

## Saksframlegg – styret i DA

Saksbehandler:	Ine Evensen	Arkiv:	
Arkivsaksnr.:	18/175 - 3		

### Direktørens sakssammendrag:

Nye regler om personvern basert på EUs personvernforordning, GDPR (forordning 2016/679), vil tre i kraft 25. mai 2018. De nye reglene får konsekvenser for domstolenes og Domstoladministrasjonens virksomhet. Direktøren orienterer med dette styret om arbeidet som er iverksatt for å sikre at de nye personvernkravene blir ivaretatt. Styret bes om å drøfte spørsmålet om felles behandlingsansvar mellom domstolene og Domstoladministrasjonen, samt felles personvernombud for domstolene, Domstoladministrasjonen, Innstillingsrådet for dommere og Tilsynsutvalget for dommere.

## PERSONVERN – TILPASNING TIL NYTT REGELVERK

### 1. Innledning – nye personvernregler og nye krav

I april 2016 vedtok EU en ny personvernforordning «The General Data Protection Regulation» (GDPR). Forordningen skal gjennomføres i norsk rett. Forslag om ny personopplysningslov var på høring i 2017, men lovproposisjon er foreløpig ikke framlagt for Stortinget. Den nye loven skal gjennomføre forordningen direkte i norsk rett, det vil si at forordningen gjelder som sådan. Forordningen gjelder for alle EUs medlemsstater fra 25. mai 2018. Departementet har tatt sikte på at den nye personopplysningsloven skal tre i kraft på samme tidspunkt.

Forordningen og forslaget til ny personopplysningslov innebærer en rekke endringer i forhold til gjeldende regelverk. De gir virksomheter nye plikter, og personene man behandler personopplysninger om, de registrerte, får nye rettigheter. Den nye personopplysningsloven – og dermed forordningen – skal gjelde generelt, men for domstolenes vedkommende er det gitt et viktig unntak for saker som behandles etter rettspleielovgivningen.

Hovedlinjene i det nye regelverket er:

- Tilsynsmyndighetens rolle går fra godkjenning til kontroll

- Det stilles strengere krav til virksomhetene når det gjelder informasjon, rutiner og dokumentasjon
- Virksomhetene må i større grad foreta risikoanalyser og konsekvensvurderinger
- Alle offentlige organer må ha et personvernombud
- Strengere sanksjoner hvis regelverket ikke etterleves

Både domstolene og DA behandler personopplysninger i sitt arbeid. For domstolene er det blant annet en rekke personopplysninger som samles inn i forbindelse med enkeltsakene som behandles, både i de dømmende oppgaver og forvaltningsoppgavene. DA er også i befatning med personopplysninger knyttet til domstolenes enkeltsaker ettersom DA utvikler, forvalter og driver saksbehandlingssystemer og portalløsninger for domstolene. I tillegg behandles det personopplysninger i det administrative arbeidet, for eksempel har både DA og domstolene personopplysninger om sine ansatte. En del av den behandlingen av personopplysninger som skjer i domstolene, og også i DA, vil omfattes av rettspleielovunntaket, se nedenfor punkt 2.2.

Domstolene og DA har ansvaret for at all behandling av personopplysninger er i tråd med det nye regelverket innen 25. mai 2018. Direktøren har derfor iverksatt et arbeid som skal sikre at domstolenes og DAs behandling av personopplysninger er tilfredsstillende og forsvarlig i forhold til de nye reglene. Direktøren ønsker i det følgende å orientere styret om det pågående arbeidet og de tiltakene som er planlagt. I tillegg ønsker direktøren styrets syn på spørsmålene om plassering av behandlingsansvar og organisering av personvernombud i domstolene og DA.

## **2. Kort om de nye personvernreglene**

### **2.1. Reglenes generelle anvendelsesområde**

Personvern handler i sin rene form om retten til et privatliv og retten til å bestemme over egne personopplysninger. De nye reglene har på samme måte som gjeldende regler et noe snevrere anvendelsesområde enn dette utgangspunktet kan antyde: I personvernforordningen artikkel 2 er det fastsatt at reglene får anvendelse på *«helt eller delvis automatisert behandling av personopplysninger og på ikke-automatisert behandling av personopplysninger som inngår i eller skal inngå i et register»*. Anvendelse av reglene forutsetter med andre ord at opplysningene enten skal behandles automatisk, eller at de inngår i eller skal inngå i et register. Automatisert behandling betyr, i denne sammenheng, at behandlingen skjer med elektroniske hjelpemidler.

Med *personopplysning* menes enhver opplysning om en identifisert eller identifiserbar fysisk person. I identifiserbar ligger at man direkte eller indirekte kan identifisere vedkommende ved hjelp av en identifikator, som for eksempel et navn, et identifikasjonsnummer, telefonnummer eller lignende. Forordningen omtaler også særlige kategorier personopplysninger, også omtalt som *sensitive personopplysninger*. Dette vil for eksempel være opplysninger om rasemessig eller etnisk opprinnelse, politisk oppfatning, religion, overbevisning eller fagforeningsmedlemskap.

*Behandling* av personopplysninger vil si enhver operasjon eller rekke av operasjoner som gjøres med slike opplysninger. Dette kan for eksempel være innsamling, registrering, lagring, endring, gjenfinning, bruk, sammenstilling og sletting.

Den behandlingsansvarlige og databehandleren pålegges en rekke plikter i forbindelse med at de behandler disse opplysningene. Den *behandlingsansvarlige* er den som alene eller sammen med andre bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes. I en organisasjon/virksomhet vil behandlingsansvaret ligge hos den øverste ledelsen. Selv om behandlingsansvaret kan ligge høyt over de nivåer i organisasjonen som har det daglige ansvaret, vil utførelsen av de oppgaver og plikter som følger av behandlingsansvaret likevel delegeres til lavere nivåer. Det formelle ansvaret for etterlevelse av reglene kan ikke delegeres.

*Databehandleren* er den som behandler personopplysninger på vegne av den behandlingsansvarlige. Dette vil være en person eller virksomhet utenfor den behandlingsansvarliges organisasjon, typisk et databehandlingsforetak. Begrepet brukes altså ikke om personer som faktisk behandler data, men betegner en bestemt type avtalepart som behandlingsansvarlige ofte anvender, for eksempel der driften av datamaskinsystemet som behandler personopplysninger er satt bort til en ekstern tjenesteleverandør («outsourcing»).

Personopplysninger skal behandles ut i fra visse grunnprinsipper. Dette er prinsippene om lovlighet, rettferdighet og gjennomsiktighet, formålsbegrensning, dataminimering, riktighet, lagringsbegrensning og integritet og fortrolighet. De grunnleggende prinsippene er i hovedsak en videreføring av de grunnkrav til behandling som følger av gjeldende personopplysningslov.

## 2.2. Unntak for saker som behandles etter rettspleielovgivningen

Det nye personvernregelverket gjelder generelt, det vil si i utgangspunktet også for domstolene. I utkast til ny personopplysningslov § 2 er det imidlertid foreslått at loven ikke skal gjelde for «*saker som behandles eller avgjøres i medhold av rettspleielovene (domstolloven, straffeprosessloven, tvisteloven og tvangsfullbyrdelsesloven mv.)*». Dette er en videreføring av gjeldende rett og ordlyden er likelydende med dagens personopplysningsforskrift § 1-3. Domstolloven, straffeprosessloven, tvisteloven og tvangsfullbyrdelsesloven er nevnt som eksempler på rettspleielover i den foreslåtte lovteksten, men listen er ikke uttømmende. Ettersom tvangsfullbyrdelsesloven er nevnt, kan det legges til grunn at unntaket også omfatter saker som behandles etter spesialprosessen, herunder konkurssaker, skiftesaker, jordskiftesaker og skjønnsprosessaker. Forvaltningsoppgaver og -saker faller utenfor.

Unntaksbestemmelsen knytter seg ikke til domstolens behandling av personopplysninger som sådan, men til saker som behandles eller avgjøres i medhold av rettspleielovene. Dette betyr at i den grad DA behandler opplysningene på vegne av domstolene, for eksempel i forbindelse med drift av saksbehandlingssystemer og portalløsninger, er behandlingen unntatt loven hvis personopplysningene er tilknyttet saker som behandles eller avgjøres i medhold av rettspleielovene.

Unntaket gjelder trolig bare for den tid saken er til behandling, det vil si den faktiske saksbehandlingsperioden fram til avgjørelsen er fattet og etterarbeidet avsluttet. Eventuell behandling av personopplysningene etter at saken er avsluttet, for eksempel til statistikk, omfattes derfor ikke av unntaket, jf. PVN-2008-02. Lignende synspunkt finnes også i rapport om

datalagringsdirektivet og menneskerettigheter, utredet av Hans Petter Graver og Henning Harborg, avgitt til Justisdepartementet og Samferdselsdepartementet 1. oktober 2015 - (UTRJD-2015-1).

Videre gjelder unntaket bare for konkrete enkeltsaker, dette følger av ordlyden. Dette betyr for eksempel at personopplysninger som registreres i forbindelse med at en advokat oppretter en bruker i Aktørportalen, ikke omfattes av unntaket. Det er da tale om opplysninger om advokaten selv, og opplysningene er ikke tilknyttet enkeltsaker som er til behandling.

At rettspleieunntaket gjelder, innebærer ikke at personvernreglene i sin helhet er uten relevans. I teori knyttet til gjeldende forskrift § 1-3, er det sagt at unntaket trolig skal tolkes slik at de bestemmelsene som gjelder generelle krav til behandlingen får anvendelse, for eksempel regler om rettslig grunnlag og informasjonssikkerhet. Regler om for eksempel innsynsrett, varslingsplikt og sletting antas å ikke få anvendelse. Også i forarbeidene til gjeldende personopplysningslov er det uttalelser som støtter denne forståelsen, blant annet i Ot.prp. nr. 92 (1998-1999) s. 31 som direkte gjelder behovet for unntak for politiregistrenes vedkommende. Det er i den forbindelse uttalt at unntak særlig vil være relevant for den registrertes innsynsrett, varslingsplikten, tilsynsmyndighetens tilgang til opplysningene osv., men at det er grunn til å anta at lovens mer generelle krav til saklig og korrekt behandling, sikring og internkontroll bør gjelde.

Bakgrunnen for unntaket og uttalelser i forarbeidene, tilsier derfor at unntaket ikke gjelder hele loven, men bare de regler som kan berøre behandlingen av enkeltsaker. Det er heller ingen gode grunner for at generelle regler som for eksempel grunnleggende krav til systemsikkerhet ikke skal gjelde for saker som behandles etter rettspleielovene.

### **3. Domstoladministrasjonens oppfølging av de nye reglene**

Personvern er et virksomhetsansvar, som det påligger den enkelte virksomhet og enhet å ivareta. Direktøren har etablert en intern arbeidsgruppe, som arbeider med gjennomføringen av de nye personvernreglene i domstolene. Arbeidsgruppen gjennomgår regelverket og virksomheten, og skal foreslå nødvendige tiltak og tilpasninger. Arbeidsgruppen skal også bistå ved gjennomføringen av de nødvendige tiltak. Arbeidsgruppen antar at det blir nødvendig å gjennomføre tiltak innenfor følgende hovedområder:

- Rutiner, retningslinjer og dokumentasjon
- Organisatoriske tiltak (personvernombud)
- Personvern i IKT-systemer og -løsninger
- Informasjons- og kompetansetiltak

I tillegg skal eksterne databehandling på vegne av domstolene og DA gjennomgås. Dette gjelder i hovedsak databehandleravtaler og personvern ved systemutvikling.

Arbeidsgruppen sørger for å informere domstolene om det nye personvernregelverket og hvilke konsekvenser regelverket har for domstolenes virksomhet. Arbeidsgruppen skal også se nærmere på hvordan det kan arbeides for å utvikle felles/standardiserte rutiner, retningslinjer eller liknende for

domstolene og igangsette et arbeid på dette område. I den forbindelse skal gruppe involvere domstolsansatte.

Arbeidsgruppen består i dag av:

- Ine Strøm Evensen, rådgiver, rettsenheten (leder)
- Anita Engan, arkivleder, enhet for økonomi og eiendom
- Tommy Kinnunen, sikkerhetsansvarlig i IKT-enheten
- Arve Hamar, seniorrådgiver, IKT-enheten
- Bjørn-Are Lyngstad, seksjonssjef, IKT-enheten
- Klaus R. Kristiansen, seniorrådgiver, rettsenheten

Arbeidsgruppen innhenter bistand og tilleggsressurser ved behov. Dette er eksempelvis aktuelt i forbindelse med informasjons- og kompetansetiltak, og ved informasjonsinnhenting. Arbeidsgruppen bistår dessuten Innstillingsrådet for dommere og Tilsynsutvalget for dommere i deres personvernarbeid.

I tillegg har DA engasjert personvernekspertise fra BDO, i første omgang for å bistå med gjennomgang og dokumentasjon av den faktiske behandlingen av personopplysninger og behovet for rutineendringer. BDOs vurdering forventes avsluttet i løpet av mars 2018. I tillegg kan det bli aktuelt å få bistand fra BDO til kvalitetssikring av rutiner, retningslinjer og andre tiltak som skal utvikles på bakgrunn av ny personvernlovgivning.

#### **4. Utvikling og implementering av rutiner og dokumentasjon**

Domstoladministrasjonen er i ferd med å gjennomgå domstolenes og DAs behandling av personopplysninger, samt gjeldende rutiner og arbeidsmåter. På bakgrunn av denne gjennomgangen vil nødvendige endringer og forbedringer bli foreslått. I det følgende gis det en kort oversikt over områder og tema hvor det sannsynligvis vil kreves endringer på bakgrunn av ny personvernlovgivning.

Ny personvernlovgivning legger større ansvar på den behandlingsansvarlige enn i dag. Det formelle ansvaret vil ligge hos ledelsen, men oppgavene som ansvaret medfører kan delegeres til lavere nivåer i organisasjonen.

Dagens ordning med konsesjoner fra Datatilsynet, erstattes av egenvurderinger fra den behandlingsansvarlige og en sterkere tilsynsrolle for Datatilsynet. Dette er en grunnleggende og omfattende endring som vil få stor betydning for den «alminnelige behandlingsansvarlige», eksempelvis finansinstitusjoner og telekom-aktører. Som følge av rettspleieunntaket og den i stor grad regelstyrte saksbehandlingen i domstolene, får ikke endringen like stor praktisk betydning i domstolene. For DA er den praktiske betydningen større, blant annet fordi DA utvikler og driver IKT-løsninger og andre felleisløsninger for domstolene.

Den behandlingsansvarlige er ansvarlig for å vurdere behandlingsgrunnlaget – hjemmelen – for å behandle personopplysninger, og hvor langt behandlingsbehovet rekker. Behandlingen skal

begrenses til det forsvarlige og nødvendige, både i omfang og tidsmessig utstrekning. Man må velge den behandlingsmåten som best ivaretar både personvern hensynene og formålet med behandlingen, eksempelvis anonymisering eller bruk av bestemte IKT-verktøy.

Det skal foretas risiko- og konsekvensvurderinger. Ved særlig omfattende behandling eller behandling med særlig risiko, etablerer ny personvernlovgivning særlige vurderingsplikter og i noen tilfeller plikt til forhåndsavklaring fra personvernmyndighetene. Dette må gjennomføres før behandlingen av personopplysninger starter.

Den behandlingsansvarlige må etablere tilstrekkelig sikkerhet ved behandlingen av personopplysninger. Dette omfatter både system- og informasjonssikkerhet. De løsningene som brukes, må ha et forsvarlig sikkerhetsnivå. Spredning og inntrengning må hindres, og det må vurderes hvem som skal ha tilgang til hva. Det må etableres tilfredsstillende systemer for tilgangsregulering og -kontroll, eventuelt logging. Sikkerhetstiltak kan etableres både i tekniske løsninger og organisatorisk.

Den behandlingsansvarlige må etablere rutiner og systemer for oppbevaring, arkivering og sletting av personopplysninger. Personopplysninger skal oppbevares sikkert, og det må etableres rutiner for sletting når behandlingen er fullført eller det ikke lenger foreligger noe behandlingsgrunnlag. Arkiverdig materiale kan og skal oppbevares etter arkivlovgivningens regler også etter at behandlingen er avsluttet.

Den behandlingsansvarlige plikter å gi informasjon til de registrerte, og etablere systemer og rutiner som ivaretar de registrertes rettigheter. Det må blant annet gis informasjon om hvilke opplysninger som behandles, hvor man skal henvende seg for å kreve innsyn og hvordan man kan kreve retting eller sletting. Det bør etableres standardinformasjon som gjøres lett tilgjengelig på internett.

Rettspleieunntaket innebærer at de registrerte har begrenset krav på innsyn i behandlingen av personopplysningen i konkrete saker som behandles etter prosesslovgivningen, og tilsvarende begrensede rettigheter når det gjelder retting, sletting og lignende. Erfaringsmessig bør det likevel utarbeides god, generell informasjon om behandlingen av personopplysninger i domstolene for å hindre misforståelser og unødvendige henvendelser.

Ny personvernlovgivning vil medføre nye og strenge krav til avvikshåndtering i de tilfellene personopplysninger kommer på avveie, eller ved ulike system- og rutinesvikt. Kravene gjelder både intern oppfølging og varsling til tilsynsmyndighetene. Tidsfristene for avvikshåndtering blir korte, og brudd på reglene om avvikshåndtering kan utløse strenge sanksjoner. Det må derfor etableres gode rutiner for avvikshåndtering og tydelige systemer for rapportering. Kontroll av at disse rutinene og systemene fungerer, bør dessuten være en integrert del av et internkontrollsystem.

For å ivareta personvern hensynene og personvernlovgivningens krav, må såkalt «innebygget personvern» bli en del av systemutviklingen i framtiden. Dette innebærer at personvern gjøres til en integrert del av framtidige saksbehandlingssystemer og andre IKT-løsninger, og at personvern blir hensyntatt gjennom både utviklings-, drifts- og vedlikeholds-/videreutviklingsfasen. Innebygget personvern er i ferd med å bli etablert som en arbeidsmetodikk ved systemutviklingsarbeid.

De nye personvernreglene innebærer i praksis en vesentlig skjerping av kravene til dokumentasjon. For det første må rutiner og systemer for behandling av personopplysninger oppdateres og dokumenteres. For det andre må vurderinger av behandlingsgrunnlag, risikovurderinger og valg av behandlingsmetoder dokumenteres. Dette gjelder også innebygget personvern i utviklingsarbeid. For det tredje må avvikshåndtering dokumenteres, både når det gjelder varsling og oppfølging. Dokumentasjonen må utformes og oppbevares slik at den er lett tilgjengelig, og slik at den raskt kan framlegges for tilsynsmyndighetene ved behov.

For å sikre at personvernlovgivningens krav til enhver tid blir ivaretatt, bør DA vurdere å etablere en mer formalisert internkontroll. Internkontrollfunksjonen kan om ønskelig ivareta avvikshåndtering, og ha et hovedansvar for dokumentasjon. Internkontrollrollen bør ikke kombineres med personvernombudsrollen, da det kan skape rollekonflikter.

## **5. Plassering av behandlingsansvaret**

Den behandlingsansvarlige er den som bestemmer formålet med behandlingen og hvilke hjelpemidler som skal anvendes i behandlingen. Et sentralt spørsmål som må avklares, er hvem som er behandlingsansvarlig for domstolene og DAs behandling av personopplysninger. Dette er et spørsmål om ansvarsfordeling mellom domstolene og DA, og om reglens åpning for felles behandlingsansvar skal benyttes.

Når det gjelder Innstillingsrådet for dommere og Tilsynsutvalget for dommere, legges det til grunn at disse organene har, og skal ha, selvstendig behandlingsansvar for behandling av personopplysninger i sin virksomhet.

Gjeldende personopplysningslov åpner for felles behandlingsansvar. Verken gjeldende lov, den nye personvernforordningen eller utkastet til ny personopplysningslov gir noen klar løsning for hvordan fordelingen skal løses i domstolene. Dette åpner for å velge den mest hensiktsmessige løsningen innenfor de alminnelige reglene i ny personvernlovgivning.

I forarbeidene til gjeldende personopplysningslov og senere teori, er spørsmålet om fordeling av behandlingsansvar mellom faglig uavhengige organer og administrativt overordnede organer drøftet. Drøftingene gir en viss veiledning også for domstolssystemet.

Schartum og Bygrave, «Personvern i informasjonssamfunnet», (3. utgave 2016) s. 167 bruker Datatilsynets behandling av personopplysninger som et eksempel for å forklare hvor behandlingsansvaret skal plasseres. Det er vist til at Datatilsynet er et uavhengig forvaltningsorgan administrativt underlagt KMD. For behandling av personopplysninger som gjelder administrasjon skal behandlingsansvaret plasseres hos departementet. For Datatilsynets behandling av personopplysninger i forbindelse med den myndigheten de har etter personopplysningsloven, ligger behandlingsansvaret hos Datatilsynet. Datatilsynet er helt uavhengig fra KMD ved utøvelse av denne myndigheten, og KMD har ingen instruksjonsmyndighet over Datatilsynets behandling av personopplysninger i den sammenhengen.

Forholdet mellom domstolene og DA kan til en viss grad sammenlignes med forholdet mellom KMD og Datatilsynet. Domstolene er uavhengige i sin dømmende virksomhet, men DA har et overordnet administrativt ansvar. Det kan derfor argumenteres med at den enkelte domstol har behandlingsansvar for behandling av personopplysninger som skjer i forbindelse med dømmende virksomhet, mens DA er behandlingsansvarlig for øvrig behandling av personopplysninger. DA og domstolene er imidlertid i en noe særegen situasjon ettersom det er DA som drifter og utvikler domstolenes saksbehandlingssystemer. Formelt er det den enkelte domstol som styrer behandlingen av personopplysningene, men i realiteten er den enkelte domstols mulighet til å påvirke hvordan personopplysninger behandles og hvilke hjelpemidler som skal anvendes, begrenset.

Grunntanken er at den som styrer behandlingen er den som er nærmest til å ha ansvaret for at behandlingen skjer i henhold til regelverket. Å plassere alt behandlingsansvaret hos den enkelte domstol er ikke i samsvar med denne grunntanken. Samtidig kan det være betenkelig i forhold til domstolenes uavhengighet å plassere alt behandlingsansvar hos DA alene. Domstolenes uavhengige rolle ville dessuten hindre DA i å ivareta behandlingsansvaret dersom det i sin helhet ble plassert hos DA.

Etter direktørens oppfatning framstår det som mest hensiktsmessig at DA og den enkelte domstol har behandlingsansvar i fellesskap når det gjelder den delen av virksomheten som ikke er dømmende, og denne løsningen harmonerer med grunntanken om styring og ansvar. Det følger av regelverket at DA og domstolene da må fordele ansvaret for å overholde personvernregelverket, særlig med hensyn til utøvelsen av den registrertes rettigheter og plikten til å informere. Etter direktørens oppfatning bør det derfor etableres en ordning som fordele ansvaret mellom DA og domstolen. Innholdet i ordningen må gjøres tilgjengelig for de registrerte. Det bør også utpekes et felles kontaktpunkt for de registrerte.

Direktøren ber om styrets tilslutning til å arbeide videre med å formalisere felles behandlingsansvar mellom domstolene og DA, men slik at domstolene skal ha behandlingsansvar for behandlingen av personopplysninger i sin dømmende virksomhet, slik at domstolenes særlige uavhengighet blir ivaretatt.

## **6. Etablering av personvernombud**

Den nye personvernlovgivningens regler om personvernombud innebærer en betydelig utvidelse sammenlignet med dagens rettstilstand. De nye reglene innebærer blant annet at alle offentlige virksomheter har plikt til å ha et personvernombud. Både domstolene, DA, Innstillingsrådet for dommere og Tilsynsutvalget for dommere må ha personvernombud etter det nye regelverket. Reglene stiller dessuten krav til ombudets kvalifikasjoner, oppgaver og posisjon i virksomheten. Personvernombudets oppgaver må avgrenses mot saker som behandles eller avgjøres i medhold av rettspleielovene.

Personvernombudet skal gi råd om hvordan virksomheten best mulig kan ivareta personverninteressene. Ombudet har imidlertid ikke noe ansvar for at personvernregelverket følges, dette ansvaret påhviler virksomheten. Personvernombudets rolle er å bistå virksomheten i arbeidet



med å ivareta personvernet. Reglene krever at den som skal være personvernombud har de nødvendige faglige og personlige egenskapene for å fylle rollen.

Personvernombudets oppgaver er fastsatt i de nye personvernreglene. Ombudet skal informere og rådgi virksomheten, både ledelsen og de ansatte som behandler personopplysninger, og kontrollere at personverninteresser ivaretas. På anmodning skal ombudet gi råd om vurdering av personvernkonsekvenser og kontrollere gjennomføringen av den. Ombudet skal også drive holdningsskapende arbeid og har ansvaret for opplæring av ansatte som er involvert i behandlingen av personopplysninger. Videre skal ombudet samarbeide med og fungere som et kontaktpunkt for tilsynsmyndigheten. Ombudet skal også være kontaktperson for de registrerte i alle spørsmål om behandling av deres personopplysninger og utøvelsen av deres rettigheter som følger av personvernregelverket.

Personvernombudet skal ha en faglig selvstendig rolle, og skal ikke være underlagt instruksjonsmyndighet i den faglige rollen som personvernombud. Ombudet rapporterer direkte til virksomhetens øverste leder. Personvernombudet kan heller ikke avsettes eller direkte eller indirekte straffes på noen måte for å utføre sine oppgaver.

Offentlige organer kan utpeke ett felles personvernombud, dersom størrelsen og organisasjonsstrukturen tilsier det. For DA og domstolene vil det etter direktørens oppfatning være hensiktsmessig å utpeke ett felles ombud. Både organisasjonsstrukturen og den store variasjonen i domstolenes størrelse tilsier at det utpekes ett felles personvernombud. Store deler av domstolenes virksomhet er dessuten unntatt fra personvernombudets arbeidsområde i medhold av rettspleieunntaket, slik at det er lite hensiktsmessig med egne personvernombud i hver enkelt domstol. Kombinasjonen av rettspleieunntakets begrensninger i personvernombudets arbeidsområde og personvernombudets uavhengige stilling medfører etter direktørens oppfatning at personvernombudets rolle ikke vil komme i konflikt med domstolenes uavhengighet.

Innstillingsrådet for dommere og Tilsynsutvalget for dommere er uavhengige forvaltningsorganer. Spørsmålet om felles personvernombud er drøftet med organenes ledere. Begge er positive til en ordning med felles personvernombud.

Etter direktørens oppfatning bør det utpekes et felles personvernombud for domstolene og DA, og Innstillingsrådet for dommere og Tilsynsutvalget for dommere bør inviteres til å delta i ordningen. Direktøren ber om styrets tilslutning til å fortsette arbeidet med å utarbeide mandat for å utpeke et felles personvernombud.

## **7. Konsekvenser ved brudd på regelverket**

Datatilsynet har i dag ansvaret for å håndheve personvernregelverket og det er foreslått at kompetansen fortsatt skal ligge til Datatilsynet når det nye regelverket trer i kraft. Datatilsynet vil ikke ha kompetanse til å føre tilsyn med behandling av personopplysninger som omfattes av rettspleielovunntaket.

Etter gjeldende rett kan Datatilsynet ilegge overtredelsesgebyr for brudd på personopplysningsloven og forskriften. Ordningen med overtredelsesgebyr videreføres i det nye regelverket, men størrelsen på gebyret økes betraktelig. Dagens regler fastsetter et maksimumsbeløp på 10 G, mens det nye regelverket setter en øvre grense på 20 millioner euro, eller hvis det gjelder foretak, 4 % av den samlede globale årsomsetningen hvis denne er høyere.

Det er også foreslått å videreføre Datatilsynets adgang til å ilegge tvangsmulkt i tilfeller Datatilsynet gir en virksomhet et pålegg.

For øvrig vil den som har lidd skade som følge av en overtredelse av forordningen, kunne ha krav på erstatning fra den behandlingsansvarlige eller databehandleren.

**Direktørens innstilling:**

Administrasjonens framstilling tas til orientering. Styret slutter seg til administrasjonens arbeidsplan, samt forslaget om delvis felles behandlingsansvar og felles personvernombud.

12.02.2018

Sven Marius Urke  
direktør

Solveig Moen – avd.dir RETT  
avdelingsdirektør