

Vår dato	Vår referanse
11.10.2017	17/00008-51
Deres dato	Deres referanse
	17/4200
Saksbehandler:	
Jon Berge Holden	

Justisdepartementets lovavdeling  
Postboks 8005 Dep  
0030 OSLO

## Hørings svar fra Difi - utkast til ny personopplysningslov - Gjennomføring av personvernforordningen i norsk rett

Vi viser til høringsnotatet.

Vår tilbakemelding er todelt: en overordnet og en direkte knyttet til høringsnotatet. I overskriftene henvises det til relevant kapittel i høringsnotatet.

### Overordnet tilbakemelding

Forordningen trer i kraft mai 2018. I lys av den stramme tidsfristen ser vi det som naturlig at lovendringene nå begrenses til nødvendige tilpasninger av gjeldende rett i forbindelse med forordningen, så langt disse behov kan overskues før bestemmelsene har «satt seg». Et viktig spørsmål er blant annet hvordan kravene til behandlingsgrunnlag vil bli forstått. Det bør derfor legges opp til at man forespeiler Stortinget at det kan bli behov for ytterligere lovendringer i tiden framover.

For forvaltningen ser vi særlig at det kan være aktuelt å klargjøre hjemler for behandling av personopplysninger i forvaltningen, særlig ifbm. bruk av stordata og tilrettelegging for «kun en gang»-prinsippet.

### Kommentarer til høringsnotatet

#### Begrepet «sensitive personopplysninger» bør videreføres, 8.3

Vi ser at lovteksten bruker begrepet «sensitive personopplysninger». Det er et innarbeidet begrep, og vi anbefaler at man bruker dette begrepet i den offisielle oversettelsen av forordningen (og ikke begrepet «særlige kategorier av opplysninger», som er benyttet i den uoffisielle oversettelsen).

## **Fødselsnummerbestemmelsen bør bidra til effektivisering, rettssikkerhet og godt personvern, 30.3.1**

Departementet foreslår å videreføre dagens bestemmelse om bruk av fødselsnummer (o.l.), med den endring at Datatilsynets kompetanse til å pålegge bruk av fødselsnummer ikke lenger skal fremgå eksplisitt av bestemmelsen, den antas følge av forordningens artikkel 58 nr 2 bokstav d.

Etter gjeldende rett kreves det (blant annet) at bruk av fødselsnummeret er *nødvendig* for at bruken skal være lovlig. Begrepet har et uklart innhold. Ved etterkontroll av personopplysningsloven skrev utrederne at «Nødvendighetsvurderingen må derfor fremdeles - generelt sett - sies å være svært åpen og skjønnsmessig, og utenfor de sakstyper som er behandlet, kan det ikke sies å være stor forutberegnelighet.»<sup>1</sup>. Av forarbeidene fremgår at forvekslingsfare og konsekvensene av forveksling er et sentralt moment i vurderingen, men at også samfunnshensyn kan tillegges vekt.

Difi ser at utstrakt bruk av fødselsnummer er ønskelig, både av effektivitets-, rettssikkerhets- og personvern hensyn. Særlig gjelder dette for å kunne realisere den politiske målsetningen om «kun en gang»:

- For at private skal slippe å oppgi samme opplysning flere ganger til det offentlige, er det nødvendig at personens opplysninger kan gjenfinnes, når opplysningene skal brukes på nytt. I de sammenhenger vil fødselsnummeret være et bedre søkebegrep enn alternativene (som navn<sup>2</sup>, fødselsdato, adresse, mobilnummer). Fødselsnummerets styrke er at det gir *unik navngiving* og har *to kontrollsiffer*.<sup>3</sup> Samlet fører det til at man praktisk talt eliminerer faren for forvekslinger på grunn av navnelikhet eller feilskrift.
- Riktignok vil kombinasjoner av fødselsdato og navn også kunne gi riktig identifisering i mange tilfeller, jf. at det for de aller fleste personer gir en unik kombinasjon. Utfordringen er imidlertid at man dels vil få falske gjenkjenninger (navnebrødre) og dels falske avvisninger (etter navneendringer). Fødselsnummer gir altså en personverngevinst ved at det bidrar til bedre opplysningskvalitet.

Dagens fødselsnummerbestemmelse forutsetter at bruken er nødvendig, men begrepets innhold er som nevnt ikke tydelig. Vi vil her gi et eksempel på bruk, som etter vårt skjønn klart bør være tillatt, men som utfordres av dagens ordlyd i bestemmelsen:

---

<sup>1</sup> «Utredning om fødselsnummer, fingeravtrykk og annen bruk av biometri i forbindelse med lov om behandling av personopplysninger § 12», skrevet av Schartum og Bygrave på oppdrag fra Justis- og politidepartementet, pkt 4.3.4

<sup>2</sup> 80% av befolkningen har et unikt navn, dvs. at de ikke har noen navnebrødre/-søstre i det norske folkeregisteret, iflg. SSB.

<sup>3</sup> Samtidig er det viktig å være klar over at nummeret ikke er en hemmelighet, det er egnet til å individualisere, skille personer fra hverandre, men ikke til å autentisere/identitetskontrollere personer – til dette kreves bruk av identitetsbevis, eksempelvis BankID, MinID, pass eller nasjonale identitetskort.

- Opplysninger om personers elektroniske adresser (e-post/mobilnummer) finnes i kontakt- og reservasjonsregisteret, som Difi vedlikeholder. For å finne adressen må forvaltningen slå opp ved hjelp av fødselsnummer. Virksomheten kan bruke registeret til alle forvaltningsoppgaver, både situasjoner hvor forveksling har store konsekvenser og der feil vil ha mindre konsekvenser. Samfunnsmessig er det åpenbart hensiktsmessig at kontaktregisteret brukes uavhengig av om konsekvensene av feil er store eller små. Men iht. ordlyden i pol § 12 – som foreslås videreført – vil mange oppfatte spørsmålet som tvilsomt.

Vi anbefaler altså at man ser på muligheten for å justere bestemmelsen. Antakeligvis vil dette kreve noe utredning, som det er usikkert om man rekker å gjennomføre før personvernforordningen skal tre i kraft. Det er imidlertid etter vårt syn verdt å se nærmere på om utviklingen har ført til at uønsket sammenkobling av opplysninger bør motvirkes med andre tiltak enn strenge vilkår for bruk av fødselsnummer, i alle fall i offentlig sektor.

Departementet spør også **om personopplysningsforskriften § 10-2 bør opprettholdes**. Vi er enige med departementet i at det **ikke** er grunn til å fastsette slike særlige krav til sikringstiltak for overføring av fødselsnumre.

Forordningen forutsetter at sikringstiltak velges basert på risiko i det enkelte tilfelle, i overensstemmelse med kravene i artikkel 32. Forordningens tilnærming, med risikobaserte krav, er etter vårt skjønn fornuftig for å sikre egnede sikringstiltak. Det er også i tråd med kravet etter eforvaltningsforskriften § 15, økonomiregelverket i staten og personopplysningslovens/-direktivets hovedregel. Vi nevner for ordens skyld også at det i teorien er stilt spørsmål ved om personopplysningsforskriften i sikkerhetsbestemmelsene dels går ut over lovhjemmelen.

En særregulering av én type opplysninger i én sammenheng (overføring) fremstår som en unødig komplisering og dramatisering av skadepotensialet knyttet til konfidensialitetsbrudd for fødselsnummeret. Til illustrasjon: på persondatarapportens forside fremgår fødselsnummeret til lederen av utvalget. Det må anses klart at behovet for sikringstiltak vil variere med sammenhengene. Skadepotensialet skal vurderes konkret, både mht. sannsynlighet for at skade med en gitt konsekvens inntreffer. Vi viser til vårt veiledningsmaterieell på dette området, jf. efvf §15.

### **Begrepet personvernombud bør videreføres, i stedet for «personvernrådgiver», 14.3.1**

Vi anbefaler at begrepet personvernombud videreføres i ny lov og at man ikke erstatter dette med begrepet «personvernrådgiver» eller lignende.

Begrepet «ombud» får bedre fram uavhengighetskravet som stilles til rollen, og at personen er et naturlig kontaktpunkt for de registrerte, og ikke primært en som skal sikre gjennomføring av de interne krav og føringer virksomhetsledelsen har gitt. I tillegg er både personvernombud og andre ombud innarbeidede og gjenkjennelige begreper i norsk rett.

Skal en virksomhet få god internkontroll (intern styring og kontroll) er den avhengig av å definere tydelige roller som skal støtte virksomhetsledelsen i gjennomføring av ledelsens

retningsvalg og prioriteringer. Det gjelder både innen virksomhetsstyring, informasjonssikkerhet, etterlevelse av personvernregelverket for øvrig mv. Både DFØ og Difi, som statens kompetanseorgan på henholdsvis virksomhetsstyring og informasjonssikkerhet, anbefaler her begrepene «fagansvarlig» for det aktuelle området. Disse roller kan etter vår vurdering ikke bekles av personvernombudet/personvernrådgiveren, jf. at det ville gitt interessekonflikter. Skillet mellom rollene kommer klarere frem med begrepsbruken «fagansvarlig og ombud» enn mellom «fagansvarlig og rådgiver».

### **Vi er skeptiske til en særnorsk hjemmel til å ilegge overtredelsesgebyr for manglende interkontroll, 23.3.2**

Departementet foreslår i § 21 at også brudd på artikkel 10 og 24 skal kunne straffes med overtredelsesgebyr.

Departementet foreslår å videreføre dagens adgang til å ilegge gebyr for manglende internkontroll, mao. brudd på forordningens artikkel 24. Vi er i tvil om det er en hensiktsmessig utvidelse. Vi viser til at

- Internkontrollbestemmelsen er tydeligere enn gjeldende rett på at tiltakene skal være risikobaserte. Bestemmelsen nevner en lang rekke skjønnsmessige faktorer som må vurderes for å fastsette pliktens innhold. Det tilsier at det blir krevende å etablere en forutsigbar tilsynspraksis på dette området.
- Forordningen nevner i overkant av 40 artikler som kan sanksjoneres med overtredelsesgebyr, herunder dokumentasjonsplikter, krav til informasjonssikkerhet, vurdering av personvernkonsekvenser og brudd på den registrertes rettigheter. Er det et reelt behov for i tillegg å sanksjonere brudd på internkontrollbestemmelsen i opplistingen?
- Etersom artikkel 24 er utelatt fra opplistingen av artiklene som etter forordningen vil medføre overtredelsesgebyr vil en særnorsk bestemmelse føre til at norsk og europeisk tilsynspraksis blir forskjellig. Forskjeller i tilsynspraksis kan oppstå på to måter: 1) ved at Datatilsynet ilegger gebyr for manglende internkontroll, når ingen andre bestemmelser er overtrådt. Er det ønskelig? 2), og ved at gebyr ilegges for brudd på internkontrollbestemmelsen, selv om også andre artikler i forordningen er brutt. Forordningen tar sikte på at tilsynsorganene skal etablere en likeartet praksis, blant annet for å unngå at behandlingsansvarlige etablerer seg i områder med en mildere tilsynspraksis. Situasjon nr 1 utfordrer dette prinsippet. I situasjon 2 er formodentlig sanksjonering av internkontrollplikten overflødig.

### **Maksimalt overtredelsesgebyr bør fortsatt være på 10G for offentlige myndigheter og organer (23.3.4)**

Når det gjelder overtredelsesgebyrets størrelse foreslår departementet at gjeldende rettstilstand videreføres.

Vi er enige med departementet i at det er fornuftig. Gebyrene som har vært gitt hittil, har vært omkring 1/10 av maksimalt overtredelsesgebyr.

For å videreføre dagens rettstilstand må lovutkastet suppleres med en setning som viderefører dagens beløpsgrense på 10 G, når det gjelder overtredelsesgebyr som ilegges offentlige myndigheter og organer.

Uten en slik supplerings vil Datatilsynet kunne ilegge offentlige myndigheter overtredelsesgebyr på inntil 190 millioner kroner. Etter vår vurdering er det ikke hensiktsmessig.

Ettersom gebyrene tilfeller statskassen, vil effekten av gebyrene ikke være en utgift for forvaltningen *samlet sett*, men gebyret fungerer som en omfordelingsmekanisme (internt i staten eller fra kommune til stat). Desto større gebyret er, desto mer vil det fungere som et inngrep i politiske myndigheters prioritering av ressurser for å løse forvaltningsoppgaver. Det er uheldig.

Videre vil overtredelsesgebyrets størrelse kunne påvirke organets prioritering av etterlevelsen av ulike regelverk. Internkontrollen i virksomheten skal innrettes basert på vesentlighet og risiko, slik at lover og regler følges og virksomhetens mål oppnås; for staten fremgår dette av økonomireglementet § 4, jf. første og tredje ledd. En videreføring av dagens beløpsgrenser vil opprettholde balansen mellom de ulike regelverkene, og holde overtredelsesgebyret på nivå med gebyrnivået fra andre tilsynsorganer. Vi viser her til at arbeidsmiljøloven åpner for overtredelsesgebyr inntil 15G (<1,5 mill NOK, aml § 18-10 første ledd), mens plan- og bygningsloven setter grensen ved 400 000 for ett tiltak (grense i forskriften § 16-1 i.f.).

### **En lapsus i § 7 – om unntak for journalistiske formål (28.3)?**

Det ser ut til at artikkel 32 ved en feil er falt ut av lovutkastets § 7. For å videreføre gjeldende rett må bestemmelsen nevnes i opplistingen i § 7. Et annet spørsmål er om varslingsreglene i artikkel 33 og 34 også bør medtas, jf. at også journalistisk virksomhet omfattes av dagens krav til varsling ifbm. sikkerhetsbrudd, jf. pof § 2-6, som er hjemlet i pol § 13.

### **Viderefør en klar bestemmelse om innsynsrett i forvaltningens saksdokumenter, 29.3**

Det er i høringsutkastet foreslått å ikke ha lovregulering av forholdet til offentleglova tilsvarende gjeldende personopplysningslov § 6 første ledd. Bakgrunnen er ifølge høringsnotatet at «[n]år forordningen artikkel 86 avklarer forholdet til offentleglova, og forordningen vedtas som norsk lov, anser departementet det som overflødig å lovfeste en ytterligere presisering av at forordningen ikke er til hinder for innsyn etter offentleglova», jf. høringsnotatets pkt. 29.3.

Den nye personopplysningsloven bør etter Difis mening klargjøre forholdet til offentleglova, tilsvarende dagens poppl. § 6 første ledd. Håndtering av innsyns krav etter offentleglova og tilknyttet behandling av personopplysninger er et praktisk viktig spørsmål. Forordningens art. 86 har en ordlyd som skriker etter klarspråk, den er lite egnet som pedagogisk hjelpemiddel til å forstå forholdet mellom personopplysningsloven og lovbestemt innsynsrett.

Til illustrasjon gjengis begge bestemmelsene her:

Forordningen artikkel 86 - Behandling og innsyn i offisielle dokumenter

Personopplysninger i offisielle dokumenter som en offentlig myndighet eller et offentlig eller privat organ er i besittelse av for å utføre en oppgave i allmennhetens interesse, kan utleveres

av myndigheten eller organet i samsvar med unionsretten eller medlemsstatenes nasjonale rett som den offentlige myndigheten eller organet er underlagt, for å bringe retten til innsyn i offisielle dokumenter i samsvar med retten til vern av personopplysninger i henhold til denne forordning.

Pol § 6 - Forholdet til lovbestemt innsynsrett etter andre lover  
Loven her begrenser ikke innsynsrett etter offentleglova, forvaltningsloven eller annen lovbestemt rett til innsyn i personopplysninger. ...

Vi anbefaler at man viderefører § 6 i ny lov.

### **Vurder klarere hjemmel til å publisere postjournaler på internett, 29.3**

De aller fleste offentlige organ publiserer i dag sine offentlige elektroniske postjournaler. Statlige organer publiserer sine offentlige elektroniske journaler i fellesløsningen Offentlig elektronisk postjournal (OEP). Fylkeskommuner og kommuner publiserer sine offentlige elektroniske journaler i egne individuelle løsninger.

Difi og Oslo kommune samarbeider nå om en ny innsynsløsning, elnnsyn, som skal settes i produksjon ved årsskiftet 2017/2018. Publisering av offentlig elektronisk postjournal er en av hovedfunksjonene i elnnsyn. Løsningen vil erstatte dagens OEP for statlig sektor og den skal tas i bruk av Oslo kommune. På sikt skal elnnsyn tilbys til andre kommuner og fylkeskommuner. Fylkeskommuner og kommuner vil i tillegg til offentlig elektronisk postjournal kunne publisere data om møter og utvalg.

Difi ber departementet vurdere om det bør gis en eksplisitt hjemmel for publisering av offentlige elektroniske postjournaler. Temaet er ikke omtalt i høringsnotatet. Spørsmålet gjelder også journaler som omfattes av OEP, jf. at offentlegforskrifta § 6 – som hjemler slik publisering – ikke er trådt i kraft ennå.

Vi nevner også at det danske justisdepartementet synes ha lagt til grunn at behandling av personopplysninger i forbindelse med publisering av postlister rettslig skal bedømmes etter personvernforordningens ordinære regler, med mindre det i nasjonal rett er fastsatt nærmere regler for behandlingen som forener hensynet til innsyn med hensynet til personvern, se betenkningen, «Databeskyttelsesforordningen – og de retlige rammer for dansk lovgivning», s. 965 – 966.

Ta gjerne kontakt med vår saksbehandler Jon Holden ([jho@difi.no](mailto:jho@difi.no), 40045568), dersom noe i uttalelsen er uklart eller ønskes utdypet.

Vennlig hilsen  
for Difi

Grete Orderud  
avdelingsdirektør

Øyvind Grinde  
seksjonssjef

*Dokumentet er godkjent elektronisk og har derfor ingen håndskrevne signaturer.*

Kopi til:  
Kommunal- og  
moderniseringsdepartementet

Postboks 8112 Dep 0032 OSLO