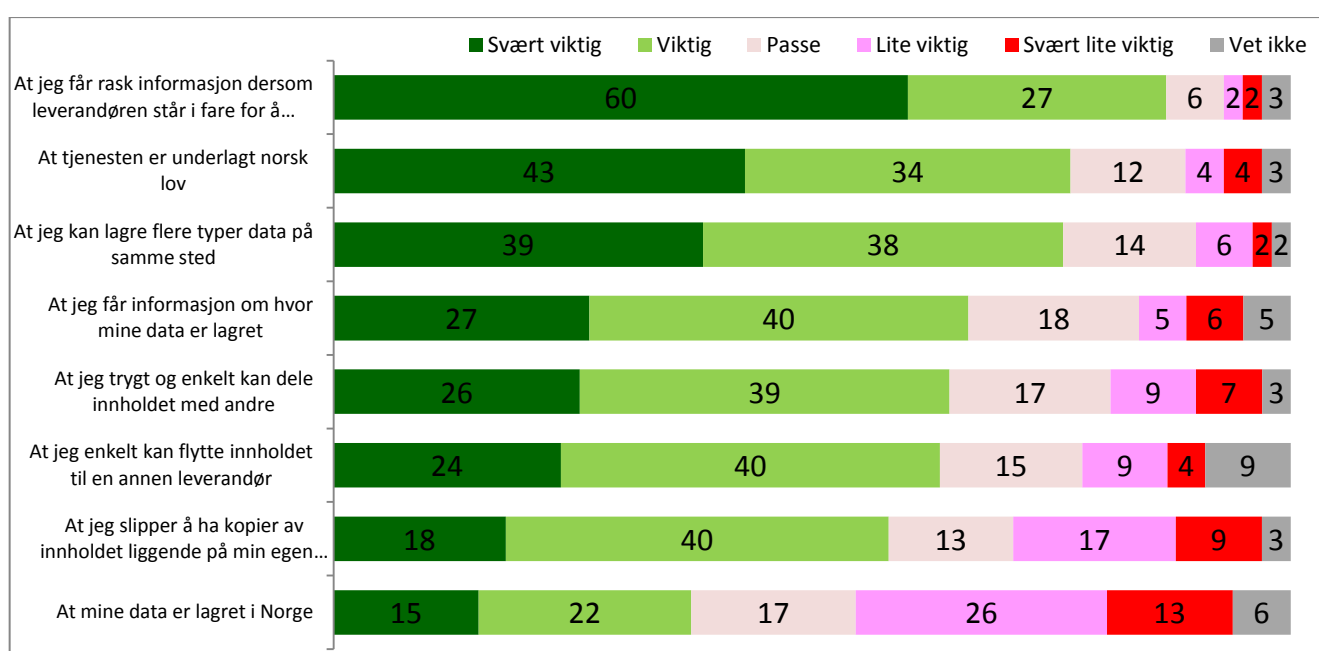
Artikkel 28 - Dokumentasjon

I forbindelse med foreslåtte artikkel 28, vil Forbrukerrådet generelt fraråde begrensningen for virksomheter med færre enn 250 ansatte. En slik begrensning vil etter vårt syn medføre at bestemmelsene sjeldent kommer til anvendelse, og at forordningsforslagets formål dermed ikke vil nås. Samtidig ser vi at mindre selskaper vil kunne oppleve en dokumentasjonsplikt som en urimelig byrde. Dette er i midlertidig ikke et tungt nok argument for å komme bort fra dokumentasjonsplikten. Det vil heller være en oppfordring om å utvikle gode, standardiserte verktøy som er egnet til å nå forslagetets formål

Artikkel 32 - Kommunikasjon av personlig datainnbrudd til den registrerte

I den ovenfor nevnte undersøkelsen utført i mars 2012, spurte TNS Gallup et representativt utvalg av den norske befolkningen om hva de anså for viktig dersom de skulle benytte en nettbasert lagringstjeneste i fremtiden.

«Hvor viktig er følgende for deg når det gjelder lagringstjenester?»



Hele 87 % av de spurte mente det var viktig/svært viktig at de får rask informasjon dersom tjenesteleverandøren står i fare for å miste, eller har mistet kontrollen over den spurtes data. Dette understreker behovet for en horisontal plikt til å informere ved databrudd.

Utkastet introduserer et to-sporsystem, hvoretter alle brudd skal meldes til tilsynsmyndigheten (artikkel 31), mens bare de bruddene som har en negativ effekt på de registrertes beskyttelse skal meldes til enkeltpersoner (artikkel 32).

Det nærmeste man finner en presisering/definisjon på hva som utgjør en negativ effekt, finner vi i recital 67. For å sikre en konsistent forståelse i et marked som strekker seg utover det nasjonale, anser Forbrukerrådet at det innføres en egen definisjon i artikkel 32. En slik definisjon må være bred og ikke kun omfatte brudd som kan føre til økonomisk tap, men også brudd som kan føre til immaterielle skader. Andre kriterier, slik som anvendt tid for i forsøk på å rette brudd og subjektive forhold hos de rammede bør vurderes inkludert i en definisjon.

Forbrukerrådet gir sin støtte til en risikobasert tilnærming til hvordan man skal vurdere hva som anses som en negativ effekt. For å avgjøre risikonivået må både kvantitative og kvalitative momenter inn i vurderingen. Eksempler kan være hva slags type data, antall individer som berøres, og hvilken datamengde det er snakk om.

Når det gjelder innholdet i meldingen til den rammede, bør den enkelte også informeres om sine rettigheter og bli utstyrt med kontaktdetaljene til Datatilsynet og andre som kan bistå, i tillegg til kravene som nevnes i artikkel 32 (2).

Forbrukerrådet støtter også fullt ut forslaget om at varslingsplikten kun gjelder i tilfeller der brudd har negativt effekt. En generell varslingsplikt kan virke mot sin hensikt.

Artikler 33-34 - Konsekvensutredning og forhåndsgodkjenning

Forbrukerrådet støtter i utgangspunktet forslaget om å innføre en plikt til å gjennomføre en Data Protection Impact Assessment (DPIA). Samtidig ser vi at forskjellene mellom personvern og krav til databehandling i europeisk rett er kan komme til uttrykk her. Forbrukerrådet mener derfor at denne bestemmelsen bør utvides, slik at også det som betegnes som personvern dekkes av de risikoanalysene det stilles krav til i artikkel 33 og 34.

Artikler 35-37 - Data Protection Officer

Forbrukerrådet støtter forslaget om å innføre en plikt for både behandlingsansvarlige og databehandlere om å utpeke Data Protection Officer (DPO) innenfor rammen av ansvarlighetsprinsippet.

Dette kravet bør være obligatorisk, og ikke kunne gjelde virksomheter med 250 ansatte eller flere. Vi kan ikke se at forslaget på noen måte godtgjør en slik begrensning. Forbrukerrådet støtter Datatilsynets forslag om at det bør være behandlingens karakter og ikke antallet ansatte som avgjør hvilke plikter som påligger en behandlingsansvarlig. Se for øvrig kommentar over om tilsvarende innsigelse.

Utkastet krever at den utpekte DPO skal være uavhengig fra den behandlingsansvarlige eller databehandleren. Etter vår oppfatning vil en slik uavhengighet fort kunne utfordres f. eks. gjennom et ansettelsesforhold, og ser gjerne at det fremmes mer konkrete bestemmelser som kan sikre uavhengigheten som er nødvendig for at formålet med bestemmelsen skal kunne oppfylles.

KAPITTEL V - Overføring av personopplysninger til tredjeland eller internasjonale organisasjoner (art. 40-45)

Stadig mer av behandlingen av personopplysninger skjer på global basis. Det er derfor avgjørende at et nytt og oppdatert regleverk utformes og forstås tilsvarende. Regelverket må sikre fri flyt av data, samtidig som beskyttelsesnivået ikke svekkes. Etter Forbrukerrådets mening tar det fremlagte forslaget høyde for disse realitetene, og introduserer et rammeverk som er egnet til sikre personopplysninger gjennom en rekke prinsipper som må være oppfylt når personopplysninger overføres utenfor Europa/EU.

Forbrukerrådet beklager samtidig at forslaget åpner for muligheten for overføring også når sikringstiltak ikke er gitt i et juridisk bindende instrument (artikkel 42.5). Etter vår mening er ikke slike unntak godt nok begrunnet, og bør enten strykes fra forslaget, eller begrenses til noen få, konkrete tilfeller.

Det bør også fremkomme klart at overføringer ikke bør være mulig for de landene som EU-kommisjonen har allerede vedtatt beslutninger om ikke å anerkjenne, slik som f. eks. Bahamas og Sør-Afrika.

De såkalte Binding Corporate Rules (BCR) er allerede blitt godkjent av Article 29 Working Party, og Forbrukerrådet støtter forlagets artikkel 43 om at deres uttrykkelige anerkjennelse er en tilstrekkelig protokoll for overføring av data til tredjeland. Det er helt avgjørende at BCRs både er bindende og kan håndheves mot de foretakene hvor hhv behandlingsansvarlige og databehandleren er ansvarlig, og at selve gjennomføringen krever godkjenning av tilsynsmyndigheten.

I henhold til artikkel 41 (1) kan samtykke fra den registrerte brukes som unntak fra reglene om internasjonale overføringer. Som vi allerede har beskrevet, er det tvilsomt om den registrerte har tilstrekkelig kunnskap og kompetanse til fullt ut å gjøre en god nok vurdering av de mulige konsekvensene en slik overføring av personlige data til et tredjeland kan få. Artikkel 44.1 bør etter vår mening derfor slettes.

Forbrukerrådet er også opptatt av den brede definisjonen av "offentlig interesse" som etter vår mening vil kunne omfatte overføring av personopplysninger til tredjeland for forebygging, etterforskning, avdekking og forfølging av straffbare forhold (Recital 87). En tilsvarende bestemmelse her vil kunne øke risikoen for overføringer til politimyndigheter, uten at de registrerte har nødvendige sikkerhet og beskyttelse av personopplysninger gjennom andre, grunnleggende rettigheter.

Når det gjelder internasjonalt samarbeid for beskyttelse av personopplysninger, tar forlagets artikkel 45 sikte på å styrke samarbeidet om håndheving mellom de forskjellige lands tilsynsmyndigheter. Forbrukerrådet anser et slikt samarbeid for avgjørende, men vi er samtidig opptatt av hvilke roller de forskjellige interessenter har i disse prosessene. Vi leser bestemmelsen opp mot den nylige kunngjorte "Consumer Privacy Bill of Rights" fra amerikanske myndigheter. Disse forutser en utvikling av blant annet bransjestandarder som et eget og egnet verktøy for utøve og håndheve personvern. Forbrukerrådet er ikke overbevist om at ordninger som f. eks. selv- og samregulering gir et robust nok håndhevingsystem.

Forbrukerrådet ønsker avslutningsvis å peke på et poeng som er fremmet av den europeiske forbrukerorganisasjonen BEUC når det gjelder fjerningen av bestemmelsen om en inter-service konsultasjon.

En bestemmelse om inter-service konsultasjon ville ha forbudt overføring av personopplysninger basert på forespørsler fra ikke-EU domstoler, administrative myndigheter og andre statlige enheter. Den tidligere bestemmelsen fastslo at ved forespørsler fra tredjepartsland, måtte behandlingsansvarlige eller databehandleren innhente tillatelse for overføring fra sin lokale tilsynsmyndighet. Denne bestemmelsen er særlig relevant med hensyn til krav bygget på amerikansk rett for utlevering av data, da særlig basert på politimyndigheters krav eller såkalte e-discoveries¹⁵.

Amerikanske myndigheter bruker rettslige verktøy som f. eks. Foreign Intelligence Surveillance Act (FISA) og Patriot Act for å samle personopplysninger angjeldende eksempelvis politiske aktiviteter hos utenlandske personer, som kanskje ikke har noen forbindelser med USA, via virksomheter med kontorer i USA. Vi deler BEUCs syn om at bestemmelsen legges til i en egen, ny artikkel.

KAPITTEL VI - Uavhengige tilsynsmyndigheter (art. 46-54)

Forbrukerrådet støtter de foreslåtte bestemmelsene som eksplisitt etablerer de relevante tilsynenes uavhengige status. Dette er helt avgjørende for å sikre et effektivt og pålitelig tilsyn av det juridiske rammeverket.

Samtidig ser vi at reguleringen ikke inneholder noen konkrete rammer for eksempelvis driftsfinansieringen av tilsynene. Utformingen av artikkel 47.5 medfører kun en oppfordring til medlemsstatene om å sikre at tilsynene er utstyrt med tilstrekkelige menneskelige, tekniske og økonomiske ressurser. Finansiering må stå i forhold til det antallet behandlingsansvarlige tilsynet regulerer og antallet enkeltpersoner hvis personopplysninger blir behandlet.

Forbrukerrådet oppfordrer derfor EU-kommisjonen til å studere Article 29 Working Party dokument "The future of Privacy"¹⁶. Der foreslås det flere komplementære og alternative finansieringsmodeller. Etter vår mening bør flere av disse komme til konkret uttrykk i artikkel 47.

KAPITTEL VIII - Rettsmidler, forpliktelser og sanksjoner (art. 73-79)

For Forbrukerrådet er det en avgjørende faktor at et regleverk legger opp til at den som har rett, også tilgodeses med verktøy som gjør det mulig å få rett. Gjeldende direktiv inneholder allerede bestemmelser som gir enkeltpersoner muligheten til å søke oppreisning og erstatning for skader som er påført som et resultat av sikkerhetsbrudd. Samtidig er på det europeiske nivå vanskelig å se at denne bestemmelsen i praksis blir effektivt gjennomført. Høye kostnader knyttet til individuelle søksmål, samt juridisk usikkerhet knyttet rett kompetent myndigheter og gjeldende lovgivning er avskrekkende momenter i håndhevingen av den registrertes rettigheter. Dette kan også være et hinder for tilgang til grunnleggende rettigheter.

¹⁵ http://en.wikipedia.org/wiki/Electronic_discovery

¹⁶ http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf

Forbrukerrådet støtter innføringen av bestemmelser som har som formål å lette mulighetene for den registrerte å håndheve sine rettigheter (artikkel 71). Det er viktig at enkeltpersoner har enkel klageadgang til tilsynsmyndighet der de bor. Det må imidlertid komme klart frem at eventuelle kostnader knyttet til eventuell oversettelse og overføring av klage til tilsynsmyndighet i et annet land ikke skal bæres av den registrerte.

Forbrukerrådet støtter også forslaget om å gi organisasjoner m. fl. rett til å fremføre klage til en tilsynsmyndighet (artikkel 73) eller å ta rettslige skritt (art. 76) på vegne av den registrerte.

Samtidig beklager vi at forslaget ikke gir anledning for organisasjoner og lignende til å fremme søksmål på vegne av flere. Etter vår mening vil f. eks. erstatningskrav som bygger på databrudd kunne være godt egnet for gruppesøksmål, gitt de relativt lave økonomiske kostnader slike brudd kan medføre. Vi støtter derfor BEUC sitt forslag om at en slik anledning gis i egen bestemmelse i artikkel 77. Det bør også avklares om også forbrukerorganisasjon omfattes av disse bestemmelsene.

Det kan undertiden være vanskelig for den registrerte å avgjøre hvilken part som skal bære et erstatningsrettslig ansvar, og Forbrukerrådet støtter derfor reglene om felles ansvar for behandlingsansvarlige og databehandler.

KAPITTEL IX - Bestemmelser knyttet til bestemte situasjoner for databehandling (art. 80-85)

Kapittel IX åpner opp for særnasjonale regler for spesielle behandlingssituasjoner knyttet til ytringsfrihet, helse, sysselsetting, taushetsplikt og religiøse foreninger.

Artikkel 80: Behandling av personopplysninger og ytringsfrihet

Forbrukerrådet støtter unntaksbestemmelsene der personopplysninger er benyttet for journalistiske eller kunstneriske formål. Ytringsfriheten må balanseres mot retten til vern av personopplysninger, og søke å sikre en effektiv beskyttelse av begge.

Forbrukerrådet vil også foreslå at begrepet journalistiske formål forstås på en slik måte at ikke bare omfatter de tradisjonelle mediene, men alle aktiviteter som har til formål å formidle informasjon, meninger og tanker til allmennheten, uavhengige av hvem, gjennom hvilket medium, eller om det er omfattet av næringsvirksomhet eller ei. Dette vil etter vårt syn best oppfylle tidligere avgjørelser fattet av EU-domstolen¹⁷.

Artikkel 81 - Behandling av helserelevante personopplysninger

Bestemmelsen stiller opp en rekke unntak fra det generelle forbudet mot å behandle sensitive helseopplysninger: Forbrukerrådet støtter unntakene der de sikrer en god balanse mellom retten til privatliv, forbrukernes sikkerhet og folkehelseinteresser. Samtidig anser vi at enkelte aspekter bør avklares videre for å hindre misbruk. Videre ønsker vi å understreke at bruk av sensitive helseopplysninger i markedsføringsøyemed bør forbli forbudt, samt at sporings- og profileringsteknologier ved bruk av helserelevante nettsider bør forbys.

¹⁷ C-73/07- Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy.

Artikkel 81 tillater bruk av helseopplysninger til forskningsformål for å bedre styringen av kostnader knyttet til helsevesenet, for å overvåke og forbedre kvalitet, sikkerhet og effektivitet for medisiner og medisinsk utstyr. Forbrukerrådet ser den individuelle og generelle nytten dette vil kunne avstedkomme, men er samtidig skeptiske til de faktiske mulighetene man har for å sikre anonyme data.

Teknologiske fremskritt innen dataanalyse og kombinasjonen med andre datasett vil kunne true anonymiteten, i verste fall føre til identifisering av enkeltpersoner. Det finnes også ubesvarte spørsmål til forslaget, blant annet om hvem som vil kunne ha lovlig tilgang til informasjonen. Vil eksempelvis forskningssektoren inkluderer farmasøytiske selskaper eller forsikringselskaper får tilgang til dataene? Reguleringen kan også sees å mangle nyanser og presisjon når det gjelder hvordan mengden av informasjon vil kunne variere etter hvilken rolle personen som har tilgang skal ha. Som eksempel er det usikkert om dataene en pasient har tilgang til, avviker fra den informasjonen som er tilgjengelig for helseansatte, administrativt ansatte og tredjeparts forskere.

Artikkel 83 - behandling for historiske, statistiske og vitenskapelige forskningsformål

Forbrukerrådet støtter unntaket for de tilfeller der personopplysninger behandles for historiske, statistiske og vitenskapelige formål. Det bør imidlertid presiseres at det som et utgangspunkt er snakk om behandlingen av anonymiserte data, og at kun er når det er umulig for de konkrete forskningsprosjektene at personopplysninger behandles med hjemmel i artikkel 83.

KAPITTEL X - Delegerede handlinger og gjennomføring av handlinger (art. 86-87)

Forskriftsutkastet tilgodeser Europakommisjonen med en rekke oppgaver relatert til både utfylling og implementering. Selv om slike handlinger i visse tilfeller kan være egnet til å sikre enhetlig gjennomføring av reguleringen, er Forbrukerrådet og BEUC bekymret for at den utstrakte bruken av denne mekanismen kan undergrave målet om å etablere et klart og begripelig sett av regler. Dette vil kunne være problematisk for både registrerte og næringsdrivende.

Forbrukerrådet ønsker derfor at antallet slike bestemmelser reduseres betydelig og begrenses til bestemmelsene som omhandler ikke-essensielle problemstillinger, som for eksempel designbestemmelser, kriterier for teknisk tiltak osv. Videre vil mekanismen som fremkommer i artikkel 86 kunne brukes som grunnlag for å vedta sektorspesifikke regler som er egnet til å klargjøre anvendelsen av de generelle rammene for de bestemte områdene av loven. På bakgrunn av dette støtter vi BEUCs forslag om at de delegerede oppgavene vedrørende utfylling og implementering begrenses til følgende bestemmelser:

- Article 6.5 which foresees the adoption of sector-specific rules clarifying the application of the legitimate interests of the controller as a ground for lawful processing;
- Article 8.3 referring to the definition of criteria and requirements to verify parental consent in case of processing of personal data of a child below the age of 13 years old;
- Article 14.7 with regards to the modalities for the provision of information to the data subject;
- Article 15.3 on the content of the communication to the data subject of the personal data undergoing processing following a request to access data;

- Article 22.4 on the appropriate measures to be adopted by the data controller to ensure compliance in accordance with the principle of accountability which requires a certain degree of flexibility;
- Article 23.3 on the design requirements for the application principle of data protection by design on specific products and sectors;
- Article 26.5 regarding the measures to be adopted by the controller in order to comply with the obligations established in the Regulation;
- Article 28.5 on definition of criteria and requirements for the documentation obligation;
- Article 30.3 which deals with technical aspects of security;
- Article 35.11 on the qualification of the data protection officer;
- Article 37.2 regarding the tasks, certification, status, powers and resources of the data protection officer;
- Article 43.3 on further specifying the criteria and requirements of binding corporate rules;
- Article 79.6 on the update of the amounts of the administrative fines

Når det gjelder de resterende bestemmelsene, er det avgjørende at det gjøres ytterligere avklaringer, all den tid de refererer til substansielle og viktige momenter, og derfor har et bestemt behov for rettslig avklaring. Dette er tilfellet av følgende bestemmelser:

- Article 9.3 referring to sensitive data; the processing of sensitive data requires an additional layer of protection due to the nature of the information they can reveal about an individual and therefore the conditions and the safeguards for their processing must be clearly defined in the draft Regulation. Alternatively, this could be the object of opinions/reports of the European Data Protection Board;
- Article 12.4 regarding the definition of threshold above which requests to access and correct one's own data will be considered excessive. Otherwise, there is a risk that Member States use different thresholds thus hindering the effective exercise of the individual's rights;
- Article 17.9 on the implementation of the right to be forgotten. Given the interaction with fundamental freedoms, the conditions for deleting links, copies from publicly available communication services should be defined upfront;
- Article 20.5 reserving the right for the Commission to define the safeguards for the data subject when profiling is allowed. This provision touches upon essential and substantive elements of data subject's protection;
- Article 31.5 which refers to the threshold for data breach notification; unless a threshold is clearly defined in the Regulation, all breaches might have to be notified to the data protection authority;
- Article 32.5 on the communication of data breach to the data subject. It is crucial to define when a breach will seriously affect the rights of the individual and will therefore require notification;
- Article 33.6 regarding the definition of operations presenting specific risks and therefore subject to a data protection impact assessment;
- Article 34.8 on the definition of the high degree of specific risk demonstrated by an impact assessment;
- Article 39.2 on certification mechanisms and privacy seals. For certification and seals to be endorsed by data subjects, full compliance with the legal framework and high standards of

protection need to be ensured. It is therefore important that the conditions for the granting and the recognition within the EU are clearly defined;

- Article 44.7 on the notion of the public interest that might justify a derogation from the rules on transfer to third countries;
- Article 81.3 on the notion of public interest in relation with the processing of personal data concerning health;
- Article 83.3 regarding the criteria for limiting data subject's rights for the processing of historical, statistical and scientific research purposes.

Forbrukerrådet klargjør gjerne sitt standpunkt utover dette dokumentet.

Med hilsen

for Forbrukerrådet

Audun Skeidsvoll
Politisk Direktør

Thomas Nortvedt
Fagdirektør – Digitale
tjenester