Databehandlers behandling av personopplysninger

Jan Sandtrø

Jan Sandtrø er advokat og partner i advokatfirmaet DLA Piper, og er spesialisert innenfor it-rettslige problemstillinger, herunder personvern.
E-post: jan.sandtro@dlapiper.com

Sammendrag:
Artikkelen omhandler databehandlers behandling av personopplysninger, herunder grensedragningen mellom den behandlingsansvarlige og databehandler, databehandlerens plikter, omfanget av behandlingen, krav til informasjonssikkerhet, databehandlerens bruk av underdatabehandler, erstatningsansvar og sanksjoner. Databehandling over landegrensene behandles også i relasjon til databehandler. Artikkelen redegjør for gjeldende rett for databehandling av personopplysninger etter personopplysningsloven og -forskriften, og omhandler også betydningen personvernforordningen vil få for databehandlers behandling av personopplysninger.

Nøkkelord: personvern, personopplysninger, databehandler, personopplysningsloven, personverndirektivet, personvernforordningen.

DOI: 10.18261/issn.0809-9510-2016-02-03-01

Innhold

1 Innledning

Emnet for denne artikkelen er rettslige spørsmål knyttet til bruk av databehandler til behandling av personopplysninger. Med utviklingen innenfor informasjonsteknologi har det blitt svært vanlig at et selskap utfører behandling av data på vegne av et annet selskap eller person. De fleste bedrifter, organisasjoner og offentlige myndigheter benytter seg av en eller flere databehandlere til å behandle sine data, herunder personopplysninger. Det kan være ulike årsaker til at behandling av personopplysninger overlates til andre, men det kan typisk skyldes at andre har bedre kompetanse eller teknologi, og/eller at dette kan utføres mer kostnadseffektivt av andre. Behandling av data kan også være en konsekvens av andre tjenester eller oppgaver som skal utføres, eksempelvis driftstjenester ved it-system eller lønnsoppgaver for medarbeidere.

Mens det gjelder en rekke strenge krav til behandling av personopplysninger, er det få formelle krav til behandling av personopplysninger på vegne av andre. Få formelle krav kan også forklare hvorfor emnet er lite behandlet i juridisk teori, og at det er få rettskilder på området.[1] Ikrafttredelsen av EUs forordning om personvern[2] («forordningen») den 24. mai 2016 og senere implementering av forordningen til norsk lov, vil imidlertid endre rettskildebildet. Forordningen skal gjelde for EU/EØS-medlemslandene fra 25. mai 2018, og den erstatter EUs personverndirektiv av 1995. Ettersom den norske personvernlovgivningen i stor grad er basert på personverndirektivet, vil forordningen også medføre endringer i norsk lovgivning.

Det er imidlertid ikke ventet at forordningen vil medføre omfattende endringer i norsk rett, siden forordningen bygger på de samme grunnprinsipper som er kjent fra personverndirektivet. Forordningen vil gjelde direkte som norsk rett, og det å erstatte personverndirektivet med en forordning, vil innebære en større grad av harmonisering av personvernreglene i EU/EØS enn under personverndirektivet. For næringslivet i Europa – ikke minst for selska-

1. Lov, forarbeider og forskrift er behandlet nedenfor i artikkelen. I tillegg er det EU-rettslig materiale, men det foreligger kun én relevant avgjørelse fra Personvernnemnda om databehandler.
2. Europaparlaments- og rådsforordning om beskyttelse av individer ved behandling av personopplysninger og om fri flyt av slike opplysninger og om oppheving av direktiv 95/46/EF (generell personvernforordning), også omtalt som «General Data Protection Regulation» (GDRP).

per med virksomhet i flere europeiske land – vil det derfor bli enklere å forholde seg til personvernreglene, siden det bare vil bli ett regelsett å forholde seg til. Forordningen åpner imidlertid for at det kan vedtas særskilt nasjonal lovgivning på noen områder. I den grad forordningen ventes å medføre endringer i norsk rett, er dette forsøkt kommentert nedenfor. Forordningen vil, som nevnt, først få virkning fra 2018 i Norge, og innen den tid vil det bli klart hvordan forordningen vil bli gjennomført i norsk rett. Ettersom forordningen vil få direkte virkning i norsk rett, bør de berørte, som behandlingsansvarlige og databehandlere, benytte muligheten til å iverksette tiltak før forordningen, og eventuell ny lovgivning i Norge, trer i kraft.

Fremstillingen i denne artikkelen om databehandlers behandling av personopplysninger, er i det vesentlige basert på dagens lovgivning på området, først og fremst personopplysningsloven og personopplysningsforskriften. De særskilte reglene innenfor spesielle sektorer og bransjer, som helse-, finans-, telesektoren mv., vil ikke bli gjennomgått.

I punkt 2 nedenfor vil personopplysningslovens virkeområde og system behandles; det redegjøres for sentrale begrep i personopplysningsloven og personverndirektivet og personvernforordningen, det lovmessige grunnlaget for bruk av databehandler, og grensedragningen mellom den behandlingsansvarlige og databehandleren som er avgjørende for oppgaver databehandleren utfører for den behandlingsansvarlige, blir også behandlet.

Behandlingen av personopplysninger databehandleren kan forestå både etter lovverk og etter avtale med den behandlingsansvarlige, gjennomgås i punkt 3. I dette punktet vil også krav som stilles til databehandleravtalen, og forhold som bør reguleres i avtalen, behandles. Plikter som tilligger databehandleren, som innsyns- og informasjonsplikt, og en rekke av de konkrete problemstillinger som oppstår for databehandleren, vil behandles i punkt 4; innsyns- og informasjonsplikter (punkt 4.1), pålegg fra Datatilsynet (punkt 4.2), forhold knyttet til informasjonssikkerhet og internkontroll (punkt 4.3), databehandlerens bruk av underdatabehandler (punkt 4.4), databehandlerens erstatningsansvar og straff ved overtredelse av regelverket (punkt 4.5).

I punkt 5 behandles bruk av databehandler i andre land enn der den behandlingsansvarlige holder til, herunder overføring av personopplysninger over landegrensene.

2 Personopplysningslovens virkeområde og system

2.1 Personopplysningsloven og behandling av personopplysninger

Behandling av personopplysninger reguleres i norsk rett av personopplysningsloven[3] (POL) og personopplysningsforskriften[4] (POF), som begge gjennomfører EUs personverndirektiv[5] (PVD).

Data som inneholder opplysninger som direkte eller indirekte kan knyttes til en bestemt person (som omtales som «registrerte»[6]), er å regne som «personopplysninger» etter POL § 2 nr. 1. En «databehandler» er den som behandler personopplysninger på vegne av den behandlingsansvarlige, jf. POL § 2 nr. 5. Den «behandlingsansvarlige» er den som bestemmer formålet med behandlingen av personopplysninger, og hvilke virkemidler som skal brukes ved behandlingen, jf. POL § 2 nr. 4, og dermed den som er hovedansvarlig for at personopplysningsloven etterleves ved behandling av personopplysninger; se nærmere i punkt 2.4 nedenfor.

Enhver bruk av personopplysninger er å anse som «behandling» av personopplysninger, og omfattes dermed av virkeområdet for POL, jf. POL § 2 nr. 2. Forståelsen av slik «behandling» er i forarbeidene til POL[7] presisert til å være «*enhver form for formålsrettet håndtering av personopplysninger […] – den [dvs. behandlingen] utføres for å oppnå et bestemt resultat*». PVD inneholder ingen tilsvarende forutsetning som POL om å «*oppnå et bestemt resultat*». Ettersom PVD ikke oppstiller et slikt vilkår, er det imidlertid tvilsomt om det er grunnlag for å oppstille et slikt tilleggsvilkår.

Personvernforordningen inneholder ikke et eksplisitt krav til formålsrettet behandling, men gjennom at det kreves at personopplysninger kun skal inn-

3. Lov om behandling av personopplysninger av 14. april 2000 nr. 31.
4. Forskrift om behandling av personopplysninger (personopplysningsforskriften) av 15. desember 2000 nr. 1265.
5. Europaparlaments- og rådsdirektiv 95/46/EF av 24. oktober 1995 om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og fri utveksling av slike opplysninger (personverndirektivet).
6. Den fysiske person som personopplysningene kan knyttes til, se POL § 2 nr. 6.
7. Se kommentarene til § 2 nr. 2 i kapittel 16 i Ot.prp. nr. 92 (1998–99).

samles til uttrykkelige og legitime formål, gjelder det implisitt et krav til formålsrettet behandling også i forordningen, se artikkel 5 nr. 1 bokstav b.

Bruk av databehandler er regulert i POL § 15 som omhandler databehandlerens rådighet over personopplysningene. I personregisterloven[8] kapittel 6, som POL § 15 erstattet, var en databehandler en som *bearbeidet* personopplysninger for andre ved bruk av elektroniske hjelpemidler.[9] Det at den behandlingsansvarlige kan benytte en ekstern medhjelper til behandling av personopplysninger – utover kun bearbeidelse – var derfor nytt i POL,[10] og databehandleren kan nå forestå all behandling av personopplysninger som den behandlingsansvarlige selv har anledning til etter loven. En klar forskjell mellom de to lovene er imidlertid at personregisterloven ikke omfattet passiv behandling, som ren oppbevaring/lagring av opplysningene,[11] mens dette omfattes av POL. Man må imidlertid være forsiktig med å legge praksis vedrørende personregisterloven generelt til grunn for forståelsen av POL, siden POL innebar omfattende endringer i rettstilstanden ved implementeringen av PVD.

Med «databehandling» forstås behandling av personopplysninger som utføres av en annen fysisk eller juridisk person etter avtale med den behandlingsansvarlige. Skal det foreligge behandling som reguleres av POL, må det gjelde behandling av personopplysninger helt eller delvis med elektroniske hjelpemidler, jf. POL § 3 (1) bokstav a, eller behandling av personopplysninger manuelt hvor opplysningene inngår eller skal inngå i et personregister, jf. § 3 (1) bokstav b.[12]

I POL, i motsetning til den tidligere personregisterloven, er ett enkeltstående oppdrag tilstrekkelig til at POLs regler om databehandlere kommer til anvendelse.[13] Hovedbestemmelsen om databehandlers råderett over personopplys-

8. Lov om personregistre m.m. av 9. juni 1978 nr. 48, som ble opphevet ved ikrafttredelsen av personopplysningsloven i 2001.
9. Se personregisterloven § 22 (1).
10. Se s. 96 i Johansen, Michal Wiik, Knut-Brede Kaspersen og Åste Marie Bergseng Skullerud (2001), *Personopplysningsloven. Kommentarutgave*, Universitetsforlaget.
11. Ot.prp. nr. 92 (1998–99) s. 103.
12. Eksempel på sistnevnte vil være foretak som forestår spørreundersøkelser.
13. Se s. 136 i Johansen, Michal Wiik, Knut-Brede Kaspersen og Åste Marie Bergseng Skullerud (2001), *Personopplysningsloven. Kommentarutgave*, Universitetsforlaget.

ningene i POL § 15 er en videreføring av personregisterloven § 23, men har fått videre betydning i POL siden «databehandler» i POL forstås mer generelt enn «databehandlerforetak» som ble benyttet i personregisterloven.[14]

Med «databehandlerforetak» siktet man til en virksomhet som hadde som formål å bearbeide personopplysninger for andre gjennom bruk av elektroniske hjelpemidler. Slik virksomhet krevde konsesjon fra Datatilsynet, som ble omtalt som «samtykke» i personregisterloven, og personregisterloven gjaldt kun databehandlere som drev i så stort omfang med databehandling at dette var å anse som en «virksomhet».

POL setter i utgangspunktet ingen skranker for at databehandler behandler «sensitive»[15] personopplysninger.[16] Datatilsynet kan imidlertid sette vilkår for bruk av databehandler i konsesjonsvilkårene for behandling av sensitive personopplysninger. Tilsvarende gjelder etter personvernforordningen.

Den bærende legislative begrunnelsen for den omfattende reguleringen i personopplysningsloven, er å verne de registrerte individer mot at deres personopplysninger benyttes på en måte som krenker deres personvern, herunder hensynet til de registrertes personlige integritet og privatlivets fred, se POL § 1 og PVD artikkel 1 nr. 1. Her finner vi også den legislative begrunnelsen for å regulere databehandlers behandling av personopplysninger på vegne av behandlingsansvarlige; de registrertes rettigheter skal ivaretas like godt *som om* den behandlingsansvarlige selv utførte databehandlingen. Dette fremgår gjennom at POL krever at det inntas regulering av informasjonssikkerhetstiltakene i databehandleravtalen, se POL § 15 og punkt 3.2 nedenfor, og at den vesentligste forpliktelsen databehandleren er direkte pålagt etter loven, er å sørge for tilfredsstillende informasjonssikkerhet, se POL § 13 og punkt 4.3 nedenfor. Et hovedhensyn bak POLs regulering av databehandlers behandling av personopplysninger er nettopp å ivareta hensynet til informasjonssikkerhet.

---

14. Ot.prp. nr. 92 (1998–99) s. 116.
15. Sensitive personopplysninger omfatter opplysninger om rasemessig eller etnisk bakgrunn, eller politisk, filosofisk eller religiøs oppfatning, at en person har vært mistenkt, siktet, tiltalt eller dømt for en straffbar handling, helseforhold, seksuelle forhold, eller medlemskap i fagforeninger, jf. POL § 2 punkt 8.
16. Se s. 136 i Johansen, Michal Wiik, Knut-Brede Kaspersen og Åste Marie Bergseng Skullerud (2001), *Personopplysningsloven. Kommentarutgave*, Universitetsforlaget.

2.2 Adgangen til å benytte databehandler

Adgangen til å benytte databehandler er bare indirekte regulert i POL. Det følger av definisjonen av databehandler i POL § 2 nr. 2 at en databehandler behandler personopplysninger *«på vegne av»* den behandlingsansvarlige. Og i POL § 15 forutsettes det at den behandlingsansvarlige kan benytte en databehandler til å behandle personopplysninger.

Det eneste formelle kravet *for å kunne benytte* databehandler, er at det må foreligge en skriftlig avtale mellom den behandlingsansvarlige og databehandleren (databehandleravtale), jf. POL § 15. I dette ligger det også et krav om at den behandlingsansvarlige eksplisitt har tilkjennegitt at denne skal benytte databehandler, og at slik tilkjennegivelse skal skje gjennom inngåelse av en databehandleravtale.[17]

Det er også et krav i POL § 15 (2) om at databehandleravtalen regulerer sikringstiltak som følger av POL § 13; se punkt 3 nedenfor.

Det eneste formelle kravet som oppstilles i POL *for å kunne være* databehandler, er at man følger kravene til sikringstiltak etter POL § 13; se nærmere i punkt 4.3. Disse kravene skal inntas i databehandleravtalen, jf. ovenfor, og det følger forutsetningsvis av POL § 15 at databehandleren plikter å etterleve databehandleravtalen. Det kreves altså ikke, som i den tidligere personregisterloven, at man har samtykke eller konsesjon til behandlingen. Databehandlerens behandling vil derfor være avledet fra den behandlingsansvarliges lovmessige grunnlag for behandlingen og rammene for behandlingen: Såfremt den behandlingsansvarlige kan behandle opplysningene, kan i utgangspunktet også databehandleren gjøre det.

Den kommende forordningen stiller mer omfattende krav til bruk av databehandler enn det gjøres etter gjeldende norsk rett, se forordningens artikkel 28. Det er et grunnleggende vilkår etter forordningen at det kun benyttes databehandler som stiller tilstrekkelige garantier for at databehandleren vil oppfylle de tekniske og organisatoriske kravene til behandling som er nedfelt i forordningen. Hva som menes med *«stille tilstrekkelige garanti»*, er noe uklart etter forordningen, men at det etableres en skriftlig avtale hvor databehandleren påtar seg

17. NOU 1997: 19 s. 133.

ansvaret eksplisitt med de krav som forordningen stiller til databehandleravtalen, se punkt 3 nedenfor, må være et minimumskrav. I tillegg legger forordningen til grunn at det skal foretas en vurdering av om databehandleren har stilt nødvendige garantier, hvor det forhold at databehandleren overholder adferdsreglement etter artikkel 40 eller er sertifisert etter sertifiseringsordning behandlet i artikkel 42, inngår som kriterier, se artikkel 28 nr. 5.

Det er ikke anledning til å behandle personopplysninger, herunder å benytte databehandler, uten at vilkårene for databehandling i POL er oppfylt. Det er derfor avgjørende at det foreligger et i loven angitt grunnlag for behandlingen.[18] Det er den behandlingsansvarliges ansvar at det foreligger et slikt grunnlag. Skjer databehandling etter avtale med den behandlingsansvarlige, vil i utgangspunktet ikke databehandleren anses som ansvarlig dersom behandlingen skjer uten at det foreligger grunnlag etter loven. Det kan i utgangspunktet heller ikke påhvile databehandleren noe ansvar for å forespørre den behandlingsansvarlige om grunnlaget, eller kontrollere om grunnlaget for behandlingen er tilfredsstillende, med mindre det skulle være forhold som tyder på at den behandlingsansvarlige mangler et slikt grunnlag.

En databehandler vil bare kunne behandle personopplysninger på den behandlingsansvarliges vegne. Den behandlingen som databehandleren kan utføre, vil derfor være begrenset til den som den behandlingsansvarlige selv kan utføre, med de eventuelle særskilte begrensninger som følger av databehandleravtalen. Ettersom grunnlaget for databehandlerens behandling er avledet av den behandlingsansvarliges behandling, kreves det ikke et eget grunnlag eller samtykke fra de registrerte for at den behandlingsansvarlige skal kunne benytte seg av databehandler.

2.3 Ingen meldeplikt om bruk av databehandler

Det er i utgangspunktet ingen plikt til å melde til Datatilsynet at databehandling helt eller delvis *utføres av databehandler*. Dette er vel en konsekvens av at loven forutsetter at databehandleren bare kan utføre behandling som den behandlingsansvarlige selv kan utføre.[19] Ifølge loven innebærer altså ikke bruk

18. POL § 11 bokstav a, jf. §§ 8 og 9.
19. Merk at annet kan følge av konsesjonsvilkårene dersom behandlingen skjer på grunnlag av konsesjon.

av databehandler utlevering eller overføring av personopplysninger som nødvendiggjør melding eller annen informasjon til Datatilsynet.

Dette i motsetning til en *overdragelse* av personopplysninger til annen tredjepart, hvor sistnevnte anses som selvstendig behandlingsansvarlig. Det er også presisert i enkelte av konsesjonene fra Datatilsynet, hvor det er inntatt i konsesjonsvilkårene at behandling av personopplysninger hos et databehandlingsforetak ikke regnes som utlevering når dette skjer på oppdrag fra den behandlingsansvarlige. Dersom overføringen skjer over landegrensene, er det imidlertid visse krav; se punkt 5.4 nedenfor.

Selv om *bruk av databehandler* ikke må meldes, kan det foreligge plikt til å melde *selve* behandlingen som den behandlingsansvarlige forestår (som da eventuelt skal utføres ved databehandler), jf. POL § 31. Må behandlingen meldes, skal meldingen også inneholde informasjon om eventuell databehandler som behandlingsansvarlig vil benytte seg av; se POL § 32 bokstav a.

Det er uklart om den behandlingsansvarlige plikter å sende ny melding dersom det besluttes å benytte databehandler etter oppstart av behandlingen, siden bruk av databehandler ikke medfører noen endring i behandlingen som ville ha krevd melding etter POL § 31 (1) første punkt. Direktivet gir ingen veiledning ettersom kravet til å opplyse om databehandler i meldingen ikke følger av direktivet, se artikkel 19 nr. 1 som POL § 32 er basert på, og forarbeidene gir ingen anvisning på hvorfor denne særnorske løsningen er valgt.[20]

Datatilsynet etterprøver ikke informasjon som mottas om bruk av databehandler, og bruk av databehandler har ingen betydning for ansvaret eller pliktene ved behandlingen. Det må på denne bakgrunn være tilstrekkelig at den behandlingsansvarlige gir beskjed til Datatilsynet om bruk av databehandler, f.eks. ved endring av meldingen.

Det å melde behandlingen av personopplysninger til Datatilsynet, dersom slik meldeplikt foreligger, jf. POL § 31, vil ofte kunne overlates til databehandleren. Er det den behandlingsansvarlige som gir melding, må også den behandlingsansvarlige informere databehandleren når behandlingen kan ta til, siden databehandleren først kan påbegynne behandlingen på samme tidspunkt som

20. Kravet om å oppgi databehandler ble inntatt i Ot.prp. nr. 92 (1998–99), men var ikke en del av det opprinnelige lovforslaget i NOU 1997: 19.

den behandlingsansvarlige ville ha kunnet om denne foresto behandlingen selv, dvs. tidligst 30 dager etter at melding er innsendt, jf. POL § 31 (2). Krever behandlingen konsesjon, enten ved at det behandles sensitive personopplysninger eller behandlingen ellers åpenbart vil krenke tungtveiende personverninteresser, se POL § 33 (2), kan behandlingen først påbegynnes når konsesjon foreligger.

Datatilsynet kan i forbindelse med konsesjon sette vilkår for hvordan personopplysningene behandles, se POL § 35, og kan også nedlegge forbud mot bruk av databehandler eller sette begrensninger for databehandlers behandling av personopplysninger. Datatilsynet vil også kunne nedlegge forbud mot at databehandler benytter seg av underdatabehandlere for å behandle personopplysninger, se punkt 4.4 nedenfor.

2.4 Forholdet mellom den behandlingsansvarlige og databehandleren

Det fremgår av POL § 2 nr. 4 at databehandleren står i et oppdragsgiverforhold til den behandlingsansvarlige. Dette innebærer at sistnevnte har instruksjonsmyndighet og ansvaret for databehandlerens behandling av personopplysninger.

Databehandleren har ikke ansvar for behandlingen av personopplysningene utover å behandle personopplysningene innenfor det som er skriftlig avtalt med den behandlingsansvarlige, og å etterkomme informasjonssikkerhetskravene i POL § 13. Det som den behandlingsansvarlige kan bestemme, er bl.a. hvilke *«hvilke hjelpemidler som skal brukes»* til behandlingen av personopplysninger, og med «hjelpemidler» omfattes å beslutte hvem som skal være databehandler.[21]

Definisjonene av databehandler og behandlingsansvarlig som er inntatt i POL § 2, tilsvarer i det vesentlige PVDs (og forordningens) definisjoner. Definisjonen av databehandler er ikke spesielt utførlig verken i POL eller PVD, og beskrives, som vi har sett, kun funksjonelt gjennom de handlinger som databehandleren gjør (*«behandler personopplysninger»*) gjennom forholdet til den behandlingsansvarlige (*«på vegne av»*). Tilsvarende gjelder etter PVD,

21. Se s. 273 i Olsen, Thomas (2015), «Personvernøkende identitetsforvaltning», *Complex* 2/2015.

hvor databehandler defineres i artikkel 2 bokstav e, og i artikkel 7 nr. 2 og 3 – som har overskriften «Sikkerhet ved behandling» – og det er inntatt krav til databehandleren uten at det fremgår eksplisitt at behandlingsansvarlig kan benytte seg av en databehandler. Både loven og direktivet omtaler således kun virkningene av og kravene til bruk av databehandler, men regulerer ikke direkte retten til å benytte seg av databehandler og eventuelle begrensninger i bruken av databehandler.

Tilsvarende gjelder forordningen, hvor kravene til bruk av databehandler følger av artikkel 28, mens det forutsettes at databehandler kan benyttes gjennom definisjonen av databehandler i artikkel 4 nr. 8.

Databehandlerrollen fremgår dermed implisitt av begrepet «behandlingsansvarlig» i POL: Først beskrives databehandleren gjennom den negative avgrensningen mot den behandlingsansvarlige. Deretter beskrives databehandlerens plikter gjennom den behandlingsansvarliges plikter, siden databehandleren kan pålegges de samme pliktene som den behandlingsansvarlige (men ikke mer omfattende plikter). Om grensedragningen mellom behandlingsansvarlig og databehandler, se nærmere i punkt 3.2 nedenfor.

Selv om det er få formelle krav til bruk av databehandler, er det klare utgangspunktet i POL og PVD at den behandlingsansvarlige er ansvarlig for databehandlerens behandling av personopplysningene. Dette ansvarsforholdet videreføres i personvernforordningen, se forordningen artikkel 5 nr. 2. Den behandlingsansvarlige er derfor forpliktet til å velge en databehandler som kan oppfylle kravene som stilles til databehandler, jf. ovenfor.

Når en databehandler er valgt og benyttes, har den behandlingsansvarlige en løpende oppfølgningsplikt overfor databehandleren,[22] og oppfølgningen skal, som nevnt, bl.a. gjennomføres ved etablering av en databehandleravtale, se punkt 3 nedenfor, som regulerer pliktene for databehandleren. I tillegg skal den behandlingsansvarlige påse at tekniske sikkerhetstiltak og organisatoriske tiltak under behandlingen overholdes av databehandleren, se nærmere beskrivelse i punkt 4.3 nedenfor.[23] Den behandlingsansvarliges oppfølgingsansvar er nærmere behandlet i punkt 4.7 nedenfor.

22. Jf. PVD artikkel 17 (2).
23. Jf. PVD artikkel 17 (2) i.f.

Mens personregisterloven kun regulerte «databehandlerforetak», altså juridiske personer, kan en databehandler etter POL også være en fysisk person.

Selv om det ikke uttrykkelig fremgår av POL, må det være adgang til å benytte to eller flere behandlingsansvarlige for behandling av samme personopplysninger, se PVD[24] og forarbeidene til POL[25]. At to anses å være behandlingsansvarlig sammen, medfører at begge har ansvar for å overholde POLs regler, samt at begge kan være ansvarlig erstatnings- og strafferettslig, se punkt 4.3 nedenfor. Det kan heller ikke være noe til hinder for å bruke to eller flere behandlingsansvarlige til å behandle ulike deler av personopplysningene, eventuelt i ulike faser av behandlingen.[26]

Personvernforordningen har egne regler om flere eller felles behandlingsansvarlige, se artikkel 26. Forordningen omhandler det spesielle problemet ved at det kan være behandlingsansvarlige i ulike jurisdiksjoner, og etter forordningen kan de registrerte velge å forholde seg til én av de behandlingsansvarlige for utøvelse av sine rettigheter.

PVD definerer «tredjemann» som andre enn «*den registrerte, den behandlingsansvarlige, databehandleren og de personer som under den behandlingsansvarliges eller databehandlerens direkte myndighet har fullmakt til å behandle opplysningene*».[27] Det følger altså en avgrensning av de definerte aktørene mot «de øvrige» etter direktivet. Bestemmelsen ble ikke innført i POL, siden departementet ikke fant behov for en generell definisjon av tredjepart.[28] Direktivet legger også begrensninger på overføring til tredjemann, og de samme begrensningene må gjelde etter norsk rett, men er altså implementert i norsk rett bl.a. ved at databehandler ikke kan overlate personopplysninger til tredjemann («noen andre» i POL § 15) uten at

24. Se direktivets artikkel 2 bokstav d.
25. Ot.prp. nr. 92 (1998–99) kapittel 16 i kommentarene til § 2 nr. 4.
26. Se Artikkel 29-gruppens opinion 1/2010 på s. 33. Artikkel 29-gruppen er en arbeidsgruppe sammensatt av bl.a. representanter fra personvernmyndighetene fra de enkelte medlemsland i EU, og har fått navnet sitt etter artikkel 29 i PVD som hjemler gruppens etablering og virke. Artikkel 29-gruppen gir råd til kommisjonen om tolkning og utdypning av PVD, og kommisjonen følger normalt gruppens råd. Artikkel 29-gruppen vil bli erstattet av «European Data Protection Board» etter personvernforordningen, se forordningens artikkel 68 flg. Selv om dette er retningslinjer fra EUs rådgivende organ, legger både EU-kommisjonen og Datatilsynet stor vekt på Artikkel 29-gruppens anbefalinger og retningslinjer.
27. PVD artikkel 2 bokstav f.
28. Ot.prp. nr. 92 (1998–99) kommentar til § 2 i kapittel 16.

dette er skriftlig avtalt med behandlingsansvarlige. Bruken av begrepet «tredjepart» innføres nå som en del av forordningen, se dennes artikkel 4 nr. 10.

3 Databehandlingens omfang og betydning av databehandleravtalen

3.1 Legale og avtalte skranker for databehandlerens behandling

3.1.1 Databehandlerens adgang til å forestå behandling er avledet

POL setter, som nevnt, skranker for den behandlingsansvarliges egen behandling av personopplysninger. Ettersom databehandleren utfører behandling «*på vegne av den behandlingsansvarlige*», jf. POL § 2 nr. 5, gjelder disse skrankene også som en *ytre ramme* for hvilken behandling databehandleren kan utføre på vegne av den behandlingsansvarlige. Databehandleren kan derfor ikke behandle personopplysninger i større utstrekning enn den behandlingsansvarlige selv har anledning til; se punkt 2.4 ovenfor. Dette er en absolutt begrensning for databehandlerens behandling av personopplysninger.

I POL § 15 er ikke det generelle begrepet «*behandling*» benyttet som ellers i POL, men kun de mer begrensede aktivitetene «*lagring eller bearbeidelse*». Et nærliggende spørsmål er da om denne presiseringen innebærer at databehandleren kan behandle personopplysninger på annen måte enn ved lagring og bearbeidelse uten at det foreligger avtale med den behandlingsansvarlige. I forarbeidene til bestemmelsen heter det at presiseringen er inntatt «for ordens skyld», slik at denne for så vidt er unødvendig.[29] Dette kan forstås slik at presiseringen ikke innebærer mer enn det som følger av første setning i bestemmelsen. Etter den systematikk som ellers gjelder i loven ved at databehandleren kun handler på vegne behandlingsansvarlige, må bestemmelsen derfor forstås slik at denne ikke gir noe unntak fra behandling som ikke er regulert av databehandleravtalen, og bestemmelsen kan heller ikke forstås som noen innskrenkning i den behandlingsansvarliges bruk av databehandler ved at databehandleren kun skal forestå «lagring eller bearbeidelse» av personopplysninger.

29. Ot.prp. nr. 92 (1998–99) s. 116.

3.1.2 Begrensninger i delegasjonsadgangen

I tillegg til de nevnte legale skrankene kan ytterligere skranker for databehandlerens databehandling følge av databehandleravtalen mellom databehandleren og den behandlingsansvarlige, jf. POL § 15. I stedet for en direkte regulering av databehandlerens plikter er altså POLs ordning at forholdet mellom behandlingsansvarlige og databehandleren skal reguleres gjennom en slik avtale.

Databehandleren kan i utgangspunktet utføre all behandling av personopplysninger som den behandlingsansvarlige kan foreta. Den behandlingsansvarlige kan derimot ikke delegere sitt ansvar eller myndighet som behandlingsansvarlig *som sådan* til databehandleren, selv om databehandleren etter databehandleravtalen også kan utføre visse oppgaver knyttet til ansvaret og myndigheten. Forpliktelser som den behandlingsansvarlige har overfor tredjepart, spesielt registrerte og Datatilsynet, kan databehandleren utføre, men ansvaret for om og hvordan forpliktelsene ivaretas, vil fortsatt påhvile den behandlingsansvarlige. Det kan også delegeres til databehandleren å avgjøre hvem som skal være underdatabehandler; se punkt 4.4 nedenfor.

Enkelte forpliktelser kan etter sin art ikke delegeres til databehandleren, eksempelvis plikten til å sørge for at grunnkravene etter POL § 11 til behandling er oppfylt før behandlingen tar til. Dette følger av lovens skille mellom behandlingsansvarlig og databehandler, se POL § 2 nr. 4 og 5 og nærmere nedenfor i punkt 3.2 om grensedragningen mellom den behandlingsansvarlige og databehandleren. Det kan heller ikke delegeres til databehandleren å bestemme hvilke hjelpemidler som skal benyttes i databehandlingen.

Etter personvernforordningen vil tilsynsmyndigheter som Datatilsynet få en utvidet rådgivningsplikt overfor behandlingsansvarlige og databehandlere. Dette gjelder både før og etter at det avdekkes overtredelse av regelverket, se forordningens artikkel 36. Datatilsynets holdning til behandlingen vil derfor i større grad enn tidligere bli avklart *før* den iverksettes eller tiltak settes inn i en allerede pågående behandling. Dette vil sikre større forutsigbarhet for de berørte.

Det er bare den behandlingsansvarlige som kan fastsette formålet med behandlingen, jf. POL § 2 nr. 4; dette kan ikke delegeres til databehandleren. Personopplysninger kan ikke benyttes til et annet formål enn det som var formålet da opplysningene ble innsamlet, jf. POL § 11 bokstav b, og formålet kan ikke

fritt endres etter innsamling av opplysningene.[30] Dette innebærer at databehandleren bare kan behandle personopplysningene innenfor formålet som ligger til grunn for behandlingen, hvilket gjelder uavhengig av hva som er avtalt med den behandlingsansvarlige. Det er imidlertid den behandlingsansvarlige som må informere databehandleren om formålet, og som er ansvarlig dersom databehandleren behandler opplysningene utenfor formålet.

Det er også den behandlingsansvarlige som har ansvaret for at de opplysninger som behandles, er tilstrekkelige og relevante for formålet,[31] og at personopplysningene ikke lagres lenger enn nødvendig ut fra formålet med behandlingen.[32]

POL gjelder ikke for behandling av personopplysninger som foretas til rent personlige eller andre private formål, jf. POL § 3 (3). Benytter man en databehandler som gjør tilgjengelig midler for behandling av personopplysninger til personlige eller private formål, vil databehandleren være underlagt personopplysningsloven, og det at databehandleren utfører databehandling for privatpersoner, vil kunne frita databehandleren fra lovens regler.[33]

Etter personregisterloven kunne databehandlervirksomhet bare skje med konsesjon fra Datatilsynet («samtykke»). Dette satt stramme rammer for overlatelsen av personopplysninger til andre for behandling, og følgen var at man forsøkte å definere inn konsulenter og andre som å være en del av virksomheten til den behandlingsansvarlige.[34] Utvidelsen i adgangen til å benytte databehandler som kom i POL, dekket dermed et praktisk behov for mer lempelige regler.

30. Se POL § 11 bokstav c.
31. Se POL § 11 bokstav d.
32. Se POL § 11 bokstav e.
33. Slik også personvernforordningen, se punkt 18 i fortalen.
34. Se Johansen, Michal Wiik, Knut-Brede Kaspersen og Åste Marie Bergseng Skullerud (2001), *Personopplysningsloven. Kommentarutgave*, Universitetsforlaget, s. 137.

3.2 Grensedragningen mellom den behandlingsansvarlige og databehandleren

3.2.1 Grensedragningens betydning

Den behandlingsansvarlige har det vesentlige ansvaret for behandling av personopplysninger etter POL og PVD, se punkt 2.2 ovenfor, og den behandlingsansvarlige har instruerende myndighet over databehandleren. Skillet mellom den behandlingsansvarlige og databehandleren er derfor avgjørende for hvem som har det overordnede ansvaret og hvem som har instruksjonsmyndighet.

Artikkel 29-gruppen har oppstilt retningslinjer for grensedragningen.[35] Etter retningslinjene er hovedhensikten med rollen som behandlingsansvarlig å allokere ansvar og forpliktelser for overholdelse av personvernreglene. Motsetningsvis viser dette at databehandlerens direkte forpliktelser etter lovverket er begrenset til kravene til informasjonssikkerhet i POL § 13. Hvilket ansvar og plikter databehandleren har i henhold til avtale som er inngått med den behandlingsansvarlige, er noe annet, se punkt 3.3 nedenfor om databehandleravtalen.

3.2.2 Betydningen av organisatorisk skille

POL benytter begrepet «databehandler» som avgrensning av rollen mot den behandlingsansvarlige, ved at databehandleren er en person eller virksomhet som *ikke* er del av den behandlingsansvarliges organisasjon. Dette forutsetter at det er et organisatorisk skille mellom den behandlingsansvarlige og databehandleren. Foreligger det ikke et slikt skille, vil det være identifikasjon mellom databehandler og den behandlingsansvarlige, og følgelig ingen behandling «på vegne av» den behandlingsansvarlige og ikke noe databehandlerforhold.

Av personregisterloven[36] fremgikk det forutsetningsvis at konsernselskap som behandlet personopplysninger for annet selskap i konsernet, skulle anses som en databehandler. Det er ikke noe i forarbeidene til POL som tyder på at POL her medførte en endring. En databehandler må derfor fortsatt kunne

35. Art. 29 Data Protection Working Party: Opinion 1/2010 on the concepts of «controller» and «processor» av 16. februar 2010 se: http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/.
36. Se § 22 (2) i loven.

være en del av samme konsern som den behandlingsansvarlige. Forutsetningen må imidlertid fortsatt være at databehandler og den behandlingsansvarlige er separate juridiske enheter, og at den behandlingsansvarlige ikke har instruksjonsmyndighet overfor databehandleren utover det som følger av databehandlerforholdet.

Etter forskrift om personregistre av 21. desember 1979 gitt i medhold av personregisterloven ble et forvaltningsorgan (som definert i forvaltningsloven § 1) som bearbeider personopplysninger for andre over-, under- eller sideordnede organer i samme etat, ikke regnet som databehandler. Tilsvarende gjaldt for forvaltningsorgan som bearbeider opplysninger for «kollegiale organer, sakkyndige eller tilsynsførere mv.» som var tilknyttet etaten, eller for private som er engasjert for å løse oppgaver for etaten, eller når forvaltningsorganet bearbeider personopplysninger som det mottok fra andre forvaltningsorganer, dersom bearbeidingen hovedsakelig skjedde ut fra organets eget behov, eller for kollegiale organer mv. som nevnt. Dette gjaldt selv om bearbeidede personopplysninger ble sendt tilbake til det organ som forvaltningsorganet mottok opplysningene fra.

Dagens lov har et videre virkeområde, og på bakgrunn av at POL er basert på PVD, må man være forsiktig med å legge personregisterloven med forskrifter til grunn for tolkning av POL. Av denne grunn bør samme forståelse som gjelder for private virksomheter, legges til grunn slik at også forvaltningsorganer som behandler personopplysninger for andre organer, kan anses som databehandler for førstnevnte, forutsatt at det er et organisatorisk skille mellom organene eller enhetene slik at det er klart at den ene enheten behandler personopplysninger *«på vegne av»* den andre.

Det har vært fremholdt at dersom den behandlingsansvarlige har instruksjonsrett over databehandleren før det etableres et databehandlerforhold, er det ikke tale om et databehandlerforhold.[37] Dette er nok en for streng forståelse av kravet til selvstendighet, siden en databehandler kan utføre behandlingstjenester *«på vegne av»* behandlingsansvarlig i henhold til POL § 2 nr. 5, uten at det foreligger instruksjonsrett etter avtale. Det må være tilstrekkelig at det er et organisatorisk skille mellom databehandleren og den behandlingsansvarlige, eksempelvis at det er to separate juridiske enheter. At det er et konsernmessig

37. Dag Wiese Schartum i kommentarer til POL i Gyldendal Rettsdata.

forhold ved at eksempelvis den behandlingsansvarlige eier databehandleren og dermed kan påvirke databehandler gjennom generalforsamling eller styre som eier, vil i denne sammenheng trolig ikke være nok til at det anses å være en identifikasjon mellom selskapene.

3.2.3 Betydningen av hvem som bestemmer formålet og hjelpemidler

Etter reguleringen i POL er det avgjørende for at en skal anses som behandlingsansvarlig, at en har den avgjørende myndighet til å *bestemme formålet* med behandlingen samt avgjøre *hvilke hjelpemidler* som skal benyttes.[38]

Når det gjelder det første vilkåret, kan formålet med behandlingen bestemmes direkte av lovverket parten er underlagt (som for teleoperatører), eller det kan følge implisitt av lovverket som den behandlingsansvarlige er underlagt (som for arbeidsgivere). Det er klart at selv om formålet for behandlingen av personopplysningene følger av lovverket som parten er underlagt, og den behandlingsansvarlige er forpliktet til å behandle personopplysningene, vil denne være å anse som behandlingsansvarlig. Det avgjørende for skillet mellom den behandlingsansvarlige og databehandleren blir dermed *hvem* av partene som er direkte underlagt det aktuelle regelverket som pålegger behandling av personopplysninger.

Dersom databehandleren har bestemmelsesrett over behandlingen av personopplysningene utover den bestemmelsesrett som kan avtales etter POL, vil dette medføre at databehandleren anses som behandlingsansvarlig for hele eller deler av behandlingen; alternativt kan databehandleren og den behandlingsansvarlige sammen bli ansett som behandlingsansvarlig. Tilsvarende vil gjelde dersom databehandleren går utover de rettigheter og rammer denne har etter POL og databehandleravtalen, og dermed blir å anse som behandlingsansvarlig for behandlingen som overtredelsen av databehandleravtalen omfatter. Dette er eksplisitt regulert i personvernforordningen, se artikkel 28 nr. 10, men det er ingen tilsvarende regulering i POL eller PVD.

38. Jf. definisjonen av «behandlingsansvarlig» i POL § 2 punkt 4.

3.2.4 Betydningen av delegasjon

Databehandleren må i noen grad kunne bestemme hvordan opplysningene skal behandles, uten at dette uten videre medfører at databehandleren må anses som behandlingsansvarlig. En behandlingsansvarlig vil ofte benytte en databehandler på grunn av sistnevntes kompetanse i behandling av data, og det vil derfor, som nevnt, ofte være naturlig at det overlates til databehandleren å treffe visse beslutninger – som en del av tjenestene som databehandleren tilbyr som databehandler. Eksempelvis vil databehandleren kunne ta beslutninger av teknisk og organisatorisk art, mens mer vesentlige beslutninger som har betydning for lovligheten av behandlingen, som hvilke data som skal behandles, hvor lenge dataene skal oppbevares, utlevering av data til tredjeparter mv., er beslutninger som må fattes av den som er behandlingsansvarlig. Tilsvarende kan databehandleren treffe beslutninger om tiltak for informasjonssikkerhet og sikring av personopplysningene ettersom det er overlatt til databehandleren å gjennomføre sikringstiltak etter POL § 13.[39]

3.2.5 Betydningen av at databehandleren bidrar med verdiøkende tjenester

Tilfører databehandleren verdiøkende tjenester til personopplysningene, eksempelvis kvalitetssikring av personopplysningene mot tredjeparts data, kan dette tale for at databehandleren selv eller sammen med behandlingsansvarlig anses som behandlingsansvarlig, enten for hele behandlingen eller for den del av behandlingen som medfører verdiøkning. I denne vurderingen vil det bl.a. være av betydning hvor gjennomgripende de verdiøkende tjenestene er for personopplysningene.[40] Foretas det bare ren kvalitetssikring av dataene som ved bruk av adressemeglere, dvs. foretak som mottar adressedata fra behandlingsansvarlig og bistår med utsendelse av adressert markedsmateriell og foretar kontroll av listene mot det sentrale reservasjonsregisteret, døderegisteret og andre registre, vil dette være å anse som en ren databehandlertjeneste selv om det skjer en verdiøkning av dataene.

---

39. Dette følger av direktivets artikkel 17 nr. 2 hvor databehandler skal kun gi de nødvendige garantier med hensyn til tekniske sikkerhetstiltak og organisatoriske tiltak under behandlingen, mens behandlingsansvarlig må påse at disse tiltakene overholdes. Allikevel ble det i SWIFT-saken, se nedenfor, vektlagt at SWIFT selv bestemte sikkerhetstiltakene.
40. Dette var forholdet i SWIFT-saken som er omtalt nedenfor.

3.2.6 Betydningen av reguleringen i databehandleravtalen

Regulering av ansvarsforholdet mellom partene i databehandleravtalen er selvsagt ikke tilstrekkelig for at den ene skal anses som databehandler og den andre som behandlingsansvarlig. Det er de reelle forhold som er avgjørende.

Dette var tilfellet i SWIFT-saken hvor tema var om det globale bankmeldingsnettverket Society for Worldwide Interbank Financial Telecommunication (SWIFT) var å anse som behandlingsansvarlig ved krav om utlevering av personopplysninger til USAs finansdepartement. Artikkel 29-gruppen[41] ga en uttalelse[42] om SWIFTs personvernansvar, og fant at SWIFT var å anse som behandlingsansvarlig. I databehandleravtalen var SWIFT angitt som databehandler, men dette ble ikke ansett som *tilstrekkelig* i vurderingen av SWIFTs ansvar for overholdelse av personvernlovgivningen. Sentralt i SWIFT-saken var også det forhold at myndighetene hadde rett til å kreve utlevert data og informasjon fra en databehandler, medfører at denne skal anses som behandlingsansvarlig. Som påpekt nedenfor i punkt 4.2 antas det at databehandleren ikke er pålagt å følge pålegg fra Datatilsynet i visse tilfeller, og det må også antas at myndigheter i Norge ikke kan kreve data utlevert fra databehandlere, men må rette kravet mot den behandlingsansvarlige som så må instruere databehandleren om å utlevere opplysningene. Utleverer databehandleren personopplysninger direkte til tredjepart, vil dette kunne være i strid med databehandleravtalen (dersom denne ikke regulerer slik utlevering) og også i strid med databehandlerens plikter etter reglene om informasjonssikkerhet. Spørsmålet settes på spissen ved utlevering til andre staters myndigheter, som i SWIFT-saken, og det kan ikke sies at denne saken ga noe klart svar.

3.2.7 Betydningen av prosessuell handleevne

Behandlingsansvarlige kan etter POL være både fysiske og juridiske personer, gitt at sistnevnte har prosessuell partsevne.[43] Det kan imidlertid være gode grunner for at det må oppstilles som krav at databehandleren også har prosessuell partsevne, siden det ellers vil være vanskelig å få håndhevet krav mot databehandleren på grunnlag av databehandleravtalen eller annet grunnlag.[44]

---

41. Om Artikkel 29-gruppen, se note 26 ovenfor.
42. Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT) av 22. november 2006.
43. Ot.prp. nr. 92 (1998–99) s. 102
44. Se eksempelvis Personvernnemndas avgjørelse PVN-2008-1.

3.2.8 Betydningen av vederlag

Det er ikke krav etter POL om at databehandleren mottar vederlag for behandlingen av personopplysningene, for at behandlingen skal anses som databehandling. Etter PVD forutsettes det at databehandling foreligger *«dersom behandlingen utføres for [behandlingsansvarliges] regning»*.[45] Det fremgår ikke av forarbeidene til POL om lovgiver bevisst ikke ønsket at det skulle være et krav om vederlag for at det skal foreligge et databehandlerforhold. Problemstillingen er ikke spesielt praktisk, men dersom spørsmålet blir satt på spissen, som i f.eks. konsernforhold, vil man måtte vurdere det konkrete forhold. Det er nok lite praktisk at databehandlertjenester utføres vederlagsfritt uten at den som utfører tjenestene, har en egeninteresse i databehandlingen som medfører at denne må anses som behandlingsansvarlig.[46]

3.2.9 Betydningen av at databehandleren opptrer i eget navn

Hvorvidt databehandleren opptrer i eget navn eller i den behandlingsansvarliges navn ved kontakt med kunder og kontraktsmotparter av den behandlingsansvarlige, står sentralt i grensedragningen. Opptrer databehandleren som agent eller på annen måte som representant for den behandlingsansvarlige, vil dette være en sterk indikator på at denne er kun databehandler. Opptrer databehandleren i eget navn og for egen regning og risiko, vil det derimot normalt være egne personopplysninger som håndteres, slik at denne ikke kan anses som en databehandler.

Grensedragningen mellom den behandlingsansvarlige og databehandleren illustreres av Personvernnemndas avgjørelser i sakene PVN-2013-05, PVN-2013-08, PVN-2013-09, PVN-2013-10, PVN-2013-11 og PVN-2013-12 (avgjørelsene var likelydende i disse sakene siden de bygde på vesentlig samme faktum) hvor en utstyrsleverandør til helseforetak hadde, som følge av vedlikehold og overvåkning av utstyret, hentet ut helseopplysninger og overført disse til selskapets morselskap i USA. Spørsmålet var om helseforetakene som behandlingsansvarlige var forpliktet til å informere de berørte pasientene, hvilket Personvernnemnda

45. Se PVD artikkel 17 nr. 2.
46. Den svenske personuppgiftslagen har valgt en annen løsning, og en «personuppgiftsbiträde» (databehandler) er den som «behandlar personuppgifter för den personuppgiftsansvariges räkning», mens vederlag er ikke et krav i den danske persondataloven.

fant at det forelå plikt til. Avgjørelsene berører imidlertid også grensegangen mellom den behandlingsansvarlige og databehandler når databehandler foretar behandling av personopplysninger som ligger utenfor det som følger av databehandleravtalen. Avgjørelsene gjaldt vurderinger etter helseregisterloven, men er relevante også for forståelsen av personopplysningslovens regler. Om forholdet mellom den behandlingsansvarlige og databehandleren ble det tillagt betydning at det var den behandlingsansvarlige som ble pålagt varslingsplikten, og ikke utstyrsleverandøren som foretok den ulovlige uthenting av helseopplysninger. Avgjørelsene viser derfor at den behandlingsansvarlige fortsatt er ansvarlig selv om databehandleren behandler personopplysninger som ikke omfattes av databehandleravtalen, og den behandlingsansvarlige kan ikke fri seg fra ansvaret som behandlingsansvarlig ved å benytte databehandler.

Det er også et spørsmål om grensen mellom «medarbeidere» i POL §§ 13 og 14 og databehandler. Medarbeidere er personer som er underlagt den behandlingsansvarliges instruksjonsmyndighet,[47] og personer som ikke er å anse som behandlingsansvarliges medarbeidere eller databehandler, er å anse som tredjemann, se ovenfor.

I forordningen er det inntatt en presisering om at enhver som utfører arbeid for den behandlingsansvarlige, databehandleren eller noen som har tilgang til personopplysninger, bare kan behandle personopplysninger etter instruks fra den behandlingsansvarlige. Formålet er å fjerne enhver tvil om at noen som har tilgang til personopplysninger, er underlagt den behandlingsansvarliges instruks, se artikkel 29.

Etter helseregisterloven § 13 kan databehandler og den som arbeider under databehandlers instruksjonsmyndighet, gis tilgang til helseopplysninger kun i den grad det er nødvendig for vedkommendes arbeid og ikke medfører brudd på taushetsplikt. Bestemmelsen forutsetter at databehandleren utfører et selvstendig arbeid som ikke utledes av den behandlingsansvarlige, og omfatter at eksempelvis forskere fungerer som databehandlere, se Personvernnemndas avgjørelse 2007/01.

3.3 Krav til databehandleravtalens innhold

3.3.1 Innledning

POL oppstiller kun to krav til hva som skal reguleres i databehandleravtalen: Hvordan databehandleren skal behandle personopplysninger (§ 15 (1)), se

47. Se Olsen, Thomas (2015), «Personvernøkende identitetsforvaltning», *Complex* 2/2015, som gjennomgår nærmere grensedragningen mellom medarbeidere, databehandlere og tredjemann.

punkt 3.3.2 nedenfor, og databehandlerens plikt til å sørge for informasjonssikkerhetstiltak (§ 15 (2)), se punkt 3.3.3 nedenfor. Det er imidlertid regulering som etter forholdene må inntas i databehandleravtalen, samt annen regulering som bør inntas, se nærmere i punkt 3.6 nedenfor.

3.3.2 Regulering av behandlingen av personopplysninger

Siden databehandleren ikke kan behandle opplysningene på «*annen måte*» enn det som følger av avtalen med den behandlingsansvarlige, gir angivelsen av *hvilke* opplysninger som kan behandles og *hvordan* opplysningene kan behandles, rammene for databehandlerens behandling, jf. POL § 15 (1).

Beskrivelsen i databehandleravtalen av hvordan personopplysningene skal behandles, bør være så konkret som mulig, slik at databehandlerens handlingsrom er klart definert. For at avtalen skal være dekkende, må det vurderes *hvilke* opplysninger eller kategorier av opplysninger som databehandleren skal behandle, siden dette kan ha betydning for hvordan behandlingen skal gjennomføres. Så må det, som det eksplisitt følger av bestemmelsen, reguleres *hvordan* behandlingen skal skje, herunder lagring, kopiering, endring, overføring mv. av personopplysningene.

Når det gjelder innholdet i beskrivelsen av hvordan databehandleren kan behandle personopplysninger, vises det til punkt 3.1 ovenfor om omfanget av behandlingen.

Behandlingsmåter og -rutiner kan være beskrevet i et annet dokument enn databehandleravtalen, men behandlingsmåtene og -rutinene må enten være vedlagt databehandleravtalen, eller databehandleravtalen må henvise til det relevante dokumentet, se Datatilsynets anførsel i Personvernnemndas sak PVN-2014-01 Skan-kontroll. Etter Personvernnemndas avgjørelse i PVN-2015-04 FaVer AS kreves det imidlertid ikke at databehandleravtalen skal inneholde behandlingsrutine eller eksplisitt vise til en slik rutine, siden behandlingsansvarlig og databehandler etter regelverket kun skal ha tilfredsstillende sikkerhetsrutiner, og at disse skal kunne dokumenteres. Etter disse to avgjørelsene må konklusjonen være at hvilke måter databehandleren skal kunne behandle personopplysninger på, må være inntatt eller henvist til i databehandleravtalen, men rutiner for behandling, herunder for informasjonssikkerhet og internkontroll, trenger ikke inntas i avtalen.

Siden det også vil bli gitt instrukser av den behandlingsansvarlige til databehandleren, jf. PVD artikkel 17 (3), kan ikke kravene til databehandleravtalen forstås slik at denne uttømmende skal regulere databehandlerens behandling.[48]

Reglene om at det må foreligge databehandleravtale, videreføres i forordningen, se artikkel 28 nr. 3. Det må foreligge en kontrakt «*eller annet rettslig bindende dokument*», og det stilles konkrete krav til hva avtalen må regulere, som hva som skal behandles (gjenstand for behandlingen), varigheten av behandlingen (hvor det må være tilstrekkelig å knytte varigheten til tilhørende tjenesteavtale mellom partene), behandlingens karakter og formål, typer av personopplysninger og kategoriene av registrerte, samt behandlingsansvarliges forpliktelser og rettigheter. Forordningen stiller altså konkrete krav til avtalens innhold, i motsetning til tidligere regelverk, hvilket viser seg spesielt gjennom opplistingen av plikter under artikkel 28 nr. 3 bokstav a til h. En rekke av pliktene som skal pålegges databehandleren gjennom forordningens regler, er tilsvarende de som gjaldt etter tidligere regelverk, men databehandleren har fått en utvidet plikt til å bistå den behandlingsansvarlige i å oppfylle dennes plikter overfor de registrerte, se spesielt artikkel 28 nr. 3 bokstav e til h. I siste avsnitt i artikkel 28 nr. 3 får også databehandleren en plikt til å informere den behandlingsansvarlige dersom databehandleren oppfatter at en instruks fra den behandlingsansvarlige er i strid med forordningen eller annen personvernlovgivning. Bestemmelsen er et utslag av at den behandlingsansvarlige har det fulle ansvaret for behandlingen, men skal forhindre at databehandleren, som ofte er den som har mest erfaring med og kjennskap til behandling av personopplysninger, skal kunne skjule seg bak den behandlingsansvarliges ansvar og ikke gi uttrykk for forhold som kan være i strid med regelverket. Konsekvensene av at databehandleren ikke informerer om forhold denne ser på som brudd på regelverket, vil kunne gjøre databehandleren medansvarlig for personvernovertredelser, avhengig av hvordan den nasjonale lovgivningen som eventuelt implementerer personvernforordningen, utformes.

Etter forordningens artikkel 20 vil de registrerte ha rett til dataportabilitet, som vil si rett til å kreve personopplysninger overført fra en behandlingsansvarlig til en annen behandlingsansvarlig under visse vilkår. For at den behandlingsansvarlige skal sikre at denne kan oppfylle plikten til dataportabilitet, bør det reguleres i databehandleravtalen at databehandleren har plikt til å oppfylle den behandlingsansvarliges plikter til dataportabilitet etter forordningen (og eventuell senere norsk lovgivning som kommer som en følge av forordningen).

48. Slik også s. 275 i Olsen, Thomas, «Personvernøkende identitetsforvaltning», *Complex* 2/2015.

Forordningen åpner for at EU-kommisjonen eller tilsynsmyndighet, som Datatilsynet, skal kunne utarbeide standardbestemmelser for bruk av databehandler eller underdatabehandler, se artikkel 28 nr. 6 til 8.

3.3.3 Regulering av informasjonssikkerhet

Det andre kravet til databehandleravtalens innhold er at de sikringstiltak som databehandleren plikter å gjennomføre skal fremgå av avtalen, jf. POL § 15 (2). For kravene til sikringstiltak som påhviler databehandleren etter POL § 13, vises det til punkt 4.3 nedenfor. Det må vurderes i det enkelte tilfelle hvor konkret reguleringen av pliktene må være i avtalen. En detaljert regulering av pliktene kan i utgangspunktet ikke være påkrevet siden databehandleren har en selvstendig plikt etter § 13 til å planlegge og iverksette tiltak.

I POL § 15 (2) tales det om avtaleregulering av «sikringstiltak», men gjennom henvisningen til POL § 13 fremgår det at det siktes til tiltak for å ivareta «informasjonssikkerhet». For en tilstrekkelig dekning av slike tiltak må avtalen dekke avvikshåndtering (se POF § 2-6), herunder avklare hvem som har ansvaret for å melde avvik til Datatilsynet dersom avviket fører til uautorisert utlevering av personopplysninger, hvordan tilgangskontroll og kontrollmekanismer skal gjennomføres, taushetsplikt, sikkerhetsrevisjoner, fysiske sikringstiltak, hvordan rutiner mv. skal dokumenteres, hvilket personell hos partene som skal ha tilgang til personopplysningene, og andre krav som følger av POF kapittel 2. Det vil i de fleste tilfeller være tilstrekkelig å vise til bestemmelsene i POL og POF, dersom det ikke gjelder spesielle forhold (som at databehandleren ikke har tilstrekkelig kompetanse innenfor området).

I POL § 13 (2) er det oppstilt en plikt til å dokumentere «informasjonssystemet og sikkerhetstiltakene» både for den behandlingsansvarlige og databehandleren. Kravene til databehandleravtalen må forstås slik at denne skal dekke dokumentasjonskravene, med den følge at databehandleravtalen skal dekke de plikter som databehandleren har til informasjonssikkerhetstiltak, herunder også planlagte og systematiske tiltak, etter § 13. En generell henvisning til POL § 12 og POF kapittel 2 vil imidlertid i de fleste tilfeller være tilstrekkelig. Avtalen må i en del tilfeller dekke sikkerhetsrevisjoner for å innfri lovens krav, siden dette er den mest praktiske måten den behandlingsansvarlige kan forvisse seg om at databehandleren etterlever kravene til tilfredsstillende informasjonssikkerhet, jf. POF § 2-5. Regulering av den behandlingsansvarli-

ges rett og databehandlerens plikt til å delta i årlige sikkerhetsrevisjoner, og rammene og tiltakene knyttet til revisjonene, bør være et minimum som reguleres i avtalen.

Sikringsspørsmål må alltid være regulert, men det vil variere hvor omfattende og inngående avtalereguleringen bør være, og databehandlerens kompetanse står her sentralt.[49] Databehandleravtalen bør imidlertid også regulere plikten til å dokumentere tiltakene og gjøre dokumentasjonen tilgjengelig, jf. POL § 13 (2) og § 14 (2).

Etter POF § 2-15 skal det gjennom avtale også etableres klare ansvars- og myndighetsforhold mellom den behandlingsansvarlige og databehandleren. Det er naturlig at dette reguleres i databehandleravtalen med regulering av bl.a. i hvilke tilfeller databehandleren selv fatter beslutninger, og med avgrensning av den behandlingsansvarliges og databehandlerens ansvarsområder.

3.4 Inngåelse av databehandleravtale; formkrav

Ettersom en behandlingsansvarlig ikke kan overlate personopplysninger til andre (herunder databehandler) uten at det foreligger en skriftlig avtale som regulerer behandlingen av personopplysningene, er den behandlingsansvarlige ansvarlig for at databehandleravtale inngås, jf. POL § 15 (1). Kravet til avtale er også en begrensning i databehandlerens bruk av underdatabehandler; se punkt 4.4 nedenfor.

Bestemmelsen slik den lyder i POL § 15 (1), avviker fra bestemmelsen som ble foreslått av lovutvalget, hvor det ble foreslått at databehandleren ikke kunne *anvende* personopplysningene *til andre formål* enn *det oppdraget gjelder*.[50] Den vesentligste endringen var å erstatte «*til andre formål*» med «*på annen måte*», og det fremgår ikke av forarbeidene hvorfor endringen ble foretatt. Det må antas at endringen var tilsiktet, siden det var en så klar endring i bestemmelsen. Som det følger ovenfor, kan ikke databehandler behandle opplysninger utenfor det formål den behandlingsansvarlige har med behandlingen. Det er således ikke nødvendig å regulere formålet med behandlingen eksplisitt i § 15. Derimot er det nødvendig å

49. NOU 1997: 19 s. 142–143.
50. Se NOU 1997: 19 Et bedre personvern, kommentarene til § 13 i lovforslaget.

regulere om databehandleren har anledning til å avgjøre på hvilken måte behandlingen kan gjøres på, på bakgrunn av at definisjonen av behandlingsansvarlig ble endret fra lovutvalgets forslag til endelig lovutkast. Dette ved at «*behandlingsansvarlig*» ble i POL § 2 nr. 4 definert som bl.a. den som bestemmer «*hvilke operasjoner som skal eller kan utføres på personopplysningene*» i lovutvalgets forslag, og dette ble erstattet med den som bestemmer «*hvilke hjelpemidler som skal brukes*». Med denne endringen er det trolig nødvendig å presisere at databehandleren ikke har anledning til å bestemme selv hvilke verktøy som skal brukes til behandlingen, uten at dette er inntatt i avtalen med den behandlingsansvarlige. Ut fra det forhold at databehandleren har ekspertisen på behandlingen, må det allikevel bl.a. være en del tekniske og prosessmessige forhold som databehandleren kan avgjøre, jf. ovenfor. For de øvrige endringene synes det som om disse ble foretatt for å bedre loven språklig sett.

Som det følger av punkt 3.2.2 ovenfor, vil også databehandling utført av et konsernselskap for et annet selskap i konsernet være å betrakte som databehandling, og følgelig må det derfor også inngås databehandleravtale mellom selskap i samme konsern.

Det er ingen formkrav til databehandleravtalen utover at den skal være skriftlig. Til sammenligning krever direktivets artikkel 17 nr. 3 at behandlingen hos databehandler skal skje etter kontrakt «*eller annet rettslig bindende dokument*»,[51] selv om det siste alternativet neppe er særlig praktisk.

At rammene for behandlingen nedfelles i en avtale og er tilgjengelig i skriftlig form, sikrer klarhet om rammene for databehandlerens behandling og forenkler den behandlingsansvarliges kontroll av om databehandleren etterlever sine forpliktelser. At det benyttes skriftlig avtale, er også en fordel av hensyn til notoritet, og det er selvsagt også en forutsetning for at Datatilsynet og Personvernnemnda skal kunne kreve avtalen fremlagt etter POL § 41 (1).

Det er ikke krav om at databehandleravtalen skal være undertegnet eller oppfyller andre formalia. Det er derfor tilstrekkelig at avtalen kun utformes elektronisk, noe som er i tråd med forordningens artikkel 28 nr. 9. Avtalen må imidlertid dekke behandlingen som databehandleren skal foreta, jf. lovens krav om at databehandleren ikke skal behandle personopplysninger på annen måte enn inntatt i avtalen, jf. nedenfor.

---

51. Olsen, Thomas (2015), «Personøkende identitetsforvaltning», *Complex* 2/2015, behandler dette spørsmålet nærmere, se s. 278 flg., og konkluderer med at andre juridisk bindende dokumenter vil kunne erstatte skriftlig avtale, slik også Datatilsynets praksis bekrefter.

Siden det ikke stilles krav til avtalens utforming, kan en databehandleravtale inngå som en del av en annen avtale mellom behandlingsansvarlig og databehandler, eksempelvis en tjeneste- eller driftsavtale. Oppfyller innholdet i et slikt avtaledokument kravene til en databehandleravtale, vil denne være å regne som en databehandleravtale i henhold til lovens krav.

Kravet i POL § 15 til skriftlig avtale må forstås slik at det som er avtalt mellom den behandlingsansvarlige og databehandleren, skal nedfelles skriftlig i databehandleravtalen. Det må imidlertid avgrenses mot enkeltstående instrukser eller avklaringer, siden kun generelle instrukser som gjelder databehandlerens videre behandling, bør inntas i avtalen.

3.5 Konsekvenser av manglende databehandleravtale

At det foreligger et databehandlerforhold, medfører at en databehandleravtale er påkrevd, jf. POL § 15. Om det foreligger et databehandlerforhold, avhenger av om den som behandler personopplysningene, gjør det på vegne av en annen, se punkt 2.2 ovenfor. Foreligger det et databehandlerforhold uten en skriftlig databehandleravtale, er dette en overtredelse av POL § 15.

Er det ikke inngått skriftlig avtale eller avtalen mangler regulering av databehandleres plikt til å gjennomføre sikringstiltak etter POL § 13, foreligger en overtredelse av POL som kan medføre overtredelsesgebyr eller straff både for den behandlingsansvarlige og databehandleren, se nærmere i punkt 4.5 nedenfor.[52] En slik overtredelse vil imidlertid i utgangspunktet være den behandlingsansvarliges ansvar siden den behandlingsansvarlige da har utlevert personopplysninger uten at det foreligger skriftlig avtale etter POL § 15.

Personvernnemnda har lagt til grunn at en databehandleravtale er en indikator på at det foreligger et databehandlerforhold,[53] og det samme gjelder der det er angitt hvem som er behandlingsansvarlig, eller om opplysningene skal utleveres til annen enn den behandlingsansvarlige. Bestemmelsen i POL § 15 kan klart nok ikke forstås slik at kravet til databehandleravtale er en forutsetning

52. Se Johansen, Michal Wiik, Knut-Brede Kaspersen og Åste Marie Bergseng Skullerud (2001): *Personopplysningsloven. Kommentarutgave*, Universitetsforlaget, s. 137.
53. Personvernnemndas klagesak 2005-05.

for at det skal anses å foreligge et databehandlerforhold. I så fall ville det bli for lett å komme seg unna ansvaret som behandlingsansvarlig; se også punkt 3.2.6 ovenfor om betydningen av at forholdet mellom den behandlingsansvarlige og databehandleren er regulert i databehandleravtale.

3.6 Annen regulering som etter forholdene er nødvendig eller bør inntas i databehandleravtalen

3.6.1 Innledning

Selv om det er få krav til hva databehandleravtalen *skal* inneholde etter gjeldende rett, og Datatilsynet ikke har stilt særskilte krav til innholdet i databehandleravtaler,[54] er det regulering som etter forholdene *er nødvendig at* er en del av en databehandleravtale. Det er videre regulering som *bør* inntas for å sikre rett behandling av personopplysningene etter POL og POF, men som ikke direkte eller indirekte følger av rettslige krav.

Regulering som etter forholdene kan være nødvendig å innta i databehandleravtalen, er bruk av underdatabehandler, som er påkrevet å regulere dersom underdatabehandler skal benyttes, se punkt 3.6.3 nedenfor. Regulering som også bør tas inn, er regulering hvor det er forhold etter lovverket som legger føringer på databehandlerens behandling på vegne av den behandlingsansvarlige. Dette gjelder bl.a. grenser for behandlingen, krav til databehandleren som skal bidra til at den behandlingsansvarlige kan oppfylle sine plikter etter lovverket, tiltak som setter databehandleren i stand til å oppfylle sine egne plikter, som informasjonsplikten etter POL § 24, forhold knyttet til overføring av personopplysninger til utlandet mv. Databehandlerens informasjonsplikt overfor den behandlingsansvarlige må også reguleres i avtalen, siden den behandlingsansvarlige skal ha kunnskap om sikkerhetsstrategien hos databehandleren, og jevnlig forsikre seg om at strategien gir tilfredsstillende informasjonssikkerhet, jf. POF § 2-15 (5). Disse forholdene behandles nedenfor.

Det er også selvsagte forhold som må reguleres i en databehandleravtale, selv om disse ikke er påkrevet etter POL, som springer ut av det at det inngås en avtale, som angivelse av partene, avtalens varighet og opphør, mv.

54. Se Blixrud, Katrine Berg og Christine Ask Ottesen (2010), *Personvern i finanssektoren*, Gyldendal, s. 57.

Med forordningen innføres det en rekke konkrete krav til databehandleravtalens innhold, og for databehandleravtaler som inngås før forordningen (eller lovgivning som eventuelt skal implementere forordningen) trer i kraft, bør man også hensynta disse kravene for å unngå senere endringer i databehandleravtaler.

3.6.2 Behandlingens formål

Databehandleren har bare adgang til å behandle opplysningene innenfor det angitte formålet for behandlingen, jf. POL § 11 bokstav b, og innenfor databehandleravtalens rammer og/eller instruksjoner gitt av den behandlingsansvarlige, se punkt 3 ovenfor. Tilsvarende gjelder etter personvernforordningen, se artikkel 28 nr. 3 a. Det er imidlertid ikke et krav at formålet med behandlingen er beskrevet i databehandleravtalen; POL § 15 krever bare regulering av *hvordan* (og ikke hvorfor) behandlingen skal skje, i databehandleravtalen.

Formålet med behandlingen av personopplysningene er imidlertid førende for omfanget av behandlingen. Den behandlingsansvarlige må derfor informere databehandleren om formålet for behandlingen for at databehandleren ikke skal gå utenfor disse rammene. Databehandleravtalen bør av den grunn enten angi rammene for behandlingen for databehandleren (som indirekte bestemmes av formålet med behandlingen), eller formålet med behandlingen av personopplysningene, slik at databehandleren vet hvilke formål den skal forholde seg til.

Skal behandlingen, herunder databehandlerens behandling, være noe annet enn formålet som lå til grunn for den opprinnelige innsamlingen av personopplysninger, må det foreligge samtykke, jf. POL 11 (1) punkt b og c, og formålet må være saklig begrunnet i den behandlingsansvarliges virksomhet. Databehandleren må også behandle personopplysningene på den måten som den behandlingsansvarlige angir, mens det er den behandlingsansvarlige som er ansvarlig for at behandlingen som databehandleren forestår, er i overensstemmelse med formålet for behandlingen.

3.6.3 Bruk av underdatabehandler

Personopplysningene databehandleren behandler på vegne av den behandlingsansvarlig, kan ikke utleveres av databehandleren til andre uten at dette er avtalt med den behandlingsansvarlige, jf. POL § 15, se punkt 4.4 nedenfor.

Det må også avtales hvordan utlevering skal skje, til hvem og hvilken behandling underdatabehandleren skal forestå. Skal det benyttes underdatabehandler, *må* dette fremgå av databehandleravtalen.

Databehandleravtalen må også regulere hvor personopplysningene blir behandlet, slik at avtalen inneholder informasjon om hvilken underdatabehandler som fysisk kan besitte personopplysningene, og hvor opplysningene skal være lokalisert. Dette kravet må forstås som et krav til geografisk lokasjon, som ikke behøver være mer konkret enn hvilket land opplysningene behandles i, hvilket viser også hvilken jurisdiksjon som gjelder. Dersom det er land med ulik lovgivning f.eks. på delstatsnivå, bør det angis mer konkret hvor opplysningene skal behandles, knyttet til jurisdiksjon.

3.6.4 De registrertes rettigheter

Skal databehandleren ha oppgaver knyttet til registrerte, som å gi registrerte innsyn i personopplysningene, rette eller slette personopplysningene etter anmodning fra registrerte, oppfylle informasjonsplikten overfor registrerte osv., bør dette reguleres i databehandleravtalen. Den behandlingsansvarlige har etter POL adgang til å delegere slike administrative funksjoner til databehandleren, jf. ovenfor.

3.6.5 Informasjonsplikt

Databehandleren har en selvstendig informasjonsplikt overfor de registrerte, se punkt 4.1 nedenfor. Hvordan databehandleren skal overholde denne informasjonsplikten, herunder hvordan databehandleren skal få informasjon fra den behandlingsansvarlige for å kunne oppfylle informasjonsplikten, bør til en viss grad reguleres i databehandleravtalen. Dersom databehandleren selv skal kunne avgjøre krav om informasjon fra de registrerte, må dette, ifølge forarbeidene, være eksplisitt regulert i avtalen.[55]

3.6.6 Databehandleravtalens varighet og opphør

Avtalens varighet bør reguleres i databehandleravtalen. Databehandleravtalens varighet bør også ta høyde for at det kan være nødvendig med en viss behandling også for å avvikle tjenestene.

55. Se Ot.prp. nr. 92 (1998–99) s. 122 og punkt 4 nedenfor.

Hva som skal skje med personopplysninger som er overlatt til databehandleren ved avtalens opphør, herunder om opplysningene skal tilbakeføres til den behandlingsansvarlige eller slettes på tilbørlig eller anvist måte, hvordan sikkerhetskopier skal håndteres mv., bør også reguleres i databehandleravtalen. Dette kan imidlertid være regulert allerede som en del av pliktene knyttet til informasjonssikkerhet.

3.6.7 Overføring til utlandet

Dersom databehandleren skal ha anledning til å overføre personopplysningene til utlandet, bør dette eksplisitt angis i databehandleravtalen. Er det regulert hvilken underdatabehandler databehandleren kan benytte, og at dataene vil være lokalisert hos underdatabehandler i utlandet, vil dette være dekkende for regulering av overføring til utlandet. Overføring av personopplysninger over landegrensene til databehandler utenfor Norge er nærmere behandlet i punkt 5.4 nedenfor.

4 Databehandlerens ansvar og plikter

4.1 Innsynsrett og informasjonsplikt

De *registrerte* kan etter POL kapittel III kreve skriftlig informasjon om hvilken behandling som gjøres av deres personopplysninger. Slik informasjon kan også kreves utlevert direkte fra databehandleren, jf. POL § 24. Bakgrunnen for dette er at databehandleren ofte er den behandlingsansvarliges ansikt utad, og dermed den som de registrerte er nærmest til å kontakte.

Ettersom det ikke kan gis allmennheten tilgang til datasystemene hvor personopplysningene er lagret, bl.a. på grunn av informasjonssikkerhetshensyn, er dette imidlertid i praksis mer en rett til (å motta) informasjon.

Opplysninger som skal gis etter nevnte kapittel III i POL, er først og fremst informasjon som databehandleren normalt vil motta som følge av databehandleroppdraget, og bør derfor reguleres i databehandleravtalen, se punkt 3 ovenfor. Typisk vil dette gjelde informasjon om den behandlingsansvarlige, formålet med behandlingen og hvilke typer personopplysninger som behandles, se POL § 18.

Det kan imidlertid være slik at databehandleren ikke har den informasjonen som etterspørres, som f.eks. hvor/hvordan personopplysningene er innsamlet,

om opplysningene vil bli utlevert til andre av den behandlingsansvarlige, og sikkerhetstiltak for andre enn databehandleren knyttet til behandling av personopplysningene. Det kan også være slik at databehandleren ikke har nok informasjon til å utdype opplysningene på en måte som gjør den registrerte i stand til å ivareta sine egne interesser i henhold til POL § 18 (4). I slike tilfeller vil den behandlingsansvarlige være den nærmeste til å gi slik informasjon.

Informasjon om det forhold at det benyttes databehandler, er ikke informasjon som pliktes gitt etter POL kapittel III. Dersom databehandleren skal utføre plikter overfor de registrerte på vegne av den behandlingsansvarlige, er det derimot en forutsetning for at pliktene skal kunne utføres, at de registrerte er kjent med bruken av databehandleren.

Rettighetene til å kreve innsyn og informasjon hos databehandleren følger ikke av PVD, og de øvrige EU/EØS-land er derfor ikke forpliktet til å implementere tilsvarende bestemmelser.

Ifølge forarbeidene til POL[56] skal det reguleres i databehandleravtalen om databehandleren kan avgjøre og besvare krav om informasjon fra registrerte. Uten en slik avtalt rett for databehandleren må databehandleren videreformidle alle krav om informasjon til den behandlingsansvarlige. Som for behandling av personopplysninger generelt vil det være den behandlingsansvarlige som har det endelige ansvaret for at krav om informasjon etterkommes.

Forespørsel om informasjon skal som et utgangspunkt besvares innen 30 dager fra mottak av henvendelsen, jf. POL § 16. Denne fristen vil også gjelde for databehandleren i de tilfeller der databehandleren har en informasjonsplikt etter henvendelse fra de registrerte eller andre. Har databehandleren etter databehandleravtalen adgang til å avgjøre krav om informasjon, må databehandleren også kunne vurdere om det foreligger unntak fra retten etter POL § 23.

Databehandleren bør kreve at den som skal motta opplysningene, legitimerer seg, siden en utlevering til andre enn de som har krav på opplysninger etter POL § 18, vil kunne være en ulovlig utlevering av personopplysninger. Der bare den registrerte kan kreve den etterspurte informasjonen, plikter databehandleren å kontrollere identiteten til den som skal motta informasjonen.

56. Ot.prp. nr. 92 (1998–99) s. 122.

Det kan etter POL § 24 andre setning kreves at de registrerte leverer skriftlig og undertegnet begjæring om informasjon før opplysningene gis. Også databehandleren må kunne kreve skriftlig begjæring. Kravet om skriftlig begjæring gjelder kun dersom det fremsettes krav om informasjon fra en registrert. Ved henvendelser fra allmennheten etter POL § 18 (1) kan det ikke kreves skriftlig begjæring, og den som etterspør opplysningene, kan til og med være anonym.

Loven gir ikke veiledning om hvordan informasjonen skal gis, og det må derfor antas at den kan gis på den måten som fremstår mest hensiktsmessig, herunder elektronisk, men informasjonen bør gis skriftlig for å sikre dokumentasjon.

I reglene om innsyn i e-postkasse mv. som ble inntatt i POF kapittel 9 pr. 1. mars 2009, er det også presisert at reglene om innsyn også gjelder der det benyttes databehandler, jf. POF § 9-1 (4). Dette er for så vidt en unødvendig presisering siden de generelle reglene som det er redegjort for ovenfor, gjelder også ved innsyn i e-post mv.

Ved innsyn i e-post mv. vil den som krever innsyn, som regel være arbeidsgiver *og* behandlingsansvarlig, og er den som er ansvarlig både for om det foreligger grunnlag for innsyn i e-post mv., og hvordan innsynet skal gjennomføres. Databehandleren er kun medvirkende til gjennomføringen av innsynet etter den behandlingsansvarliges instruksjon, og databehandleren har ikke grunnlag for eller plikt til å motsette seg medvirkning til innsyn selv om denne er uenig i at innsyn er berettiget.

Hvorvidt databehandleren er forpliktet til å medvirke til innsyn i e-post mv., vil bero på pliktene databehandleren har etter databehandleravtalen. Normalt vil databehandleren eksempelvis være forpliktet til å utlevere personopplysningene til den behandlingsansvarlige, men ikke være forpliktet til å gjennomgå e-poster eller annen informasjon.

4.2 Pålegg fra Datatilsynet

Der personopplysninger behandles av databehandleren, kan det være aktuelt for Datatilsynet å gi databehandleren pålegg etter POL. Dersom det gjelder områder hvor databehandleren er direkte forpliktet etter lovverket, som for informasjonsplikten og pliktene tilknyttet informasjonssikkerhet, er det på det rene at Datatilsynet kan gi databehandleren pålegg etter POL § 42 (3) nr. 2.

Der databehandlerens plikter bare er utledet fra den behandlingsansvarlige, og databehandleren ikke har direkte ansvar etter loven, kan derimot ikke Data-

tilsynet gi databehandleren pålegg. Datatilsynet må i stedet rette pålegget til den behandlingsansvarlige, som igjen må instruere databehandleren. Dette må ses på bakgrunn av at den behandlingsansvarlige kan ha grunner til å motsette seg pålegg fra Datatilsynet, og at den behandlingsansvarlige i så fall ønsker å få beslutningen overprøvd i Personvernnemnda eller av domstolene.

4.3 Informasjonssikkerhet og internkontroll

4.3.1 Krav etter personopplysningsloven

I POL § 13 er det inntatt krav knyttet til informasjonssikkerhet som gjelder direkte for databehandleren (og den behandlingsansvarlige). Databehandleren plikter således å følge kravene selv uten at dette pålegges eksplisitt i databehandleravtalen eller på annen måte av den behandlingsansvarlige. Etter POL § 15 (2) skal pliktene etter § 13 inntas i databehandleravtalen, men at pliktene inntas i databehandleravtalen er kun en formalitet for databehandleren, siden databehandlerens plikt til å gjennomføre sikringstiltakene følger direkte av ordlyden i POL § 13.

Etter forordningen er kravene til informasjonssikkerhet (omtalt som «behandlingssikkerhed» i forordningens danske versjon) videreført, se artikkel 32 i forordningen. Kravene til informasjonssikkerhet er noe annerledes utformet i forordningen enn under gjeldende rett, og kravet om informasjonssikkerhetstiltak er relativt ut fra den relevante risiko som foreligger i tilknytning til behandlingen. Det er allikevel lite trolig at kravene til informasjonssikkerhet blir mindre strenge med forordningens regler og eventuell implementering til norsk rett. Forordningen inneholder også et krav til at den behandlingsansvarlige skal melde brudd på «personvernsikkerheten» innen 72 timer til tilsynsmyndigheten, se forordningens artikkel 33. Med brudd på personvernsikkerheten må forstås overtredelse av regelverket som skal sikre personvernet for de registrerte. (Det er uklart hvorfor det benyttes «personvernsikkerhet» i artikkel 33 og «behandlingssikkerhet» i artikkel 32, men det synes å være det samme som legges til grunn i begge bestemmelsene.) Dette er et strengere krav enn i PVD og POL, og med de få meldinger som Datatilsynet mottar som følge av informasjonssikkerhetsbrudd, kan det synes nødvendig med klarere regler. For at den behandlingsansvarlige skal kunne melde brudd, pålegges databehandleren å melde brudd «uten unødig forsinkelse» til den behandlingsansvarlige etter at databehandleren «ble oppmerksom på» bruddet, se forordningen artikkel 33 nr. 2. Se krav til meldingen og dokumentasjon i artikkel 33 for øvrig.

4.3.2 Innholdet i kravet til informasjonssikkerhet

Hovedkravet etter POL § 13 er at databehandleren skal gjennomføre planlagte og systematiske tiltak som er egnet til å sørge for *tilfredsstillende informasjonssikkerhet*. Hva som er tilfredsstillende, vil bero på en konkret vurdering som databehandleren selv må foreta, men hva den behandlingsansvarlige vil anse som tilfredsstillende, vil ha stor betydning siden denne er den endelige ansvarlige for opplysningene og behandlingen av disse. Tiltakene som kan iverksettes for informasjonssikkerheten, vil i første rekke være tekniske siden POL i det vesentlige omhandler behandling av personopplysninger med elektroniske hjelpemidler, men også organisatoriske og fysiske tiltak vil være aktuelle og nødvendige. Eksempler på organisatoriske tiltak vil være å sikre kompetanse og kunnskap hos medarbeidere som behandler personopplysninger, samt å ha klare ansvarsforhold og rutiner for avvikshåndtering dersom sikkerhetsbrudd oppstår. Fysiske tiltak vil typisk være tilgangskontroll til lokaler samt fysisk sikring av maskinvare (som servere).

Grunnkravene som etter loven oppstilles for en tilfredsstillende informasjonssikkerhet, er at personopplysningene er sikret konfidensialitet (at opplysningene kun er tilgjengelige for dem som skal ha tilgang), integritet (at opplysningene ikke endres uten at dette er tilsiktet eller godkjent) og tilgjengelighet (at opplysningene er tilgjengelige hvor tilgang er nødvendig, både for dem som behandler opplysningene, og på forespørsel fra registrerte). Hva som er et tilfredsstillende informasjonssikkerhetsnivå, er avhengig av hvilken type opplysninger som behandles, og følgelig vil det kreves et høyere sikkerhetsnivå ved behandling av sensitive opplysninger. Sikkerhetsnivået må vurderes mot risikoen for at de nevnte mål ikke oppnås, hvor risikoen er summen av faktorenes sannsynlighet for sikkerhetsbrudd (eksempelvis at uvedkommende får tilgang til opplysningene) og konsekvensen av sikkerhetsbruddet.

Hvordan kravene til informasjonssikkerhet oppfylles, må i utgangspunktet være basert på en tilsvarende vurdering hos den behandlingsansvarlige som hos databehandleren, siden kravene til databehandler er utledet fra kravene til behandlingsansvarlig, jf. ovenfor.[57] Imidlertid må det oppstilles noen ytterli-

57. Om kravene til informasjonssikkerhet generelt vises det til kapittel 15 i Blixrud, Katrine Berg og Christine Ask Ottesen (2010), *Personvern i finanssektoren*, Gyldendal, og Jansen, Arild og Dag Wiese Schartum (red.) (2005), *Informasjonssikkerhet – rettslige krav til sikker bruk av IKT*, Fagbokforlaget.

gere krav ved bruk av databehandler, som at overføringen av personopplysningene til databehandleren skal være sikker, hvilket vil medføre at opplysningene oppbevares sikkert ved overføringen, og at opplysningene krypteres når de forlater den behandlingsansvarlige, og dekrypteres ved mottak hos databehandleren.[58] Videre må opplysningenes integritet kontrolleres, bl.a. ved gjennomgang av opplysningene ved mottak, undersøkelse av om mediet er skadet, endret eller aksessert, kontroll av integritetsparametere mv. Tilsvarende må gjelde ved overføring tilbake til den behandlingsansvarlige. Dersom databehandleren betjener flere behandlingsansvarlige, må det også sikres at de ulike behandlingsansvarlige ikke har tilgang til hverandres opplysninger,[59] at de behandlingsansvarlige sikres rapporter og logger over behandlingen som setter dem i stand til å vurdere om behandlingen er tilfredsstillende mv. Ved bruk av databehandler gjennom nettskytjenester («cloud computing»), slik at overføring av data og kommunikasjon med databehandleren skjer via internett, er nevnte krav av spesiell betydning. Databehandleren plikter å følge reglene om informasjonssikkerhet i POF kapittel 2, jf. POF § 2-15 og POL § 15, og kan be Datatilsynet om råd og veiledning vedrørende sikkerhetstiltak og tilfredsstillende informasjonssikkerhetsnivå, jf. POL § 42 (3) nr. 6.

Dersom EU-kommisjonens standardbestemmelser benyttes ved overføring av personopplysninger til databehandler i land utenfor EU/EØS, se punkt 5.4.6 nedenfor, følger det av nr. 12 i fortalen til EU-kommisjonens beslutning 2010/87/EU at databehandleren kan benytte samme sikkerhetsnivå overfor flere behandlingsansvarlige fra EU/EØS-land. Dette kan medføre at databehandleren har et annet sikkerhetsnivå enn det som er normalt etter norske forhold, men siden dette er et nivå som holdes i et annet EU/EØS-land, må det trolig også aksepteres at dette nivået er lavere enn det som benyttes i Norge.

Etter forordningen kan den behandlingsansvarlige kun benytte seg av databehandlere som gir tilstrekkelige garantier for at kravene i forordningen vil oppfylles. Slike garantier vil være i form av ekspertise, pålitelighet og ressurser for å implementere de nødvendige tekniske og organisatoriske foranstaltninger, se punkt 81 i fortalen til forordningen.

58. Eksempelvis kan ikke personnumre sendes via e-post siden e-post er en overføringsmåte som ikke tilfredsstiller kravene etter POF § 10-2. Det må også antas etter regelen i POF § 2-11 at personopplysninger som hovedregel skal krypteres ved overføring over internett.
59. Se Personvernnemndas avgjørelse PVN-2014-01 Skan-Kontroll om kravene til adskillelse.

4.3.3 Internkontroll

POL § 15 om databehandlerens rådighet over personopplysningene viser til POL § 13 om informasjonssikkerhet, men viser ikke til § 14 om internkontroll. Dette, i tillegg til at § 13 omtaler den behandlingsansvarlige *og databehandleren* som pliktsubjekter, mens § 14 kun omtaler den behandlingsansvarlige, betyr at de plikter som pålegges den behandlingsansvarlige etter § 14, ikke gjelder for databehandleren. Dette er i overensstemmelse med de plikter som pålegges behandlingsansvarlige ellers, siden POL § 14 gjelder systematiske tiltak for å oppfylle kravene i loven, som i det vesentlige påhviler den behandlingsansvarlige, og ikke databehandleren. At kravene om internkontroll ikke gjelder databehandleren, innebærer at det kun er konkrete krav til informasjonssikkerhet som gjelder for databehandleren, og de mer virksomhetsomgripende krav til internkontroll gjelder ikke.

Databehandleren plikter derfor kun å gjennomføre tiltak som har konkret med behandlingen av personopplysningene og sikringen av disse å gjøre, men det kan allikevel følge krav av de øvrige plikter som databehandleren har etter enten lovverket eller databehandleravtalen, som forutsetter at et internkontrollsystem er implementert.

Databehandleren plikter imidlertid, ved å utøve behandling på vegne av den behandlingsansvarlige, som et utgangspunkt å følge internkontrollsystemet hos den behandlingsansvarlige. Dette innebærer at databehandleren skal behandle opplysningene i samsvar med den behandlingsansvarliges rutiner for internkontroll,[60] og da spesielt ved oppfyllelse av plikter som tilligger databehandleren etter loven, på vegne av den behandlingsansvarlige. Den behandlingsansvarlige har plikt til å kontrollere databehandlerens etterlevelse av lovverk og databehandleravtale, se punkt 3.3.2 ovenfor, og databehandleren må derfor inkluderes som en del av den *behandlingsansvarliges* internkontroll.

4.3.4 Dokumentasjonskrav

Databehandleren har plikt til å dokumentere *informasjonssystemet*, dvs. systemets arkitektur og hvor personopplysninger er lagret, samt *sikkerhetstiltakene*, dvs. tiltakene som foreligger for å sikre personopplysningene, etter POL § 13

60. Se POF § 3-1 (4).

(2). Dokumentasjonen skal, som tiltakene, være hensiktsmessig for å sikre at det oppnås et tilfredsstillende informasjonssikkerhetsnivå. Det settes krav til dokumentasjonens tilgjengelighet, og bestemmelsen må forstås slik at dokumentasjon som databehandleren utarbeider, skal være tilgjengelig for medarbeiderne hos den behandlingsansvarlige og hos databehandleren. Hensikten med tilgjengeligheten er at dokumentasjonen skal benyttes som arbeidsdokumenter for medarbeidere som håndtere personopplysningene.[61] Dokumentasjonen skal også være tilgjengelig for Datatilsynet og Personvernnemnda på forespørsel, men oversendes ikke uoppfordret til de nevnte.

Noen plikt til å dokumentere utover det nevnte har ikke databehandleren, jf. distinksjonen mellom § 13 og § 14, slik at det kun er den behandlingsansvarlige som skal dokumentere de planlagte og systematiske tiltak som til enhver tid er nødvendige for å oppfylle kravene etter POL. Dokumentasjonen skal imidlertid være tilgjengelig også for databehandlerens medarbeidere, jf. § 14 (2). Tiltakene vil her både være tiltak etter § 13 ovenfor samt tiltak for å sikre at de grunnleggende kravene etter POL etterleves, som behandling innenfor formålet, rett til innsyn/informasjon, retting og sletting av opplysninger, sikring av opplysningenes kvalitet (tilstrekkelige, fullstendige og korrekte opplysninger), etterlevelse av konsesjonskrav mv. Siden databehandleren behandler personopplysninger på vegne av den behandlingsansvarlige, er databehandleren forpliktet til å følge lovens regler på lik linje med den behandlingsansvarlige, og gjennom dokumentasjonsplikten etter denne bestemmelsen vil databehandleren instrueres av den behandlingsansvarlige om tiltak av betydning for behandlingen. Bestemmelsen innebærer både en plikt for den behandlingsansvarlige til å gjøre dokumentasjon av tiltakene tilgjengelig for databehandleren, og en plikt for databehandleren til å gjøre dokumentasjonen tilgjengelig for sine medarbeidere. Det følger også av POF § 3-1 (4) at databehandleren skal behandle personopplysninger i samsvar med de rutiner den behandlingsansvarlige har oppstilt. Dette er de rutiner som den behandlingsansvarlige plikter å etablere etter tredje avsnitt i samme bestemmelse, men også rutiner som den behandlingsansvarlige etablerer og som går utover plikten etter bestemmelsens tredje avsnitt, må databehandleren følge. Dette følger av POL § 15 som generelt

61. Se Ot.prp. nr. 92 (1998–99) s. 115.

pålegger databehandleren ikke å behandle opplysningene på annen måte enn det som er avtalt med den behandlingsansvarlige.

Etter forordningen har databehandleren en plikt til å ta inn en generell beskrivelse av de tekniske og organisatoriske informasjonssikkerhetstiltak som er iverksatt etter forordningens artikkel 30 nr. 2, se punkt 4.6 nedenfor. Disse kravene er imidlertid ikke strengere enn kravene til dokumentasjon som følger av POL og POF, jf. ovenfor.

4.3.5 Den behandlingsansvarliges kontrollplikt. Avviksbehandling

Den behandlingsansvarlige har et ansvar for å påse at databehandleren oppfyller lovens krav som nevnt ovenfor, jf. POL § 13 (3).[62] Kontrollplikten omfatter det å vurdere om databehandleren følger kravene til sikkerhetstiltak som er nedfelt i databehandleravtalen, samt å kontrollere om databehandleren følger de generelle kravene etter POL § 13 (1) og (2) som er omtalt ovenfor.

Selv om den behandlingsansvarlige har en plikt og ansvar for kontroll av databehandleren, har databehandleren et selvstendig ansvar for å sikre tilfredsstillende informasjonssikkerhet for behandlingen i egen virksomhet.

Bestemmelsen innebærer altså en plikt for den behandlingsansvarlige til å gi informasjon om og legge til rette for aktuelle sikringstiltak, og medfører en plikt for databehandleren til å etterspørre og etterleve eksisterende sikkerhetskrav.[63]

Avdekkes det at personopplysningene behandles i strid med de fastlagte rutiner, herunder i strid med det som følger av databehandleravtalen, ved at tiltakene fra databehandlerens side ikke er tilstrekkelige, skal dette behandles som avvik, jf. POF § 2-6. Dette gjelder uavhengig av om avviket avdekkes som følge av den behandlingsansvarliges kontroll eller på annen måte. Ved et avvik som medfører sikkerhetsbrudd, kan den behandlingsansvarlige bli ansvarlig for manglende kontroll, mens databehandleren kan bli ansvarlig for manglende sikkerhetstiltak. Følgene av avvik er naturlig nok at man skal gjenopprette normaltilstanden og dokumentere denne prosessen.

62. Se NOU 1997: 19 s. 89–90.
63. Se NOU 1997: 19 s. 142–143.

Ved avvik, og dersom den behandlingsansvarlige anser at tiltakene for informasjonssikkerhet ikke er tilstrekkelige, kan den behandlingsansvarlige pålegge databehandleren å iverksette tiltak som bedrer informasjonssikkerheten. Instruksjonsmyndighet for den behandlingsansvarlige følger ikke direkte av loven, men det følger av POL § 15 at databehandleravtalen skal regulere sikringstiltakene, og ved at databehandleren ikke kan behandle personopplysninger på annen måte enn avtalt med den behandlingsansvarlige, har den behandlingsansvarlige en instruksjonsmyndighet gjennom databehandleravtalen.

Følger ikke databehandleren instruksjonene, er den behandlingsansvarlige henvist til å bruke sanksjonene i databehandleravtalen ved manglende oppfyllelse, eller kontakte Datatilsynet for å gi databehandleren pålegg siden databehandleren har en direkte plikt vedrørende informasjonssikkerhet etter loven, eller i ytterste konsekvens heve avtalen for å få behandlingen til å opphøre. Det vil også i enkelte tilfeller foreligge en plikt for den behandlingsansvarlige til å melde fra om avvik til Datatilsynet dersom avviket medførte «*uautorisert utlevering av personopplysninger hvor konfidensialitet er nødvendig*», se POF § 2-6 (3).

Etter PVD artikkel 17 nr. 2 fremgår det at medlemsstatene skal i lovverket innta en plikt for den behandlingsansvarlige til å velge en databehandler som gir de nødvendige garantier med hensyn til tekniske sikkerhetstiltak og organisatoriske tiltak under behandlingen. I POL eller POF fremkommer det ingen plikt for den behandlingsansvarlige til kun å velge databehandler som gir slik garanti, eller en plikt for databehandleren til å avgi slik garanti. Etter forarbeidene til loven er det blitt funnet tilstrekkelig at den behandlingsansvarlige pålegges et krav til informasjonssikkerhet og internkontroll. Det er derfor ikke innført et krav om garanti etter norsk rett, og POL kan ikke forstås slik at databehandleren plikter å bekrefte overfor den behandlingsansvarlige at sikringstiltak er iverksatt eller gjennomført. Annet kan imidlertid følge av databehandleravtalen, og direktivets krav kan underbygge at den behandlingsansvarlige plikter å foreta et forsvarlig valg av databehandler.

Plikten til å velge databehandler som gir garantier, gjelder etter direktivet kun dersom det benyttes en databehandler som utfører behandlingen for den behandlingsansvarliges regning. Det kan problematiseres om plikten til å gi garanti gjelder dersom databehandleren utfører behandlingen vederlagsfritt, som eksempelvis ved tjenestedeling («shared services») som en del av et konsern. Siden det ikke gjelder et krav om garanti etter POL, er det ikke inntatt en forutsetning om at kravene om garanti for sikkerhetstiltak eller organisatoriske tiltak gjelder kun dersom databehandlingen er utført med vederlag fra den behandlingsansvarlige.

Plikten til informasjonssikkerhetstiltak gjelder for databehandleren direkte, slik at POL § 13 må forstås slik at plikten til informasjonssikkerhetstiltak gjelder for databehandleren uavhengig av om denne mottar vederlag.[64]

I personvernforordningen er også «betryggende garanti» et hyppig benyttet begrep, og det kan ikke legges annet i dette begrepet under forordningen enn det ble lagt i det under direktivet, ved at det må avgis en skriftlig bekreftelse fra den part som påtar seg garantien, se punkt 4.3.2 ovenfor.

4.4 Databehandlerens adgang til å bruke og bytte underdatabehandler

Etter POL § 15 (1) andre setning kan databehandleren overlate personopplysninger «*til andre for lagring eller bearbeidelse*», typisk en «underdatabehandler», dersom dette er særskilt avtalt i databehandleravtalen.

Adgangen til å benytte underdatabehandler må ses på bakgrunn av at databehandlere ofte er it-selskaper som yter ulike tjenester til den behandlingsansvarlige, og at også databehandleren ofte er avhengig av å benytte underleverandører. Med de siste års teknologiske utvikling har bruk av underdatabehandler fått økt aktualitet, og det er vanlig at den behandlingsansvarlige behandler personopplysninger ved hjelp av en eller flere spesialiserte underleverandører.

Konsesjonsvilkårene kan sette forbud mot at den behandlingsansvarlige tillater bruk av underdatabehandler.[65] Kravene til informasjonssikkerhet kan etter omstendighetene også være til hinder for bruk av underdatabehandler. Dersom underdatabehandleren er lokalisert utenfor EU/EØS-området, kan dette være til hinder for at personopplysninger behandles av underdatabehandler; se punkt 5.3 nedenfor.

Ved bruk av underdatabehandler bør det fremgå klart av databehandleravtalen hva henholdsvis den behandlingsansvarlige, databehandleren og under-

64. Det er ikke noe krav om at det skal erlegges vederlag for at det skal foreligge et databehandlerforhold, se punkt 3.2.8 ovenfor.

65. Det kan også tenkes at tilsynsmyndigheter som Datatilsynet og Finanstilsynet nedlegger forbud mot bruk av underleverandør som ikke skal behandle personopplysninger, ut fra rent informasjonssikkerhetsmessige vurderinger.

databehandleren skal forestå. På denne måten sikres klare linjer, og man motvirker at databehandlerens ansvar pulveriseres.[66]

Slik loven er utformet, er det imidlertid ikke et *krav* om at de enkelte underdatabehandlere skal spesifiseres eller navngis i databehandleravtalen. I utgangspunktet er det derfor opp til databehandleren – innenfor rammene i databehandleravtalen – å avgjøre hva som skal utføres av underdatabehandlere, og hvilke underdatabehandlere som skal benyttes.

Bytte av underdatabehandler kan være regulert i databehandleravtalen. Ettersom bruk av underdatabehandler krever samtykke fra den behandlingsansvarlige, vil også skifte av underdatabehandler kreve samtykke. Det klare utgangspunkt må derfor være at et generelt samtykke i databehandleravtalen til å benytte underdatabehandler ikke er tilstrekkelig.[67]

POL § 15 krever ikke at det inngås en særskilt databehandleravtale mellom databehandleren og underdatabehandleren. Det kan imidlertid være hensiktsmessig med en egen avtale mellom databehandler og underdatabehandler, bl.a. av dokumentasjonshensyn og for at den behandlingsansvarlige skal kunne utøve sitt oppfølgingsansvar; se punkt 4.7 nedenfor.

Når det gjelder plikten til å overholde kravene til informasjonssikkerhet mv. i POL § 13 (se punkt 4.3 ovenfor), må underdatabehandleren anses som databehandler etter POL når denne behandler personopplysninger på vegne av den behandlingsansvarlige, selv om behandlingen skjer via databehandleren. Dette må gjelde uavhengig av om det er inngått en egen databehandleravtale mellom databehandleren og underdatabehandleren.

I forordningen videreføres reglene om bruk av underdatabehandler, og at det ikke skal kunne benyttes underdatabehandler uten den behandlingsansvarliges skriftlige forhåndsgodkjennelse, som kan være konkret knyttet til spesifikke underdatabehandlere, eller en generell godkjennelse for bruk av underdatabehandler, se forordningens artikkel 28 nr. 2. Nytt i forordningen er plikten for databehandleren til å informere den behandlingsansvar-

66. Dette er anbefalt av Artikkel 29-gruppen, jf. note 35.

67. Artikkel 29-gruppen har uttalt at den behandlingsansvarlige kan avgjøre om denne vil pålegge databehandleren å innhente samtykke ved bytte av underdatabehandler, eller om den behandlingsansvarliges generelle samtykke til bruk av underdatabehandler er tilstrekkelig; se Artikkel 29-gruppens uttalelse i WP 176 av 12. juli 2010.

lige om planlagte endringer av underdatabehandlere, enten ny underdatabehandler kommer til, eller en eksisterende byttes ut, slik at den behandlingsansvarlige får anledning til å fremsette eventuelle innsigelser mot endringene. Etter forordningens artikkel 28 nr. 4 er det også uttrykkelig bestemt at underdatabehandleren pålegges de samme plikter som er fastsatt i databehandleravtalen mellom den behandlingsansvarlige og databehandleren, se om pliktene ovenfor. Underdatabehandleren må også stille samme skriftlige garanti (bekreftelse) før denne vil overholde kravene i personvernforordningen. Ut fra ordlyden i forordningen kan det synes som om pliktene i databehandleravtalen skal kunne pålegges underdatabehandleren direkte dersom det ikke er inngått skriftlig avtale, men dette er trolig ikke hensikten. Dersom en underdatabehandler ikke oppfyller pliktene etter databehandleravtalen eller forordningens regler, vil databehandleren være ansvarlig for den manglende oppfyllelse fra underdatabehandleren, se artikkel 28 nr. 4 i.f.

4.5 Erstatningsansvar og sanksjoner

4.5.1 Erstatningsansvar

Etter POL § 49 er den behandlingsansvarlige erstatningsansvarlig for skade som oppstår som følge av at personopplysninger behandles i strid med personopplysningsloven. Dette gjelder ikke dersom den behandlingsansvarlige godtgjør at skaden ikke skyldes feil eller forsømmelser på den behandlingsansvarliges side, dvs. skyldansvar med omvendt bevisbyrde, jf. § 49 (2).

Den behandlingsansvarlige hefter for skade som oppstår ved databehandlerens behandling i strid med POL, ved at en skade som skyldes databehandleren, normalt vil være en skade som *«skyldes feil eller forsømmelse på den behandlingsansvarliges side»* etter POL § 49. I tillegg hefter den behandlingsansvarlige for databehandlerens handlinger i henhold til de alminnelige regler om kontraktshjelperansvar.[68]

Erstatningsberettigede etter bestemmelsen er *alle*, ikke bare registrerte, som er påført skade ved behandling i strid med POL.

Erstatningen skal svare til det økonomiske tap som skadelidte er påført som følge av overtredelsen av personopplysningsloven, jf. POL § 49 (3) første set-

68. Ot.prp. nr. 92 (1998–99) s. 135, og s. 469 flg. i Hagstrøm, Viggo (2011), *Obligasjonsrett*, Universitetsforlaget.

ning. Det kan også tilkjennes rimelig erstatning for skade av ikke-økonomisk art (oppreisning) etter POL § 49 (3) andre setning, hvor rene rimelighetsbetraktninger legges til grunn for utmålingen. Det er lite praksis vedrørende utmålingen av erstatning for brudd på POL, men dersom mange registrerte rammes av et brudd, kan den totale erstatningssummen bli betydelig, særlig hvis det omfatter oppreisning.

Etter personvernforordningen skal det ytes erstatning for «enhver skade» som den registrerte påføres. Dette omfatter også immaterielle skader, dvs. skader som ikke medfører økonomisk tap, og i punkt 75 til fortalen er det ramset opp en rekke forhold som kan gi grunnlag for erstatning, som «*… forskelsbehandling, identitetstyveri eller -svig, finansielle tab, skade på omdømme, tab af fortrolighed for personoplysninger, der er omfattet af tavshedspligt, uautoriseret ophævelse af pseudonymisering eller andre betydelige økonomiske eller sociale konsekvenser; hvis de registrerede kan blive berøvet deres rettigheder og frihedsrettigheder eller forhindret i at udøve kontrol med deres personoplysninger …*». Det er omvendt bevisbyrde også i forordningen, se artikkel 82 nr. 3, og ved vurderingen av hva som er å anse som «skade», skal dette fortolkes «bredt i lyset av rettspraksis ved EU-domstolen», se punkt 146 til fortalen. Den behandlingsansvarlige og databehandler/databehandlere hefter solidarisk for skade som oppstår, så de registrerte kan rette kravet mot den det er mest hensiktsmessig å få inndrevet kravet fra, av dem som har vært involvert i behandlingen, og den som må utbetale kravet må på sin side rette regress mot de øvrige involverte, se artikkel 82 nr. 4 og 5 i forordningen.

Databehandlerens erstatningsansvar er ikke særskilt regulert i POL, slik at et erstatningskrav direkte mot databehandleren må baseres på alminnelige erstatningsrettslige prinsipper. Det vil imidlertid som regel være enklere for skadelidte å rette erstatningskrav mot den behandlingsansvarlige etter POL § 49. Den behandlingsansvarliges adgang til å søke regress hos databehandleren kan være nærmere regulert i databehandleravtalen, og det er ikke uvanlig at ansvarsbegrensninger inntas i databehandleravtalen.

Forordningen vil endre på ovennevnte ved at databehandleren nå er direkte erstatningsansvarlig overfor de registrerte, og hefter solidarisk med de øvrige som er involvert i behandlingen av personopplysningene, se artikkel 82 nr. 1 . Databehandleren er imidlertid kun ansvarlig for skade som oppstår som en følge av at databehandleren selv ikke har oppfylt

forordningens plikter som er spesifikke for databehandlere. Siden forordningen medfører en utvidelse i plikter for databehandlere, se punkt 3 ovenfor, vil databehandleren være mer eksponert for erstatningsansvar etter forordningen enn etter gjeldende rett. I tillegg vil databehandleren kunne bli erstatningsansvarlig dersom denne har unnlatt å følge eller handlet i strid med de instrukser som den behandlingsansvarlige kan gi etter forordningen, jf. artikkel 82 nr. 2. Sak mot databehandler kan anlegges enten i den jurisdiksjon hvor databehandleren er etablert, eller i den jurisdiksjon hvor den registrerte har sitt normale oppholdssted (men med spesielle regler for offentlige myndigheter), jf. artikkel 79 nr. 2.

4.5.2 Sanksjoner. Overtredelsesgebyr

Etter POL § 46 kan Datatilsynet ilegge overtredelsesgebyr for overtredelse av POL eller POF. Overtredelsesgebyr er den mest praktiske sanksjonen, som også blir hyppigst benyttet i praksis. Gebyret kan pålegges enhver som overtrer loven eller forskriften, noe som omfatter både den behandlingsansvarlige og databehandleren.

Gebyret skal utmåles skjønnsmessig etter de kriterier som er angitt i POL § 46 (2), og for foretak kan gebyr ilegges dersom overtredelse av loven skyldes forhold som ikke er utenfor foretakets kontroll (kontrollansvar), mens fysiske personer må ha handlet uaktsomt eller forsettlig for å bli ilagt gebyr.

Etter personvernforordningen kan tilsynsmyndighet (som Datatilsynet) gi pålegg, foreta undersøkelser, revisjon, gi advarsler, kritisere (som må forstås som å gi offentlig kritikk), forby handlinger mv. overfor databehandlere, jf. artikkel 58. Som sanksjoner for overtredelse av forordningen kan tilsynsmyndigheten ilegge databehandlere administrative bøter, jf. artikkel 58 nr. 2 bokstav f, jf. artikkel 83. Bøtene skal stå i rimelig forhold til overtredelsen og ha avskrekkende virkning, jf. artikkel 83 nr. 1, hvor momentene i artikkel 83 nr. 2 skal hensyntas. Det er satt maksimalsatser for bøtene som, avhengig av hvilke bestemmelser som er overtrådt, er på 20 mill. EUR eller 4 % av samlet global omsetning for foregående regnskapsår for bl.a. overtredelse av de grunnleggende prinsipper for behandling og manglende etterlevelse av påbud fra tilsynsmyndighet, og 10 mill. EUR eller 2 % for en rekke andre overtredelser, se nærmere i artikkel 83 nr. 4 og 5. Det kan også fastsettes andre sanksjoner under nasjonal lovgivning for overtredelser som ikke er sanksjonert av administrative bøter, jf. artikkel 84 nr. 1.

4.5.3 Tvangsmulkt

Dersom Datatilsynet gir et pålegg, kan tilsynet også fastsette en tvangsmulkt som løper for hver dag inntil pålegget er innfridd, jf. POL § 47. Slikt pålegg er mest praktisk å rette mot den behandlingsansvarlige, som igjen må instruere databehandler. I den grad det gjelder plikter direkte for databehandler etter regelverket, kan Datatilsynet også gi pålegg overfor databehandler, med tilhørende tvangsmulkt.

4.5.4 Straffeansvar

POLs straffebestemmelse retter seg mot *«den som»* grovt uaktsomt eller forsettlig overtrer straffebudet, se POL § 48. Bestemmelsen omfatter således ikke bare den behandlingsansvarlige, men også databehandleren og andre. Av de straffbare forhold som er inntatt i bestemmelsen, er det imidlertid kun første avsnitt punkt c, om behandling av personopplysninger i strid med POL § 15 som gjelder databehandlerens rådighet over personopplysninger, som vil kunne være aktuelt for databehandlere. Dersom databehandler handler utenfor eller i strid med databehandleravtalen og behandler personopplysninger på annen måte enn det som er avtalt med den behandlingsansvarlige, vil databehandleren kunne anses som behandlingsansvarlig med de plikter det innebærer, se punkt 3.2 ovenfor. Det vil ha som følge at databehandleren kan bli strafferettslig ansvarlig etter andre forhold nevnt i POL § 48.

Det er også straffebestemmelser i POF § 10-3 som pålegger straff for den som unnlater å følge reglene i POF kapittel 2 til og med 7, samt enkelte bestemmelser i kapittel 8. Spesielt bestemmelsene i POF kapittel 2 om informasjonssikkerhet kan være av betydning for databehandler, siden databehandler plikter å følge kravene til informasjonssikkerhet etter POL § 13. De øvrige straffebud er mest aktuelle for den behandlingsansvarlige, men etter POF § 10-3 straffes medvirkning tilsvarende, og en databehandler som medvirker til den behandlingsansvarliges eget brudd på reglene, kan dermed straffes.

Databehandleren kan også straffes for medvirkning til brudd på POL, jf. POL § 48 (3). Etter lovens forarbeider[69] omfatter straffebudet også hjelpere som den behandlingsansvarlige benytter, men dette forutsetter at den behand-

69. Ot.prp. nr. 92 (1998–99) s. 135.

lingsansvarlige kan straffes i første rekke. Det er kun grovt uaktsomme eller forsettlige overtredelser av POL som er straffbare, og straff for overtredelse av POL vil derfor kun skje ved temmelig klare overtredelser.[70] Ved en overtredelse av POL vil normalt Datatilsynet utferdige et pålegg etter POL § 46, og ved fortsatt overtredelse anmelde forholdet etter POL § 48. Siden POL har et vidt virkeområde med få konkrete bestemmelser, vil det ofte være vanskelig å sanksjonere med straff.[71] Dette fremkommer også av Datatilsynets restriktive praksis ved anmeldelse av overtredelse av POL.[72]

Strafferammen for overtredelse av POL § 48 er fengsel i opptil ett år, og i opptil tre år ved skjerpende omstendigheter.

Personvernforordningen åpner for at det kan besluttes nasjonale lovregler om inndragelse av fortjeneste oppnådd ved overtredelse av forordningen, se punkt 149 til fortalen.

4.6 Spesielle regler etter personvernforordningen

4.6.1 Databehandlerens plikt til å føre oversikt over behandlingen

Personvernforordningen innfører en plikt for databehandleren, enten selv eller ved representant, til å føre en oversikt over all behandling av personopplysninger som databehandleren forestår på vegne av en behandlingsansvarlig, se forordningens artikkel 30 nr. 2. Disse opplysningene skal stilles til rådighet for tilsynsmyndigheter, som Datatilsynet. Oversikten skal inneholde kontaktopplysninger for den behandlingsansvarlige og databehandleren for den konkrete behandling, kategorier av behandling som foretas på vegne av den behandlingsansvarlige (som harmonerer med kravene til innhold i databehandleravtalen, se punkt 3 ovenfor), de overføringer av personopplysninger til tredjeland som er foretatt, hvilket vil

70. Se s. 302 i Johansen, Michal Wiik, Knut-Brede Kaspersen og Åste Marie Bergseng Skullerud (2001), *Personopplysningsloven. Kommentarutgave*, Universitetsforlaget.

71. Ot.prp. nr. 92 (1998–99) s. 94. Vi har få dommer på straff ved overtredelse av POL, og det er kun ilagt bøter, og ikke fengselsstraff, i de dommene som foreligger i dag. Det foreligger noen dommer om datainnbrudd hvor også POL er blitt inntatt i tiltalebeslutningen, men hvor POLs regler er blitt ansett å være «upassende» i slike saker, se eksempelvis Halden tingretts dom av 28. september 2010 (THALD-2010-92742).

72. Se Jørgen Skorstad på s. 141–143 i Blixrud, Katrine Berg og Christine Ask Ottesen (2010), *Personvern i finanssektoren*, Gyldendal.

være mest aktuelt dersom overføring foretas av databehandleren selv til underdatabehandler i tredjeland, se nærmere om dette under punkt 5.3 nedenfor, og en generell beskrivelse av tiltak knyttet til informasjonssikkerhet. Kravet om å føre oversikt gjelder ikke databehandlere som er såkalte mikrovirksomheter med mindre enn 250 ansatte, under visse forutsetninger, se artikkel 30 nr. 5.

4.6.2 Overholdelse av adferdsregler

Det gis hjemmel i forordningen for at det kan utferdiges adferdsregler for databehandlere, bl.a. av tilsynsmyndigheter (som Datatilsynet) og EU-kommisjonen; se forordningens artikkel 40 hvor prosedyrer for godkjennelse av adferdsregler er regulert, samt artikkel 41 om kontroll av allerede godkjente adferdsregler. Adferdsregler kan være generelle eller spesifikke bestemmelser om hvordan personopplysninger skal behandles. Overholdelse av adferdsregler vil ha betydning for om en databehandler gir de nødvendig garantier for å oppfylle kravene til forordningen og beskytte de registrertes rettigheter.

4.6.3 Sertifisering

Tilsvarende som for adferdsregler kan bl.a. tilsynsmyndigheter (som Datatilsynet) og EU-kommisjonen etablere sertifiseringsordninger for databehandlere, se forordningens artikkel 42 flg. Som for adferdsreglene er sertifisering en del av vurderingen av om man kan benytte en databehandler, se punkt 2 ovenfor, selv om sertifisering vil være frivillig. Sertifisering vil være en periodisk prosess.

4.6.4 Personvernombud

Etter forordningens artikkel 37 skal databehandlere som behandler personopplysninger til offentlig myndighet, ha et personvernombud når hovedvirksomheten til databehandleren er eller krever overvåkning av et stort antall registrerte, eller når hovedaktiviteten er behandling av sensitive opplysninger i stort omfang.[73] Det åpnes også for at det kan pålegges personvernombud i andre tilfeller etter nasjonal rett.[74]

---

73. Forordningen bruker ikke betegnelsen «personvernombud», men bl.a. «databeskyttelsesrådgiver» (på dansk) og «Data Protection Officer» (på engelsk). Hvilken betegnelse som vil bli benyttet under norsk rett, som f.eks. «personvernombud» eller «personvernrådgiver», er uklart, så derfor benyttes det relativt innarbeidede begrepet «personvernombud» her.
74. Siden det er noe uklart etter forordningen hvilke virksomheter som plikter å ha personvernombud, vil det bli laget retningslinjer av EU, trolig gjennom Artikkel 29-gruppen, om hvilke virksomheter som skal ha personvernombud.

Forordningen inneholder kvalifikasjonskrav til personvernombudet, ved at vedkommende skal ha ekspertise innenfor personvernrett og tilhørende praksis, samt evne til å utføre de oppgaver som pålegges vedkommende, jf. artikkel 37 nr. 5. Disse oppgavene er opplistet i forordningens artikkel 39, og personvernombudet har et vesentlig selvstendig ansvar for å sikre at forordningens regler overholdes ved kontroll av overholdelse, fordele ansvar, opplæring, opplysning, revisjoner mv.

I tillegg skal personvernombudet informere databehandleren og de ansatte om endringer i regelverket, rådgi om konsekvensanalyser og samarbeide med tilsynsmyndigheter. Personvernombudet skal *involveres tilstrekkelig og rettidig i alle spørsmål* vedrørende beskyttelse av personopplysninger, jf. artikkel 38 nr. 1, som viser at personvernombudet skal ha en sentral plass i databehandlerens organisasjon hva gjelder spørsmål knyttet til behandling av personopplysninger. Det fremgår ikke klart av forordningen, men det må også tilligge databehandlerens personvernombud å ha et tett samarbeid og kontakt med den behandlingsansvarlige, herunder den behandlingsansvarliges personvernombud om denne har dette. De registrerte kan også kontakte personvernombudet for spørsmål knyttet til behandlingen, jf. artikkel 38 nr. 4.

Personvernombudet kan være ansatt hos databehandleren, eller innleid for å utføre tjenestene, jf. artikkel 37 nr. 6. Et konsern kan utnevne et personvernombud for alle konsernets selskaper, jf. artikkel 37 nr. 2. Personvernombudet rapporterer til det øverste ledelsesnivå hos databehandleren, som vil være daglig leder/administrerende direktør (ikke styrets leder), eller konsernsjef i konsernforhold. Personvernombudet hos databehandleren er således under databehandlerens instruksjonsmyndighet arbeids- eller oppdragsmessig, men det følger klart av forordningen at personvernombudet ikke skal instrueres av sin arbeids- eller oppdragsgiver (databehandleren) om utførelse av sine oppgaver, se artikkel 38 nr. 3. Personvernombudet har således en selvstendig stilling, og personvernombudet kan ikke sies opp, avskjediges, eller straffes (hvilket trolig også må omfatte erstatningsansvar for uaktsomme handlinger) for utførelse av sine oppgaver. Personvernombudet kan ha andre oppgaver ved siden av oppgavene som personvernombud, såfremt disse oppgavene ikke medfører en interessekonflikt med oppgavene som personvernombud, jf. artikkel 38 nr. 6.

Personvernombudet har taushetsplikt, jf. artikkel 38 nr. 5, men det er uklart hvem denne taushetsplikten gjelder overfor. Siden personvernombudet har sitt virke med utspring i databehandlerens virksomhet, vil trolig ikke taushetsplikten gjelde overfor databehandleren. I personvernombudets kontakt med registrerte og med tilsynsmyndigheten vil personvernombudet trolig ikke være pålagt å gi tilsynsmyndigheten mer informasjon enn databehandleren er pålagt etter forordningen eller nasjonal lovgivning.

Databehandleren skal offentliggjøre kontaktopplysningene for personvernombudet (f.eks. på nettsidene til selskapet) og informere tilsynsmyndigheten (som Datatilsynet) om utnevnelsen, jf. artikkel 37 nr. 7.

4.7 Den behandlingsansvarliges oppfølgingsansvar

Den behandlingsansvarlige har et oppfølgingsansvar overfor databehandleren. Dette er en naturlig konsekvens av at det er den behandlingsansvarlige som er ansvarlig for databehandlerens behandling av personopplysningene, se punkt 2 ovenfor.[75] Oppfølgningen skal bl.a. gjennomføres ved å følge opp at krav og plikter i databehandleravtalen overholdes av databehandleren. I tillegg skal den behandlingsansvarlige kontrollere at tekniske sikkerhetstiltak og organisatoriske tiltak under behandlingen overholdes av databehandleren, se punkt 4.3.5 ovenfor.[76]

Dette oppfølgingsansvaret gjelder også overfor databehandlerens underleverandører, selv om disse ikke har direkte befatning med personopplysningene.[77] Det er imidlertid nødvendig å regulere slik rett til oppfølging, herunder hvordan oppfølging skal kunne skje, om den behandlingsansvarlige skal utøve oppfølgingen direkte mot underleverandørene; se om databehandlerens bruk av underleverandører og underdatabehandlere i punkt 4.4 ovenfor.

Etter POF § 2-5 skal det gjennomføres sikkerhetsrevisjoner av informasjonssystemet. Når informasjonssystemet håndteres av databehandleren, og denne har kontrollen over dette, må revisjonen gjennomføres hos databehandleren (eller dennes underdatabehandlere). Revisjonen kan enten gjennomføres av den behandlingsansvarlige selv eller av tredjepart.[78]

75. Jf. PVD artikkel 17 (2) og personvernforordningen artikkel 5 nr. 2.
76. Jf. PVD artikkel 17 (2) i.f.
77. Jf. Ot.prp. nr. 92 (1998–99) s. 116.
78. Se Olsen, Thomas, «Personvernøkende identitetsforvaltning», *Complex* 2/2015, s. 277.

5 Databehandling over landegrensene

5.1 Innledning

Overføring av personopplysninger over landegrensene er meget praktisk, særlig innenfor konsern med virksomhet i flere land og ved bruk av databehandler i utlandet. Som følge av nye forretningsmodeller (som off- og nearshoring) og nye tjenester (som nettskytjenester) har emnet blitt stadig mer aktuelt og omdiskutert. Dette må ses på bakgrunn av at det kan medføre en personvernmessig risiko å overføre personopplysninger over landegrensene, typisk der databehandleren er lokalisert i et land med dårligere lovmessig beskyttelse av personvernet enn i Norge og andre europeiske land.

5.2 «Overføring» av personopplysninger

5.2.1 Oversikt

Databehandlerens utførelse av behandlingstjenester for den behandlingsansvarlige vil normalt forutsette at det overføres data, herunder personopplysninger, fra den behandlingsansvarlige til databehandleren. Det kan også skje en overføring av personopplysninger fra databehandler til dennes underdatabehandlere som en del av databehandlertjenestene. Etter omstendighetene vil imidlertid databehandleren kunne utføre databehandling selv om dataene er lagret hos den behandlingsansvarlige. Hvorvidt det ved databehandlerens tilgang til den behandlingsansvarliges systemer og data skal anses å skje en «overføring» av personopplysninger, må vurderes i det enkelte tilfelle.

En slik overføring krever i utgangspunktet ingen hjemmel eller godkjenning siden databehandleren utfører behandling på vegne av den behandlingsansvarlige, og overføringen skjer som ledd i databehandlerens tjenester, se punkt 2.2 ovenfor.

Medfører overføringen til databehandleren at personopplysningene «overføres» over landegrensene, kommer imidlertid POL kapittel V til anvendelse. Det er derfor nødvendig å se nærmere på hva som omfattes av «overføring», og hvorvidt slik overføring kan skje til databehandler i Norge eller til en underdatabehandler utenfor Norge (punkt 5.3 nedenfor) eller databehandler i utlandet (punkt 5.4). Overføring kan også skje ved databehandlers bruk av underdatabehandler utenfor Norge, se punkt 5.3 nedenfor.

5.2.2 *Uttrykket «overføring»*

Overføring er verken definert i PVD eller POL, men begrepet benyttes i POL § 29 og er nærmere omtalt i forarbeidene til loven.[79] Begrepet har også vært gjenstand for vurdering i enkelte saker vedrørende overføring av personopplysninger til land utenfor EU/EØS.

I overføringsbegrepet ligger det språklig at det må være en *tilsiktet handling* at opplysningene overføres, herunder at den som overfører opplysningene, må ha en intensjon om at opplysningene skal mottas av den aktuelle mottaker. Tilgang til opplysninger lagret hos den behandlingsansvarlige for en databehandler («pull») er ikke tilstrekkelig; det må være en reell overførende handling («push») fra den som besitter opplysningene (normalt den behandlingsansvarlige).[80]

Dersom det ikke foreligger en tilsiktet handling, men konsekvensen likevel er overføring av opplysninger, vil det kunne foreligge et brudd på informasjonssikkerhetsrutinene hos den behandlingsansvarlige (eller hos databehandleren dersom det foreligger en utilsiktet overføring til underdatabehandler), se punkt 4.3 ovenfor om informasjonssikkerhet.

5.2.3 *Kravet til mottakerstaten*

Overføring av personopplysninger over landegrensene kan kun skje til stater «*som sikrer en forsvarlig behandling av opplysningene*», jf. POL § 29 (1). Loven inneholder altså en forutsetning om *behandling* av de overførte personopplysninger i det land som opplysningene overføres til. Tilsvarende forutsetning gjelder etter PVD, hvor det også er klarere formulert siden overføring («transfer») til land utenfor EU/EØS (dvs. såkalte tredjeland[81]) gjelder personopplysninger «*which are undergoing processing or are intended for processing after transfer*», dvs. kun personopplysninger som behandles eller skal behandles

79. Spesielt Ot.prp. nr. 92 (1998–99).
80. Se EU-domstolens avgjørelse av 6. november 2003 (Bodil Lindqvist) sak nr. C-101/01 (62001J0101).
81. I POL og POF benyttes «tredjeland», mens PVD benytter «tredjestat» for land utenfor EU/EØS-området. Personvernforordningen benytter «tredjeland», og åpner også for overføring til internasjonale organisasjoner.

etter overføringen. Selv om det ikke er helt klart etter POL, må det innfortolkes et tilsvarende krav om at det skal skje en behandling i tredjelandet for at det skal dreie seg om «overføring».

Reglene om overføring av personopplysninger gjelder uavhengig av hvordan overføringen gjennomføres, herunder om overføringen skjer elektronisk eller ved papir.

Det må foreligge en adressat for opplysningene, altså en spesifikk mottaker av personopplysningene som overføres, for at det anses å være en overføring.[82] Dette i motsetning til generell spredning og allmenngjøring av opplysninger, som kan være en behandling, men ikke en overføring.[83]

5.2.4 Overføring via og/eller mellomlagring i tredjeland

En ren overføring til databehandler via et tredjeland (dvs. land utenfor EU/EØS) – uten at personopplysningene behandles der – vil ikke anses som overføring av personopplysninger. Men overføring via tredjeland må skje i overensstemmelse med kravene til informasjonssikkerhet. Tilsvarende gjelder dersom personopplysninger i forbindelse med overføringen mellomlagres i et tredjeland uten at den behandlingsansvarlige eller databehandler er kjent med dette.

Det kan spørres om overføring via internett, også til mottaker i Norge, medfører en overføring til tredjeland siden en slik overføring rent teknisk kan innebære at data mellomlagres («caches») i land som ikke har tilstrekkelig personvernlovgivning. Forutsatt at det dreier seg om en ren mellomlagring, uten noen behandling, vil det som et klart utgangspunkt ikke dreie seg om «overføring», jf. punkt 5.2.3 ovenfor. En slik løsning stemmer også best med POL § 4 (2), som bestemmer at POL ikke gjelder for data fra annet land som kun overføres via Norge. Det kan også hevdes at tredjelandets personvernlovgivning (eller mangel på sådan) vanskelig kan få betydning når dataene bare mellomlagres kortvarig (og deretter slettes) som en konsekvens av overføringen.

Det kan imidlertid være en informasjonssikkerhetsutfordring forbundet med overføring over internett. Den behandlingsansvarlige må derfor vurdere

82. Se Ot.prp. nr. 92 (1998–99) kapittel 16, kommentarer til § 29.

83. Dette følger også av enkelte av EU-medlemslandenes innlegg i EU-domstolens avgjørelse av 6. november 2003 (Bodil Lindqvist) i sak nr. C-101/01 (62001J0101).

om overføringen skal krypteres eller om andre sikringstiltak skal iverksettes, avhengig av opplysningene som skal overføres.

Overføring av anonymiserte opplysninger til tredjeland, hvor identifikatoren – dvs. koblingen mellom opplysningene og den fysiske personen – beholdes i Norge, er et grensetilfelle hva gjelder overføring. Det må derfor foretas en vurdering i det enkelte tilfelle om dette er å anse som overføring av personopplysninger, og i vurderingen skal det «*tas i betraktning alle hjelpemidler som det er rimelig å tro at noen kan komme til å anvende for identifiseringsformål*», jf. lovens forarbeider. Forarbeidene[84] er kategoriske på at det «*vil dreie seg om en personopplysning selv om det må benyttes en nøkkel – f.eks. i form av en tallkode – for å knytte forbindelsen mellom opplysningen og den bestemte personen*», men opplysninger som er anonymisert på en slik måte at den registrerte ikke lenger kan identifiseres, kan etter mitt syn ikke anses som personopplysninger.[85] Foreligger det ikke personopplysninger, dvs. det er ikke mulig å koble opplysningene til personer, er det heller ikke nødvendig med grunnlag for overføring av opplysningene, f.eks. til tredjeland.

5.2.5 Betydningen av formålet med overføringen

Ved vurderingen av om overføringen er å anse som behandling, har formålet for overføringen normalt hatt betydning for om overføringen er saklig begrunnet, spesielt i de tilfeller hvor Datatilsynet skal vurdere overføringens lovlighet. Ved overføring til databehandler vil formålet være av mindre betydning siden overlatelse av opplysninger til databehandleren normalt vil være en del av behandlingsformålet til den behandlingsansvarlige.

Det kan stilles spørsmål om prinsippet om behandling innenfor det angitte formål har betydning for om personopplysningene kan overføres, dvs. om innsamlingsformålet for personopplysningene kan være til hinder for at opplysningene senere overføres. Generelt kan det antas at formålet ikke kan sette slike begrensninger,[86] men det må trolig bero på en tolkning av det angitte formålet i det enkelte tilfelle. Ved en slik tolkning må utgangspunktet være at kun der-

84. Se kommentarene til § 2 nr. 1 i kapittel 16 i Ot.prp. nr. 92 (1998–99).
85. Se avgjørelse i Personvernnemnda i PVN-2006-04 og «The Concept of Personal Data» WP 136 fra Artikkel 29-gruppen.
86. Slik også s. 37 i Blume, Peter (2006), *Retlig regulering af internationale persondataoverførsler*, Djøf Forlag.

som formålet legger begrensninger, kan dette være til hinder for overføring. At formålsangivelsen ikke omhandler overføring, kan derimot ikke være til hinder for overføring.

5.3 Personopplysningslovens virkeområde; den behandlingsansvarlige må være etablert i Norge

Det mest aktuelle – sett med norske øyne – er selvsagt situasjonen med behandlingsansvarlig i Norge og databehandler utenfor Norge; se nærmere om dette nedenfor i punkt 5.4. Først skal vi imidlertid se på situasjonen med databehandler i Norge og behandlingsansvarlig utenfor Norge.

Personopplysningsloven gjelder kun for behandlingsansvarlige som «*er etablert i Norge*», jf. POL § 4 (1). Kravet til etablering medfører at «*det må utføres aktivitet innenfor en forholdsvis fast struktur*»,[87] og den behandlingsansvarlige må ha «*tilstrekkelig tilknytning til Norge*».[88] At en behandlingsansvarlig anses for å være etablert i et land, medfører at dette landets personvernregler kommer til anvendelse på behandlingen av personopplysningene. For behandlingsansvarlige som er etablert innenfor EU/EØS-området, er en slik løsning «akseptabel» etter PVD siden disse landene har en lovgivning som gir tilfredsstillende personvern.

Behandlingsansvarlige etablert utenfor EU/EØS-området vil derimot ikke være underlagt tilsvarende personvernregler som i PVD. POL skal likevel gjelde for behandling når behandlingsansvarlig «*benytter hjelpemidler i Norge*», jf. POL § 4 (2). «Hjelpemidler» skal forstås vidt og teknologinøytralt,[89] og selv om det ikke er avklart etter norsk rett, må bestemmelsen trolig forstås slik at POL også gjelder når databehandleren i Norge kan sies å være et hjelpemiddel for den behandlingsansvarlige. Et unntak fra dette følger av POL § 4 (2) andre punkt for personopplysninger i transitt gjennom Norge. Dersom opplysninger går gjennom Norge fra eksempelvis fra USA til India, vil ikke dette være behandling underlagt POL. Dette er i tråd med at data i transitt ikke anses å være en overføring, se punkt 5.2 ovenfor.

87. PVD punkt 19 i fortalen og punkt 22 i fortalen til personvernforordningen.
88. Se kommentarene til § 4 i kapittel 16 i Ot.prp. nr. 92 (1998–99).
89. Se Artikkel 29-gruppens «Opinion 8/2010 on applicable law» av 16. desember 2010.

Etter personvernforordningen vil det her skje en utvidelse ved at all behandling som gjøres for en behandlingsansvarlig eller databehandler som er etablert i EU/EØS, vil omfattes av forordningens bestemmelser. Som etablert regnes en effektiv og faktisk utøvelse av aktiviteter gjennom en mer permanent struktur, og den juridiske organisasjonsform som er valgt, som f.eks. filial, er ikke avgjørende, se punkt 22 til fortalen. Forordningen kan også gjelde for behandlingsansvarlige og databehandlere som ikke er etablert i EU/EØS, dersom disse tilbyr varer eller tjenester rettet mot registrerte i EU/EØS, se punkt 23 til fortalen, eller overvåker adferden til EU/EØS-borgere, se punkt 24 til fortalen.

Behandlingsansvarlige etablert utenfor EU/EØS-området som benytter hjelpemiddel i Norge, skal ha en representant etablert i Norge, jf. POL § 4 (3). Det kan være hensiktsmessig at databehandleren er en slik representant, men den behandlingsansvarlige vil likevel være ansvarlig for behandlingen.[90] Det følger også av bestemmelsen at en databehandler da vil være underlagt de samme bestemmelser som den behandlingsansvarlige, noe som innebærer at databehandleren også vil være underlagt POLs regler for behandlingen.

Det er ikke krav om at databehandleren skal være etablert i Norge for at POL skal gjelde for denne. Men som det fremgår, vil databehandlerens behandling av personopplysninger være utledet av den behandlingsansvarliges behandlingsgrunnlag. Derfor vil reglene som gjelder for den behandlingsansvarlige i det land denne er etablert, gjelde tilsvarende for databehandler i Norge. Men som det følger av ovennevnte: Dersom den behandlingsansvarlige er etablert utenfor EU/EØS-området og bruk av databehandler kan anses å være et «hjelpemiddel» for den behandlingsansvarlige i Norge, vil likevel behandlingen reguleres av den norske personopplysningsloven.

Datatilsynet har generell tilsynskompetanse for behandling av personopplysninger i Norge, jf. POL § 42 (3) nr. 3, og Datatilsynet skal kontrollere databehandlers behandling av personopplysningene basert på den lovgivning som er gjeldende i det land hvor den behandlingsansvarlige er etablert.[91] Databehandleren vil uavhengig av hvor den behandlingsansvarlige anses å være etablert, være forpliktet til å følge kravene til informasjonssikkerhet etter POL § 13,

90. S. 87–88 i Johansen, Michal Wiik, Knut-Brede Kaspersen og Åste Marie Bergseng Skullerud (2001), *Personopplysningsloven. Kommentarutgave*, Universitetsforlaget.

91. S. 86 i Johansen, Michal Wiik, Knut-Brede Kaspersen og Åste Marie Bergseng Skullerud (2001), *Personopplysningsloven. Kommentarutgave*, Universitetsforlaget

og tilsyn etter disse reglene under norsk rett faller innenfor Datatilsynets kontrollområde.

Benytter databehandler i Norge en underdatabehandler som er etablert *innenfor* EU/EØS-land, kan det fritt overføres personopplysninger mellom databehandler og underdatabehandler, jf. POL § 29. Benytter databehandler i Norge underdatabehandler i land *utenfor* EU/EØS, dvs. såkalte tredjeland, vil det skje en overføring av personopplysningene til tredjeland, hvilket krever et grunnlag, se punkt 5.4 nedenfor.

For databehandlers bruk av underdatabehandler i tredjeland, dvs. land utenfor EU/EØS, ble det etter EU-kommisjonens beslutning av 5. februar 2010 innført standardbestemmelser/-avtaler som medfører at databehandler kan overføre personopplysninger til underdatabehandlere, se punkt 5.4.6 nedenfor.

Overføring av personopplysninger til underdatabehandler i tredjeland må registreres av databehandleren i den oversikt som databehandleren plikter å føre etter reglene i forordningens artikkel 30 nr. 2, se punkt 4.6 ovenfor.

5.4 Behandlingsansvarlig i Norge, databehandler utenfor Norge

5.4.1 Oversikt

Er den behandlingsansvarlige etablert i Norge og det benyttes databehandler etablert i utlandet, kan overføring av personopplysninger til utlandet kun skje dersom kravene i POL §§ 29 og 30, jf. POF kapittel 6, er oppfylt. Som et utgangspunkt kan personopplysninger *bare* overføres til land som sikrer en forsvarlig behandling av personopplysningene, jf. POL § 29.

Det er imidlertid en rekke unntak fra dette utgangspunktet, og etter POL § 30 kan personopplysninger unntaksvis også overføres til land som ikke anses å ha et tilfredsstillende personvernnivå, se punkt 5.4.3 til 5.4.5 nedenfor. Bestemmelsen er tilnærmet lik artikkel 26 i PVD, og hvordan andre EU/EØS-land praktiserer bestemmelsen, kan dermed være relevant. Det må imidlertid understrekes at det bare unntaksvis er grunnlag for slik overføring. Artikkel 29-gruppen gir som generell anbefaling[92] at overføring til stater som ikke sikrer

92. Se Artikkel 29-gruppens workpaper nr. 114 på s. 9.

forsvarlig behandling av personopplysninger, skjer gjennom EU-kommisjonens standardbestemmelser, se punkt 5.4.6 nedenfor eller bindende virksomhetsregler, se punkt 5.4.7 nedenfor (eller eventuelt gjennom EU-US Privacy Shield som nå er et alternativ, se punkt 5.4.8 nedenfor).

Systematikken i forordningen er noe annerledes enn i PVD og POL. Etter forordningen kan personopplysninger overføres til tredjeland av den behandlingsansvarlige eller av databehandler dersom den som overfører har gitt tilstrekkelige garantier, rettigheter for de registrerte kan håndheves, og det er tilstrekkelige rettsmidler tilgjengelig for håndhevelse, jf. artikkel 46 nr. 1. Etter forordningen kan altså en databehandler velge å overføre personopplysninger selv *uten* godkjenning fra den behandlingsansvarlige og uten godkjenning fra tilsynsmyndighet (som Datatilsynet) dersom vilkårene i forordningen er til stede. Dette er en vesentlig utvidelse av retten til overføring til tredjeland i forhold til gjeldende rett.

Som «tilstrekkelige garantier» er det gitt alternativer i artikkel 46 nr. 2: som et rettslig bindende instrument (dvs. kontrakt eller lignende) som kan håndheves mellom offentlige myndigheter eller organer, bindende virksomhetsregler (se punkt 5.4.7 nedenfor), standardbestemmelser (se punkt 5.4.6 nedenfor), godkjente adferdsregler og godkjent sertifisering sammen med bindende tilsagn. I tillegg kan personopplysninger overføres på grunnlag av avtale mellom den som overfører personopplysningene (som kan være den behandlingsansvarlige og databehandler), og den som mottar opplysningene (som kan være databehandler eller underdatabehandler), dersom det foreligger godkjenning fra tilsynsmyndighet (som Datatilsynet) etter mekanismen i artikkel 63. Tilsvarende gjelder for overføring som del av administrativ ordning mellom offentlige myndigheter.

Nytt i forordningen er overføring på grunnlag av godkjente adferdsregler og sertifisering, samt kodifiseringen av regler for overføring etter bindende virksomhetsregler. Det er ikke klart i forordningen hvordan adferdsregler og sertifisering skal gi grunnlag for overføring, men adferdsreglene og sertifiseringen skal utarbeides og godkjennes etter reglene i artikkel 41 til 44; se om overholdelse av adferdsregler i punkt 4.6 ovenfor. I særlige situasjoner kan overførsel skje på grunnlag av samtykke fra registrerte, se artikkel 49 nr. 1 bokstav a. Samtykke er etter gjeldende rett det mest praktiske grunnlaget, såfremt det ikke er overføring av personopplysninger for et stort antall registrerte hvor det kan være vanskelig å innhente samtykke. Imidlertid har det vist seg vanskelig å praktisere overføring på grunnlag av samtykke, pga. faren for at samtykke trekkes tilbake (se punkt 5.4.3 nedenfor). Derfor legger forordningen opp til at andre grunnlag fortrinnsvis skal benyttes.

5.4.2 Kravet til forsvarlig vernenivå

Hovedregelen for overføring av personopplysninger ut av Norge er, som nevnt, at overføring kun kan skje til land som sikrer en forsvarlig behandling av personopplysningene, jf. POL § 29. Medlemslandene i EU/EØS har gjennomført PVD og vil oppfylle dette kravet. Dersom de generelle kravene til behandling av personopplysninger er oppfylt, er det derfor ingen begrensninger på overføring av personopplysninger til databehandler i EU/EØS-området.[93] For land utenfor EU/EØS stilles det krav til at personvernlovgivningen i det land databehandleren er lokalisert, har et «forsvarlig vernenivå».

Etter forordningen gjelder tilsvarende krav hvor overførsel til tredjeland eller internasjonal organisasjon, eller overføring videre derfra, kun kan skje dersom tredjelandet eller organisasjonen har et «tilstrekkelig[94] beskyttelsesnivå», jf. artikkel 45 nr. 1. Vurderingen av om et land har et tilstrekkelig beskyttelsesnivå, skal gjøres av EU-kommisjonen, og kriteriene som er listet opp i artikkel 45 nr. 2, legges til grunn for vurderingen. Kommisjonen kan også godkjenne sektorer i tredjeland for å ha tilstrekkelig beskyttelsesnivå, f.eks. finanssektoren i et land. Tredjeland og sektorer skal være gjenstand for ny vurdering minimum hvert fjerde år.

Etter forordningens artikkel 27, jf. artikkel 4 nr. 17, skal databehandler som ikke er etablert innenfor EU/EØS, skriftlig oppnevne en representant som skal være etablert innenfor EU/EØS. Dette er et krav som ikke er inntatt i PVD eller POL. Kravet til representant gjelder ikke dersom behandlingen er sporadisk og ikke i særlig stort omfang omfatter behandling av sensitive personopplysninger (omtalt som «særlige kategorier av personopplysninger» i forordningen, se artikkel 9 nr. 1).

---

93. Overføring innenfor EU/EØS er imidlertid ikke helt uproblematisk siden direktivet er implementert ulikt i de enkelte land, slik at det ikke er tilsvarende personvernlovgivning i de enkelte land. Eksempelvis er det en snevrere forståelse av hvilke opplysninger som anses som personopplysninger, i Storbritannia enn i Norge. Slike utfordringer vil forhåpentligvis forsvinne ved ikrafttredelse av personvernforordningen, se punkt 1 ovenfor.
94. Selv om det benyttes «tilstrekkelig» i forordningen (i den danske versjonen) og PVD benyttet «forsvarlig», så benyttes «adequate level of protection» i den engelske teksten både for PVD og forordningen, så det skal ikke bli noen endring i kravet til beskyttelsesnivå ved forordningen.

Den største gruppen land som *uten videre* anses å sikre forsvarlig behandling av personopplysninger, er EU/EØS-landene. Dette fremgår ikke klart av POL § 29, men er utvilsomt. Hva gjelder land utenfor EU/EØS, skal det etter bestemmelsen foretas en *nærmere vurdering* av om det aktuelle mottakerlandet sikrer en forsvarlig behandling av personopplysningene.

Det fremgår ikke av bestemmelsen *hvem* som skal foreta vurderingen etter § 29. Ettersom bestemmelsene retter seg mot den behandlingsansvarlige, må det i utgangspunktet være den behandlingsansvarlige som må foreta denne vurderingen, selv om Datatilsynet har en sentral veiledningsfunksjon ved vurderingen.[95] I praksis vil man imidlertid forholde seg til EU-kommisjonens godkjenning av land med tilstrekkelig vernenivå, se nedenfor, siden den behandlingsansvarlige sjelden er i stand til selv å foreta en slik vurdering.

POF § 6-2 bryter med ovennevnte, siden det forutsettes at vurderingen kan gjøres av Datatilsynet. Denne bestemmelsen må imidlertid forstås slik at dette gjelder *i andre tilfeller* hvor Datatilsynet foretar en vurdering av personvernnivået i et land, eksempelvis dersom det gis tillatelse til overføring i et enkelt tilfelle etter POF § 6-2 (2). Foretas en slik vurdering av Datatilsynet, foreligger det en plikt til å informere EU-kommisjonen og de øvrige EU/EØS-land dersom Datatilsynet kommer til at et land ikke sikrer forsvarlig behandling av personopplysninger. EU-kommisjonen kan overprøve Datatilsynets beslutning, og Datatilsynet er forpliktet til å etterleve EU-kommisjonens beslutning, jf. POF § 6-2 (3).

Etter POL § 29 (2) skal bl.a. personopplysningenes art og behandlingens formål og varighet vektlegges i vurderingen. I tillegg vil de rammer som vedkommende lands regler oppstiller, ha betydning, som landets rettsregler og sikkerhetstiltak, og også regler for god forretningsskikk i vedkommende land.[96] Andre forhold vil også kunne være relevante, jf. PVD artikkel 25 nr. 2 hvor det fremgår at «*alle forhold som har innflytelse på overføringen eller på en kategori overføringer*», skal vurderes. Etter direktivet vil forskjellene mellom de norske personvernreglene og reglene i landet hvor databehandleren er lokalisert, være relevant.

---

95. Se merknader til § 29 i kapittel 16 i Ot.prp. nr. 92 (1998–99). Dette er tilsvarende som i andre EU-land, bl.a. Danmark, se Peter Blume, *Databeskyttelsesret*, 3. utgave 2008, s. 317.
96. Se merknader til § 29 i kapittel 16 i Ot.prp. nr. 92 (1998–99).

EU-kommisjonens beslutninger etter PVD artikkel 25 og 26 om hvilke land som sikrer forsvarlig behandling av personopplysninger, vil også ha virkning for Norge, med den følge at personopplysninger kan overføres til disse landene med hjemmel i POL § 29 (1), jf. POF § 6-1. Det er Artikkel 29-gruppen som foretar vurderinger av de enkelte tredjeland, og selv om gruppens synspunkter ikke er juridisk bindende, vil vurdering av tredjeland stort sett etterkommes av EU-kommisjonen.[97] Per i dag har EU-kommisjonen besluttet at Andorra, Argentina, Canada, Færøyene, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Sveits og Uruguay skal anses å ha et tilfredsstillende beskyttelsesnivå, men beslutningene tas opp til ny vurdering regelmessig.[98] Artikkel 29-gruppen legger spesielt vekt på reglene om re-eksport av personopplysninger og hvordan disse praktiseres i tredjeland, siden re-eksport vil underminere reglene om forsvarlig behandling i mottakerlandet.[99]

5.4.3 Samtykke som grunnlag for overføring

Den mest praktiske hjemmelen for overføring av personopplysninger, avhengig av hvor mange registrerte det gjelder, er at de registrerte har samtykket til overføringen av opplysninger. Samtykke er et grunnlag for overføring til tredjeland etter POL § 30 (1) punkt a.

Samtykke må være frivillig, uttrykkelig og informert, jf. POL § 2 nr. 7. For de konkrete kravene til samtykke etter POL vises det til generell personvernrettslig litteratur. Her er det tilstrekkelig å vise til at kravet om informert samtykke innebærer at registrerte er innforstått med hvordan opplysningene skal behandles og hvilken risiko behandling og overføring av personopplysningene over landegrensene innebærer. De registrerte må derfor minimum være informert om at opplysningene vil bli behandlet av databehandler i utlandet, eventuelt av underdatabehandler, og at opplysningene overføres til tredjeland med angivelse av landet (eventuelt jurisdiksjon).[100]

---

97. Se s. 313–314 i Blume, Peter (2008), *Databeskyttelsesret*, Djøf Forlag.
98. Se EU-kommisjonens nettsider (http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm), hvor også prosessen for godkjennelse er beskrevet nærmere.
99. Se fotnote 97.
100. Annerledes i Johansen, Michal Wiik, Knut-Brede Kaspersen og Åste Marie Bergseng Skullerud (2001), *Personopplysningsloven. Kommentarutgave*, Universitetsforlaget, s. 220, som stiller strengere krav til samtykket.

Kravet om at samtykket skal være spesifikt er ikke klart etter den norske lovteksten, men det fremkommer av direktivteksten at det er den foreslåtte eller forestående overføringen det skal samtykkes til.[101] Samtykke er således ikke egnet som grunnlag for fremtidige overføringer som er vagt eller uklart angitt.[102] Registrerte må informeres om den risiko overføringen av personopplysningene til et land som ikke sikrer tilstrekkelig beskyttelse innebærer,[103] og den informasjon som den registrerte gis før samtykke eventuelt avgis må være tilstrekkelig til at den registrerte kan gjøre et reelt valg.[104] Dersom de registrerte samtykker til overføringen og samtykket er tilstrekkelig, kan ikke Datatilsynet gripe inn og nekte overføringen.[105] Hvis derimot samtykket ikke er dekkende, vil overføringen være ulovlig etter POL § 29, se punkt 4.5 ovenfor.

Et samtykke kan til enhver tid trekkes tilbake av den registrerte, noe som vanskeliggjør overføring til databehandler basert på samtykke.[106] Dette er et forhold som den behandlingsansvarlige bør hensynta dersom samtykke skal benyttes som grunnlag for overføringen.

Hvordan tilbaketrekking av samtykke fra en eller flere registrerte skal håndteres, bør reguleres i databehandleravtalen. Det vil normalt ikke være stor risiko for at samtykke til overføring til databehandler i tredjeland blir trukket tilbake, men konsekvensene ved at samtykke trekkes tilbake, vil i enkelte tilfeller kunne ha omfattende økonomisk og/eller teknisk betydning for den behandlingsansvarlige. Spesielt dersom det leveres driftstjenester fra databehandleren, vil det være problematisk for den behandlingsansvarlige å behandle personopplysningene selv eller benytte databehandler i Norge eller EU/EØS-land for de registrerte som har trukket tilbake sitt samtykke.

---

101. Se Jørgen Skorstad på s. 190 i Blixrud, Katrine Berg og Christine Ask Ottesen (2010), *Personvern i finanssektoren*, Gyldendal.
102. Se også Artikkel 29-gruppens Workpaper 114 på s. 12.
103. Se Artikkel 29-gruppens Workpaper nr. 12 på s. 25, hvor det også fremkommer at manglende informasjon om risikoen medfører at samtykket ikke gir grunnlag for overføring.
104. Se Artikkel 29-gruppens opinion nr. 12/2011 WP 183.
105. Se fotnote 93.
106. Se Artikkel 29-gruppens Workpaper 114 hvor bruk av samtykke til overføring av personopplysninger til samordnet HR-database ble ansett å være vanskelig pga. retten for den enkelte til å trekke samtykket tilbake.

Den behandlingsansvarlige bør være påpasselig med at det foreligger dekkende samtykke, siden en overføring vil kunne være irreversibel når opplysninger først er overført til et land som ikke sikrer forsvarlig behandling av personopplysninger.

Som nevnt ovenfor kan samtykke fra de registrerte også gi grunnlag for overføring etter forordningen, men etter forordningens systematikk er det en forutsetning at de øvrige grunnlag ikke er anvendelige, se artikkel 49. Som etter gjeldende rett skal det foreligge et *informert* samtykke, hvor spesielt de mulige risikoelementer ved overføringen skal informeres om, siden overføring vil skje til et land som ikke har tilstrekkelig beskyttelsesnivå, jf. artikkel 45. At samtykke først skal benyttes dersom de primære grunnlagene ikke foreligger, kan vanskelig ses som et reelt grunnlag for å avslå overføring på grunnlag av samtykke, se nedenfor.

5.4.4 *Grunnlag som følge av avtale, for å ivareta interesser og som følge av rettskrav*

Overføring kan også skje dersom overføringen er *nødvendig* for å oppfylle en avtale med registrerte, for å utføre gjøremål etter registrertes ønske før en slik avtale inngås, for å inngå eller oppfylle en avtale med en tredjeperson i registrertes interesse, for å vareta registrertes vitale interesser, eller for å fastsette, gjøre gjeldende eller forsvare et rettskrav, se POL § 30 bokstav c, d, e og f.

For at dette skal kunne tjene som grunnlag for overføring av personopplysninger til databehandler i annet land, er det en forutsetning at dette gjøres for å oppfylle avtale, utføre gjøremål mv., og ikke kan gjøres ved at opplysningene behandles i Norge eller land som sikrer forsvarlig behandling av personopplysninger, jf. kravet om at overføringen er «*nødvendig*» i lovbestemmelsen. Har databehandleren kompetanse som ikke finnes i Norge eller land som sikrer personvernet tilstrekkelig, kan dette begrunne overføringen, men dette vil kun gjelde i helt spesielle tilfeller. I de nevnte tilfeller følger det også at overføringen må være i registrertes interesse.

Økonomiske motiver hos den behandlingsansvarlige for å overføre opplysningene, som at databehandleren behandler opplysningene til lavere kostnader enn databehandlere i andre land, er ikke tilstrekkelig til at overføringen anses nødvendig. Dette gjelder også dersom behandlingen vil være rimeligere for registrerte, hvis det er den registrerte som betaler for behandlingen. Den behandlingsansvarlige bør i slike tilfeller heller benytte samtykke som grunn-

lag for overføringen, noe som trolig vil være mest hensiktsmessig i de fleste av de nevnte forholdene.[107]

De øvrige unntak etter POL § 30, som folkerettslig plikt til overføring som følge av medlemskap i internasjonal organisasjon, for å beskytte viktig samfunnsinteresse, eller overføring fra offentlig register som følge av lovmessig rett, er mindre praktisk med hensyn til bruk av databehandler i utlandet, og vil ikke gjennomgås nærmere her.

Også etter forordningen gir de ovennevnte forhold grunnlag for overføring til tredjeland, men forordningens systematikk er at de grunnlag som er nevnt innledningsvis ovenfor, som overføring til land som gir betryggende beskyttelse, bruk av bindende virksomhetsregler mv., bør anvendes før grunnlagene som nevnt i POL § 30 benyttes, se forordningens artikkel 49. At grunnlagene i artikkel 49 først skal benyttes dersom de primære grunnlagene ikke foreligger, kan imidlertid vanskelig ses som grunn nok til å avslå overføring etter artikkel 49. Bestemmelsen må snarere forstås som et ønske om at man søker å benytte de primære grunnlagene i artikkel 45, 46 og 47 før man benytter grunnlagene i artikkel 49.

Etter forordningen kan videreoverføring av personopplysninger til andre tredjeland skje dersom det er en éngangsoverføring, personopplysningene gjelder kun et begrenset antall registrerte, og er nødvendig av legitime interesser som følges opp av den behandlingsansvarlige. Det kreves også at den registrertes interesser ikke har større vekt enn de nevnte legitime interesser, at alle forhold er vurdert av den behandlingsansvarlige, og at det er gitt tilstrekkelige garantier for beskyttelse av personopplysningene, se nærmere i artikkel 49 nr. 1 i.f. En tilsvarende regulering er ikke i gjeldende regelverk i PVD eller POL, men dette er et meget snevert unntak ettersom alle de nevnte kravene til videreoverføring er kumulative og må således foreligge. Det er også klart fra bestemmelsen at en videreoverføring kan ikke foretas av databehandleren uten at den behandlingsansvarlige har godkjent videreoverføring og har medvirket til denne. Alle vurderinger og garantier i forbindelse med videreoverføring skal dokumenteres av den behandlingsansvarlige og databehandleren, jf. artikkel 49 nr. 6.

107. Tilsvarende i Johansen, Michal Wiik, Knut-Brede Kaspersen og Åste Marie Bergseng Skullerud (2001), *Personopplysningsloven. Kommentarutgave*, Universitetsforlaget, s. 220–221.

5.4.5 Tillatelse fra Datatilsynet til overføring

Datatilsynet kan i enkelte tilfeller tillate overføring selv om det ikke foreligger grunnlag for overføring etter POL § 30 bokstav a til h, se POL § 30 (2). Slik tillatelse kan imidlertid kun gis dersom den behandlingsansvarlige «*gir tilstrekkelige garantier for vern av den registrertes rettigheter*». Det må i slike tilfeller innhentes tillatelse fra Datatilsynet *før* overføringen foretas.

Vurderingen fra Datatilsynet vil ta utgangspunkt i personvernhensynet til de registrerte, herunder hva slags opplysninger som skal overføres, formålet med behandlingen og over hvor lang tid behandlingen skal foregå hos databehandleren, som holdes opp mot personvernbeskyttelsen i landet hvor databehandleren er lokalisert.[108] Datatilsynet vil kunne stille vilkår i tillatelsen til overføring. Tillater Datatilsynet overføring etter denne bestemmelsen, skal Datatilsynet gi melding til EU-kommisjonen og øvrige medlemsstater i EU/EØS om at slik tillatelse er gitt.

Når det gjelder garantier som den behandlingsansvarlige kan gi, har Datatilsynet akseptert databehandleravtaler mellom behandlingsansvarlig og databehandler, og hvor sistnevnte påtar seg å behandle personopplysningene i overensstemmelse med norsk personvernlovgivning, som tilstrekkelig garanti. Andre garantier som er godtatt, er EU-kommisjonens standardbestemmelser, se punkt 5.4.6, og bindende virksomhetsregler som er omtalt i punkt 5.4.7 nedenfor. Siden det er omfattende muligheter til overføring etter POL § 30 (1), spesielt ved samtykke, må det foreligge tungtveiende grunner for at Datatilsynet skal gi samtykke etter bestemmelsens andre avsnitt. Datatilsynet anbefaler derfor at man heller bruker EU-kommisjonens standardbestemmelser eller bindende virksomhetsregler for overføringen.

Eventuelle overføringer skal oppgis i melding til Datatilsynet, dersom slik er pålagt, og i eventuell konsesjonssøknad hvor databehandleren må oppgis, se punkt 2.3 ovenfor.

5.4.6 EU-kommisjonens standardbestemmelser

Som det fremgår ovenfor, er det få tredjeland som EU-kommisjonen anser for å ha et tilfredsstillende personvernnivå, og de vesentligste land i databehand-

108. Se www.datatilsynet.no.

lersammenheng, som India, Australia og USA, er ikke blant disse. Samtykke eller de øvrige grunnlagene for overføring vil heller ikke normalt være aktuelle eller praktisk anvendbare ved bruk av databehandler i tredjeland. Bruk av databehandler er i dag praktisk ved ulike tjenestebaserte it-ytelser, som drifts- og lagringstjenester samt tjenestebasert programvare og andre tjenester over internett, og endringer i leveransemodellene over mot mer globaliserte og sømløse løsninger vil, som nevnt, aktualisere overføring av personopplysninger til tredjeland ytterligere.

EU-kommisjonen har derfor utviklet et sett standardbestemmelser (standardkontrakter) for overføring av personopplysninger til tredjeland, som nå er den mest praktiske løsningen for overføring av personopplysninger til databehandler der samtykke fra de registrerte er vanskelig å innhente.[109]

Standardbestemmelsene er utarbeidet med hjemmel i PVD artikkel 26 nr. 4, jf. artikkel 31 nr. 2, og skal gi tilstrekkelig garantier fra den behandlingsansvarlige for at personopplysninger som overføres til tredjeland, blir forsvarlig behandlet der. Artikkel 26 nr. 4 er implementert i norsk rett ved POL § 30 (2), og etter POF § 6-1 skal Datatilsynet etterleve beslutninger av EU-kommisjonen. Artikkel 26 nr. 4 viser imidlertid til at standardbestemmelser *kan* gi tilfredsstillende garantier, slik at bruken av bestemmelsene ikke er tilstrekkelig *i seg selv* til at overføring skal kunne gjennomføres. Det må i tillegg gis en tillatelse av Datatilsynet, som følger forutsetningsvis av POL § 30 (2).

To av standardkontraktene som er utarbeidet av EU-kommisjonen etter artikkel 26 nr. 4, gjelder for overføring til *behandlingsansvarlig* i tredjeland som skal bruke personopplysningene til eget formål.[110] I 2002 kom det standardbestemmelser for overføring til *databehandler* i tredjeland,[111] som fra 15. juni 2010 ble erstattet av nye vilkår.[112]

Databehandler kan ikke benytte underdatabehandler uten at den behandlingsansvarlige har samtykket til dette, se punkt 4.4 ovenfor. Behandlingsansvarlig som er etablert i Norge, og dermed underlagt POL, må derfor samtykke

109. Standardkontraktene finnes på Datatilsynets nettsider, på dansk og engelsk: https://www.datatilsynet.no/Regelverk/Internasjonalt/Overfoering/.
110. EU-kommisjonens beslutning 2001/497/EC og 2004/915/EC.
111. EU-kommisjonens beslutning 2002/16/EC.
112. EU-kommisjonens beslutning 2010/87/EU.

til bruk av underdatabehandler uavhengig av hvor databehandleren er lokalisert. Dette gjelder også hvor personopplysningene er overført på grunnlag av samtykke, EU-kommisjonens standardbestemmelser eller etter bindende virksomhetsregler.

En målsetting med standardbestemmelsene fra 2010 var å hensynta databehandlingens raske utbredelse globalt og over internett, og regulere forhold som ikke var omfattet av 2002-versjonen av standardbestemmelsene.[113] Standardbestemmelsene av 2010 har derfor som formål å dekke mer komplekse «utkontrakteringsmodeller», og skal gjøre det mulig for databehandlere utenfor EU/EØS å benytte underdatabehandler som også er lokalisert utenfor EU/EØS.

Den reviderte versjonen av standardbestemmelsene for bruk av databehandlere i 2010 kom etter press fra globale aktører som ønsket å ha én avtale mellom kunden (behandlingsansvarlig) og leverandøren (databehandleren) som dekker også leverandørens bruk av underdatabehandlere og databehandler-til-databehandler-overføring av personopplysninger. 2010-versjonen av standardbestemmelsene gjør det enklere å overføre data utenfor EU/EØS ved at en rekke av de begrensninger som gjaldt tidligere for overføring av personopplysninger, blir fjernet. Tidligere var det ikke anledning for databehandlere til å benytte seg av underdatabehandlere uten at det var inngått direkte avtale mellom behandlingsansvarlig og underdatabehandleren. Dette var tungvint og problematisk for databehandlere, siden dette eksponerte deres underdatabehandlere direkte for kundene. Etter gjeldende standardbestemmelser for overføring til databehandler kan nå underdatabehandlere som er lokalisert i lavkostland uten tilstrekkelig personvernlovgivning, benyttes, forutsatt at behandlingsansvarlig har gitt skriftlig forhåndssamtykke til bruk av underdatabehandlere.[114]

Overføring etter standardbestemmelsene av 2010 kan kun gjennomføres dersom databehandleren og underdatabehandleren er etablert i tredjeland. Er databehandleren etablert innenfor EU/EØS, må altså andre regler benyttes ved overføring til underdatabehandleren hvis ikke behandlingsansvarlige skal overføre direkte til databehandlerens underdatabehandler.

113. EU-kommisjonen har også vært utsatt for et ikke ubetydelig press fra it-industrien for å endre standardbestemmelsene og gjøre det enklere å overføre personopplysninger til tredjeland.

114. Se punkt 11 i standardkontrakten av 2010. Det følger her at underleverandør (underdatabehandler) kan inngå avtale med databehandleren ved å undertegne på kontrakten som er inngått mellom den behandlingsansvarlige og databehandleren.

Benytter databehandleren underdatabehandler i tredjeland, vil det gjelde andre forutsetninger for overføringen etter kommisjonens beslutning, som at den behandlingsansvarlige gir forhåndssamtykke til bruk av underdatabehandler. Slikt forhåndssamtykke kan gis i avtalen med databehandleren, og databehandleren inngår skriftlig avtale med underdatabehandleren hvor de samme vilkårene som gjelder mellom den behandlingsansvarlige og databehandleren om behandling av personopplysninger, inntas. Databehandleren vil også være ansvarlig overfor den behandlingsansvarlige for den databehandling som underdatabehandleren foretar, til tross for hva som ellers måtte være avtalt med underdatabehandleren. Det må også inntas en skadesløsholdelseserklæring mellom databehandleren og underdatabehandleren i tilfelle en tredjepart blir skadelidende for brudd på avtalen om databehandling mellom partene.

Standardbestemmelsene stiller krav til databehandlerens bruk av underdatabehandler, bl.a. ved at den behandlingsansvarlige samtykker til bruk av underdatabehandler, at det inngås skriftlig avtale mellom databehandleren og underdatabehandleren, hvor sistnevnte påtar seg samme plikter som databehandleren, og at avtalen med underdatabehandleren reguleres av samme lovgivning som standardbestemmelsene er underlagt. Sistnevnte innebærer at en avtale med amerikansk databehandler med underdatabehandler i India er underlagt norsk personvernlovgivning dersom den behandlingsansvarlige er norsk.

Standardbestemmelsene dekker *direkte* bare overføring av data fra behandlingsansvarlig etablert i EU/EØS til databehandler utenfor EU/EØS som benytter underdatabehandler utenfor EU/EØS, og ikke overføring fra databehandler i EU/EØS til underdatabehandler utenfor EU/EØS.[115] Det kan likevel være at Datatilsynet vil godkjenne avtalen for sistnevnte bruk, og det er gode grunner for at tilsynet skal gjøre dette siden situasjonen hvor databehandleren er utenfor EU/EØS, ikke er vesentlig annerledes. Det er forutsatt at standardbestemmelsene kan benyttes mellom behandlingsansvarlig og databehandleren (som begge er etablert i EU/EØS), og mellom databehandleren og underdatabehandleren (hvor sistnevnte er utenfor EU/EØS), med nødvendige tilpasninger.[116]

115. Se punkt 23 i fortalen til 2010/87/EU.

116. Artikkel 29-gruppen har utformet utkast til standardbestemmelser for overføring av personopplysninger fra databehandler i EU/EØS til underdatabehandler i tredjeland, se Working document 01/2014 av 21. mars 2014.

Selv om standardbestemmelsene tar sikte på å gjøre administrasjonen enklere, påhviler det partene ved en utkontraktering som involverer behandling og overføring av personopplysninger, en del forpliktelser som kan oppfattes som omstendelige. Eksempelvis må det utarbeides en liste over avtaler med underdatabehandlere som skal være tilgjengelig for tilsynsmyndigheten (Datatilsynet), som revideres minst årlig, og alle underdatabehandlere må akseptere å overholde lovgivningen i det land den behandlingsansvarlige er etablert. Artikkel 29-gruppen har presisert at det kun er avtaler som dataeksportøren (dvs. den behandlingsansvarlige) er part i, som skal forelegges for Datatilsynet (eller tilsvarende myndighet i andre EU/EØS-land). Og for underdatabehandlere skal det kun utarbeides en liste over underdatabehandlere som mottas fra dataimportøren (dvs. databehandleren).

Standardbestemmelsene dekker heller ikke det forhold at man benytter databehandler innenfor EU/EØS som så benytter underdatabehandler utenfor EU/EØS, og den behandlingsansvarlige er normalt henvist til å inngå standardbestemmelsene direkte med underdatabehandleren i slike tilfeller, jf. ovenfor.

De registrerte er ikke part i standardkontraktene, men avtalene er utformet som tredjepartsløfter som begunstiger de registrerte direkte, og hvor de registrerte har rettigheter og mulighet til sanksjoner ved mislighold av bestemmelsene fra kontraktspartenes, dvs. den behandlingsansvarlige og databehandleren, side.

Når det gjelder direktekrav mot underdatabehandlere, kan ifølge standardbestemmelsene slike krav bare fremmes hvis krav ikke kan gjøres gjeldende overfor databehandleren, dvs. et subsidiært ansvar. For at det skal bli aktuelt med slike direktekrav, må imidlertid underdatabehandleren også inngå EU-kommisjonens standardbestemmelser. Standardbestemmelsene er imidlertid ikke utformet slik at underdatabehandleren også skal inngå disse, så underdatabehandleren må ha tiltrådt avtalen eller det må foreligge annet grunnlag dersom underdatabehandleren skal være ansvarlig. De registrerte må trolig også kunne fremme krav om erstatning for ikke-økonomisk tap etter POL § 29 overfor den behandlingsansvarlige, og eventuelt databehandler eller underdatabehandler, dersom det forekommer brudd på POL i forbindelse med bruken av databehandler i tredjeland.

Datatilsynet er også gitt en rekke beføyelser som er inntatt som egne bestemmelser i standardkontraktene, som partene må akseptere dersom standard-

kontraktene skal kunne benyttes. Beføyelsene gir tilsynsmyndigheten rett til å pålegge utlevering av informasjon, og til å gjennomføre inspeksjon knyttet til overføringen av tilsynsmyndigheten selv eller ved andre. Sistnevnte er basert på at Datatilsynet skal påse at personopplysningene er tilstrekkelig beskyttet også etter overføringen,[117] og inspeksjon kan foretas hos databehandleren og eventuelle underdatabehandlere av denne, og det kan gis pålegg overfor nevnte. Datatilsynet kan også forby eller suspendere tillatelsen til å overføre personopplysninger eller kategorier opplysninger i særlige tilfeller.

Etter standardbestemmelsene skal de registrerte informeres dersom det skjer en overføring av sensitive personopplysninger.[118] Dette vil i enkelte tilfeller vanskeliggjøre bruk av databehandler i tredjeland på grunnlag av standardbestemmelsene, siden det å informere alle registrerte vil kunne være en omfattende oppgave.

Standardbestemmelsene inneholder plikter for partene knyttet til behandling av personopplysninger, og medfører strenge rammer for hvordan opplysningene kan overføres og skal håndteres av databehandleren. Partene kan supplere standardbestemmelsene med andre bestemmelser, og gjøre endringer i standardbestemmelsene for å tilpasse dem til det konkrete behov, eller det kan utarbeides egne vilkår.

Det anbefales imidlertid at tilleggsvilkår mellom den behandlingsansvarlige og databehandler reguleres i egen avtale, og at det i minst mulig grad gjøres endringer i standardbestemmelsene slik de er utformet av EU-kommisjonen. Bakgrunnen er at behandlingen hos Datatilsynet tar langt kortere tid dersom det ikke gjøres endringer i standardbestemmelsene. Er standardbestemmelsene endret, må Datatilsynet vurdere vilkårene for å avgjøre om disse gir tilstrekkelig garanti for behandlingen. Etter forordningen åpnes det for å innta standardbestemmelsene i tjenesteavtaler eller andre kontrakter, se punkt 109 til fortalen, men det er trolig at endringer i standardbestemmelsene vil også øke behandlingstiden etter forordningen.

117. Se punkt 11 i fortalen til EU-kommisjonens beslutning av 5. februar 2010 om standardbestemmelser for overføring til databehandler (2010/87/EU).
118. For hva som omfattes av sensitive personopplysninger, se POL § 2 nr. 8. I enkelte andre land, som Danmark, kreves det godkjenning av overføring av sensitive opplysninger, men noe slikt krav gjelder ikke etter POL.

Selv om standardbestemmelsene benyttes, vil den behandlingsansvarlige være ansvarlig for eventuelle overtredelser av personvernreglene, også for overtredelser begått av databehandleren. Etter standardbestemmelsene kan den behandlingsansvarlige i slike tilfeller kreve erstattet tap denne er påført som følge av databehandlerens overtredelse av lovgivningen. Ved brudd på personvernlovgivningen av databehandlerens underdatabehandler, er det databehandleren som er ansvarlig.

De registrerte kan fremme krav om erstatning overfor den behandlingsansvarlige ved brudd på standardbestemmelsene, herunder krav som følge av overtredelse av POL. Dersom den registrerte ikke kan kreve erstatning fra den behandlingsansvarlige fordi sistnevnte har forsvunnet, er oppløst (som for juridiske personer) eller er insolvent, kan kravet fremsettes overfor databehandleren. I tilfelle kravet ikke kan fremsettes overfor databehandleren, kan den registrerte fremme kravet mot eventuelle underdatabehandlere av databehandleren.

Datatilsynet skal akseptere standardbestemmelsene som «*tilstrekkelige garantier for vern av den registrertes rettigheter*» etter POL § 30 (2), dersom det ikke foreligger spesielle forhold etter norsk rett eller knyttet til partene. Datatilsynet kan like fullt sette vilkår for tillatelsen eller nekte å gi tillatelse selv om standardbestemmelsene er benyttet, men dette er forutsatt av EU-kommisjonen til kun å gjelde unntaksvis.[119] Datatilsynet bruker noe tid på behandlingen av standardkontraktene ved overføring, og denne tidsbruken bør hensyntas ved planlegging.[120]

Å overføre personopplysninger til tredjeland etter standardbestemmelser er det også grunnlag for etter forordningen, hvor det kan gis standardbestemmelser enten av EU-kommisjonen, jf. artikkel 46 nr. 2 bokstav c, eller av en tilsynsmyndighet (som Datatilsynet) som må godkjennes av EU-kommisjonen, se artikkel 46 nr. 2 bokstav d. For å sikre sammenheng i

119. Se fotnote 110.

120. Pr. i dag bruker Datatilsynet to til seks uker på behandling av overførsel etter standardbestemmelsene, og kan bruke lengre tid dersom det er gjort endringer i standardbestemmelsene, eller det er benyttet annen avtale enn standardbestemmelsene. Merk også at dersom det foretas endringer i standardbestemmelsene, er ikke Datatilsynet forpliktet til å følge kommisjonens beslutning, som standardbestemmelsene er, jf. POF § 6-1 (4).

håndhevelsen av personvernforordningen skal tilsynsmyndigheten konferere med Databeskyttelsesrådet, jf. artikkel 64, før standardbestemmelser utstedes.

5.4.7 Bindende virksomhetsregler

Personopplysninger kan også overføres til tredjeland gjennom såkalte bindende virksomhetsregler («Binding Corporate Rules» eller BCR) dersom den behandlingsansvarlige benytter en databehandler som er del av egen virksomhet. Gjennom bindende virksomhetsregler for databehandlere («Binding Corporate Rules for Processors» eller BCRP) kan en databehandler som er etablert i Norge, overføre personopplysninger til annet konsernselskap i tredjeland.

Bindende virksomhetsregler er ikke regulert i POL, POF eller PVD (men er regulert i forordningen), og er frivillige retningslinjer som regulerer håndteringen av personopplysninger innad i *én virksomhet* eller mellom flere virksomheter i *ett konsern*. Bindende virksomhetsregler er spesielt praktiske for selskaper som har virksomhet i flere land, både som behandlingsansvarlig og som databehandler. De gir en mer smidig måte å kunne overføre personopplysninger på – når de bindende virksomhetsreglene er på plass i virksomheten – enn samtykke eller EU-kommisjonens standardbestemmelser.

Bruken av bindende virksomhetsregler er, som EU-kommisjonens standardbestemmelser, hjemlet i PVD artikkel 26 (2) som er implementert i norsk rett gjennom POL § 30 (2), selv om det ikke fremkommer noen direkte referanse til bindende virksomhetsregler i artikkelen. Bindende virksomhetsregler anses derfor som en garanti for vern av registrertes rettigheter etter POL § 30 (2), med den følge at Datatilsynet kan gi tillatelse til overføring av personopplysninger, men da kun innenfor virksomheten.

Bindende virksomhetsregler (BCR) benyttes når det er et konsern hvor konsernselskap i tredjeland skal være databehandler for andre av selskapets konsernselskapers personopplysninger.[121] I databehandlersammenheng vil bindende virksomhetsregler være aktuelle dersom det benyttes «shared services» i

121. BCR er «Binding Corporate Rules (BCR) for Controllers» («BCR for your own data»). BCR ble introdusert i 2003 av Artikkel 29-gruppen og har i en rekke dokumenter gitt prosedyrene for bruk av BCR, se spesielt Working Paper 74, 107 og 108. Andre dokumenter som gir veiledning for bruk av BCR, er Working Paper 133, 153, 154 og 155.

en virksomhet, dvs. at en enhet eller et selskap utfører databehandleroppgaver for andre deler av virksomheten. Denne enheten må være del av eller eget selskap som anses å være en del av virksomheten, men må være en egen enhet for å anses å være databehandler, jf. punkt 3.2 ovenfor. Kravet til samme virksomhet må i denne sammenheng medføre at både databehandleren og den behandlingsansvarlige er underlagt samme organisatoriske hierarki. Det er ikke klare krav til organisasjoner som skal kunne benytte bindende virksomhetsregler, men det er forutsatt at virksomhetsreglene skal være *bindende* i den forstand at selskaper i konsernet skal kunne pålegges reglene. En forutsetning er da at morselskapet kan pålegge de aktuelle selskapene i konsernet å følge de aktuelle reglene. Det avgjørende er dermed ikke at morselskapet er behandlingsansvarlig – det kan andre selskaper i konsernet være – men at virksomhetsreglene kan *ensidig pålegges* de øvrige selskaper i konsernet. Dette kan gjøres på flere måter, bl.a. gjennom avtaler mellom konsernselskapene, publisering av reglene, og policybeslutninger innad i konsernet. Det er ulik praksis ved de enkelte tilsynsmyndigheter i EU/EØS-landene, så det bør undersøkes hva som aksepteres i de enkelte land dersom BCR skal benyttes.

Bindende virksomhetsregler for databehandlere (BCRP) benyttes når det er et konsern som behandler personopplysninger på vegne av andre selskaper/konsern som databehandler.[122] Bindende virksomhetsregler for databehandlere er spesielt aktuelt dersom et selskap er databehandler for et annet selskap, og databehandlerselskapet ønsker å benytte konsernselskap, herunder datterselskap, i tredjeland for å behandle personopplysningene.

Virksomhetsreglene for databehandlere skal inntas som et vedlegg til avtalen mellom den behandlingsansvarlige og databehandleren, og med dette *«gi tilstrekkelige garantier for vern av den registrertes rettigheter»* etter POL § 30 (2). Men som for de andre overføringsgrunnlagene (herunder bindende virksomhetsregler og EU-kommisjonens standardbestemmelser) vil den behandlingsansvarlige forbli ansvarlig for at personopplysningene behandles betryggende i tredjelandet. Den behandlingsansvarlige har fortsatt et oppfølgingsansvar også

122. BCRP er «Binding Corporate Rules (BCR) for Processors» («BCR for third party data»). BCRP ble introdusert i juni 2012 i Working Paper 195 og 195a, og det sentrale dokumentet kom i april 2013 (Working Paper 204), som ble revidert i mai 2015.

ved bruk av bindende virksomhetsregler for databehandlere overfor databehandlerens konsernselskaper.

Det stilles krav til innholdet i avtalen mellom den behandlingsansvarlige og databehandleren i tilknytning til bindende virksomhetsregler for databehandlere. Avtalen skal bl.a. fastslå at den behandlingsansvarlige påtar seg å informere de registrerte om sensitive personopplysninger som skal behandles, at personopplysninger skal overføres til tredjeland, at både virksomhetsreglene for databehandlere og avtalen mellom den behandlingsansvarlige og databehandleren skal gjøres tilgjengelig for de registrerte, regulering av bruk av underdatabehandler i tredjeland mv.[123] Det er også krav til rutiner for å føre oppdatert oversikt over hvilke selskaper i databehandlerkonsernet og underdatabehandlere som har tilgang til personopplysningene, og rapportering av endringer til tilsynsmyndigheten.[124]

Databehandlerkonsernet må utpeke ett selskap innenfor EU/EØS som er ansvarlig overfor de registrerte for eventuelt personvernbrudd, mens den behandlingsansvarlige kan ved personvernbrudd rette krav mot ethvert selskap i databehandlerkonsernet, samt mot selskap etablert i EU/EØS. Det er etablert omvendt bevisbyrde under de bindende virksomhetsreglene for databehandlere; om de registrerte eller den behandlingsansvarlige er påført skade som sannsynligvis skyldes brudd på virksomhetsreglene (herunder på personvernreglene som virksomhetsreglene viser til), må det selskap i databehandlerkonsernet som har påtatt seg ansvar etter virksomhetsreglene for databehandlere, dokumentere at det *ikke* er databehandler som er ansvarlig for bruddet som medførte skaden, eller at brudd ikke har skjedd. For å sikre transparens er både den behandlingsansvarlige og databehandleren forpliktet til å gjøre virksomhetsreglene samt informasjon om rettighetene til de registrerte tilgjengelig på sine nettsider.[125]

Et selskap i konsernet som har etablert og fått godkjent bindende virksomhetsregler for databehandlere, kan benytte seg av underdatabehandlere til å behandle den behandlingsansvarliges personopplysninger. Men til tross for

123. Se Working Paper 204 (rev. 01 av 22. mai 2015) punkt 2.3.3.2 samt de prosessmessige og organisatoriske kravene i kapittel 4.

124. Se Working Paper 204 (rev. 01 av 22. mai 2015) punkt 3.2.

125. Det er rettighetene som er opplistet i punkt 2.3.3.1 i Working Paper 204 (rev. 01 av 22. mai 2015), som skal listes på nettsidene, se punkt 4.8.

at en virksomhet har etablert virksomhetsregler for databehandlere, er det påkrevd å søke godkjennelse fra tilsynsmyndighet for overføring av personopplysninger til databehandlerens underdatabehandlere, og å inngå skriftlig avtale for behandlingen av personopplysningene som pålegger de samme plikter for underdatabehandler som databehandleren er pålagt. Det er derfor ikke anledning til å overføre personopplysninger *utenfor eget konsern* etter virksomhetsreglene for databehandlere.

Tilsvarende som for EU-kommisjonens standardbestemmelser innebærer de bindende virksomhetsreglene at det avgis et tredjepartsløfte overfor de registrerte, som gir de registrerte direkte rettigheter.

Det er ingen krav til innholdet for bindende virksomhetsregler under gjeldende rett, men det er gitt veiledninger fra Artikkel 29-gruppen som er så eksplisitte at de bør følges. Det avgjørende er imidlertid at reglene må innebære at det etableres et akseptabelt beskyttelsesnivå for registrerte for behandlingen i tredjeland.

Bindende virksomhetsregler inngås for hele virksomheten/konsernet, men vil bare ha betydning for den del av virksomheten eller de konsernselskaper som er lokalisert og behandler personopplysninger i tredjeland. Det kan imidlertid være informasjonssikkerhetstiltak som vil påvirke virksomheten i EU/EØS-land også.

Prosedyren for å etablere bindende virksomhetsregler er i grove trekk:[126] Etter at virksomheten har utformet sine regler for håndtering av personopplysninger i virksomheten(e) som behandler opplysninger i tredjeland, må disse godkjennes av minst én tilsynsmyndighet innenfor EU/EØS. Den behandlingsansvarlige må avgjøre hvilken tilsynsmyndighet («Data Protection Authority» eller «DPA») som skal gi første vurdering og eventuell godkjennelse av reglene og styre prosessen mot de øvrige tilsynsmyndighetene i EU/EØS.[127] Denne myndigheten («Lead DPA») har frist på 15 dager (fristen kan utvides til maksimum én måned) til å gi tilbakemelding til den behandlingsansvarlige på sistnevntes bindende virksomhetsregler. Reglene bør utformes i tråd med vei-

126. For mer informasjon om prosedyrene vises det til EU-kommisjonens nettsider: http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/index_en.htm.

127. Etter forordningen er det gitt klarere regler om hvilken tilsynsmyndighet som skal anses som skal anses som Lead DPA ut fra hvor virksomheten til den behandlingsansvarlige er lokalisert og organisert.

ledning fra Lead DPA og Artikkel 29-gruppen for å sikre effektiv behandling og godkjenning.

Når endelig utkast til bindende virksomhetsregler foreligger, skal tilsynsmyndigheten sirkulere utkastet til de tilsynsmyndigheter som er relevante for gjennomgangen av virksomhetsreglene. Hvem de relevante tilsynsmyndigheter vil være, avhenger av hvilke land de enhetene som kan tenkes å overføre data til i tredjeland i virksomheten/konsernet, er lokalisert i innenfor EU/EØS. Enkelte land har anerkjent en «Mutual Recognition Procedure» som medfører at disse landene aksepterer vurderingen til Lead DPA som tilstrekkelig, og godkjenner derfor kun mottak av virksomhetsreglene.[128] Land som ikke har anerkjent prosedyren, må vurdere om de bindende virksomhetsreglene er i overensstemmelse med regelverket og Artikkel 29-gruppens krav, som skal skje innen én måned fra mottak av utkastet. Når virksomhetsreglene er endelige, kan virksomheten anmode om godkjennelse av overføring på grunnlag av virksomhetsreglene fra hver enkelt tilsynsmyndighet, siden reglene anses som garanti ved overføring fra alle EU/EØS-land og alle enheter i virksomheten kan benytte seg av godkjenningen.

På grunn av prosedyrene for godkjenning vil det ta noe tid å få godkjent bindende virksomhetsregler, og dette er derfor ikke et alternativ dersom overføring skal skje innen relativt kort tid. Standardbestemmelsene vil da være et mer aktuelt alternativ også for virksomheter som overfører personopplysninger innad i egen virksomhet.

Etter en undersøkelse gjennomført i 2010 av EU-kommisjonen bruker de enkelte tilsynsmyndigheter i EU fra to dager til tre måneder på å godkjenne overføring av personopplysninger under virksomhetsreglene. Dette er overføring etter at det foreligger virksomhetsregler godkjent av Lead DPA, hvor man må ha godkjennelse fra tilsynsmyndigheten i det enkelte land hvor personopplysninger skal overføres fra. Datatilsynet i Norge har oppgitt å bruke mellom to og åtte uker. En rekke av tilsynsmyndighetene krever også at skjemaer og dokumenter oversettes til lokalt språk før godkjennelse gis.

128. Det er en viss usikkerhet knyttet til Mutual Recognition Procedure, bl.a. siden Norge er inntatt som et land som har akseptert prosedyrene (http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/mutual_recognition/index_en.htm), og Datatilsynet i Norge mener allikevel tilsynet må vurdere konsernreglene.

Bindende virksomhetsregler benyttes i praksis i liten grad, men dette kan endres som følge av at bindende virksomhetsregler er inntatt i forordningens artikkel 47. Kravene til bindende virksomhetsregler som er inntatt i forordningen, er kortfattede mot det regelverk som er etablert av Artikkel 29-gruppen, og det er ikke klart hvilke regler som vil gjelde under forordningens nye bestemmelser. Det er imidlertid grunn til å anta at det vil komme veiledning fra Artikkel 29-gruppen om bindende virksomhetsregler etter forordningens regler. Ifølge forordningen skal bindende virksomhetsregler utarbeides av den virksomhet som ønsker å overføre personopplysninger, og skal godkjennes av den tilsynsmyndighet som foretaket er underlagt (som vil være Datatilsynet for virksomheter etablert i Norge). For å sikre sammenheng i håndhevelsen av personvernforordningen skal tilsynsmyndigheten konferere med Databeskyttelsesrådet, jf. artikkel 64, før bindende virksomhetsregler godkjennes. Virksomhetsreglene skal minimum ha det innholdet som følger av artikkel 47 nr. 2, og skal uttrykkelig gi de registrerte rettigheter som kan håndheves. Sistnevnte må innebære at de registrerte kan håndheve sine rettigheter etter virksomhetsreglene selv om de registrerte ikke er part i virksomhetsreglene. Virksomhetsreglene kan omfatte alle selskaper i et konsern eller en gruppe selskaper som «*utøver felles økonomisk aktivitet*». Det må antas at sistnevnte også omfatter selskaper som faller utenfor aksjeloven/allmennaksjelovens konsernbegrep, men som har felles økonomiske interesser eksempelvis gjennom felles eierskap. EU-kommisjonen kan uforme prosedyrer og krav til format for utveksling av opplysninger i forbindelse med utforming og inngåelse av bindende virksomhetsregler, jf. artikkel 47 nr. 3.

5.4.8 Informasjon om overføring i melding

Melding om behandling av personopplysninger, i de tilfeller hvor det foreligger meldeplikt, skal inneholde angivelse av databehandler med adresse og hvem personopplysninger skal utleveres til, herunder eventuelle mottakere i andre land, jf. POL § 32, se punkt 2.3 ovenfor.

Etter PVD artikkel 19 skal melding til tilsynsmyndigheten (som blir Datatilsynet i Norge dersom den behandlingsansvarlige er etablert i Norge) om behandling inneholde informasjon om «*planlagte overføringer av opplysninger til tredjestater*», dvs. fremtidige overføringer, som innebærer stort sett tilsvarende som reglene etter POL siden meldingen etter POL § 32 skal inneholde informasjon om hvem personopplysningene «*vil bli*» overført til.

Ved at den behandlingsansvarlige må melde om bruk av databehandler, vil det også måtte meldes om at opplysningene skal overføres til databehandler dersom denne holder til i tredjeland. Datatilsynet vil dermed i de tilfeller hvor det

foreligger meldeplikt, bli kjent med overføring til tredjeland. Ellers vil Datatilsynet også bli kjent med overføringen dersom det søkes om tillatelse til overføring, se punkt 5.4.5 ovenfor. Er det ikke meldeplikt for behandlingen eller ikke krav om å søke om tillatelse til overføring, vil Datatilsynet derimot ikke ha noen anledning til å bli kjent med overføringen. Dette vil eksempelvis gjelde overføring av opplysninger på grunnlag av samtykke.

5.4.9 Straffbar overføring

Ved overføring til utlandet i strid med POL § 29 vil Datatilsynet kunne pålegge overtredelsesgebyr og tvangsmulkt inntil pålegg fra Datatilsynet er oppfylt, som f.eks. sletting av overførte opplysninger. Straff etter POL § 48 vil kun være aktuelt dersom pålegg fra Datatilsynet ikke overholdes, siden overtredelse av POL § 29 ikke er straffbart i seg selv. Dersom opplysningene ikke kan slettes, kan erstatning etter POL § 49 være aktuelt, se punkt 4.5.1 ovenfor.

Unnlatelse av å følge reglene i POF kapittel 6 om overføring av opplysninger til utlandet er straffbart etter POF § 10-3. Å overtre reglene om forbud for å overføre opplysninger til utlandet etter POL kapittel V er derimot ikke straffbart etter POL § 48. Siden reglene i POF er kun bestemmelser som utfyller reglene etter POL (se nedenfor), synes det å være en feil i POF ved at det er strafferegulert for overtredelse av POF kapittel 6. Når lovgiver har valgt å unnlate overføring av personopplysninger til utlandet i straffebestemmelsen, vil det være vanskelig å se at det kan foreligge en overtredelse av POF kapittel 6 som kan idømmes straff. POF § 10-3 må derfor forstås slik at det ikke kan idømmes straff for overtredelse av POF kapittel 6. Imidlertid kan overtredelsesgebyr eller tvangsmulkt som følge av pålegg ilegges, og en måte man kan idømmes straff på, er ved ikke å imøtekomme Datatilsynets pålegg i forbindelse med overføring av opplysninger til utlandet (som et pålegg om å tilbakeføre eller slette opplysninger), hvoretter straff kan idømmes etter POL § 48 (1) punkt d.

5.4.10 Overføring til databehandler i USA

USA er ikke blant de land som EU-kommisjonen anser for å sikre forsvarlig behandling av personopplysninger, og overføring kan således ikke skje til databehandler lokalisert i USA etter hovedregelen i POL § 29. Som det følger ovenfor, er unntakene i POL § 30 snevre, og for å sikre at det var mulig å overføre

personopplysninger til USA, besluttet derfor EU-kommisjonen med hjemmel i PVD artikkel 25 nr. 6 i 2000 at virksomheter i USA som aksepterer å følge en rekke prinsipper utformet av US Department of Commerce – de såkalte «Safe Harbor-reglene» – skal anses å ha *«et tilstrekkelig vernenivå»*.

Safe Harbor-reglene ble benyttet i mange år, men som en følge av bl.a. Snowden-avsløringene av amerikanske myndigheters masseovervåkning også av EU-borgere avsa EU-domstolen en avgjørelse i oktober 2015[129] om at EU-kommisjonens Safe Harbor-beslutning var ugyldig, og Safe Harbor var dermed ikke et lovlig grunnlag for overføring av personopplysninger til USA.

EU-domstolens avgjørelse fikk stor betydning for enkelte virksomheter som hadde basert seg på Safe Harbor-reglene som eneste overføringsgrunnlag. I februar 2016 inngikk EU-kommisjonen og USA en ny avtale med regler for overføring av personopplysninger til USA: EU-US Privacy Shield, som trådte i kraft 12. juli 2016. Den nye avtalen pålegger strengere plikter for amerikanske virksomheter som mottar personopplysninger fra Europa, og det er begrensede muligheter og strengere krav for amerikanske myndigheter til å få generell tilgang til personopplysningene. Dersom amerikanske myndigheter skal gis tilgang til personopplysningene, skal dette skje etter klare regler og på en transparent måte, adgangen skal være underlagt årlige gjennomganger, og en «ombudsperson» skal være klageinstans for påstått ulovlig tilgang fra myndighetene side.

129. EU-domstolens sak nr. C-362/14 (Schrems).