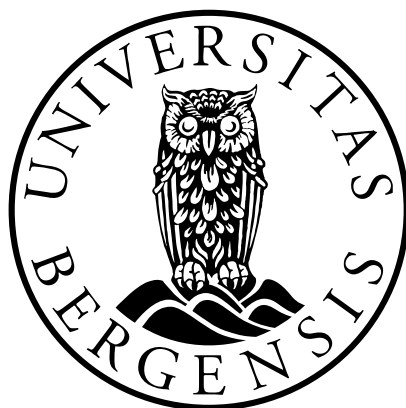


Bakgrunnssjekk i ansettelsesprosessen:
*Arbeidsgivers behov for et forsvarlig
ansettelsesgrunnlag og
kandidatens rett til integritetsvern*

Kandidatnummer: 55

Antall ord: 13 478

*(PS! Bruk ordtellingsfunksjon. Fotnoter og sluttnoter skal medregnes i ordgrensen.
Forord, forside, innholdsfortegnelse, registre, litteraturliste og vedlegg medregnes ikke.)*



JUS399 Masteroppgave
Det juridiske fakultet

UNIVERSITETET I BERGEN

1.juni 2017

Innhold

1.	Innledning	4
1.1	Oppgavens tema og problemstillinger	4
1.2	Bakgrunn og aktualitet	4
1.3	Metode	5
1.4	Begreper	6
1.4.1	Arbeidsgiver	6
1.4.2	Kandidat	7
1.4.3	Personopplysning	7
1.4.4	Sensitive personopplysninger	7
1.4.5	Behandlingsansvarlig	9
1.4.6	Databehandler	9
1.5	Avgrensninger	10
1.5.1	Virksomhet i privat sektor	10
1.5.2	Tidspunkt for innhenting og bruk av informasjon	10
1.5.3	Innsyn i politiattest	10
1.5.4	Diskriminering	11
1.6	Den videre fremstillingen	11
2.	Bakgrunnssjekk i ansettelsesprosessen	12
2.1	Innledning	12
2.2	Bakgrunnssjekk	12
2.2.1	Fenomenet bakgrunnssjekk	12
2.2.2	Utvidet bakgrunnssjekk	13
2.2.3	Rollefordeling i en bakgrunnssjekk	15
2.3	Hvilke behov legitimerer arbeidsgivers innsyn i politiattest?	16
2.3.1	Effektivitet og økonomi	16
2.3.2	Beskyttelse av omdømme	16
2.3.3	Sikkerhet for virksomhet og ansatte	17
2.4	Hensynene til næringslivet – et globalt perspektiv	17

2.4.1	Etablering av virksomhet i Norge og forholdet til avtaleparter	17
2.4.2	Kriminalitetsforebyggende tiltak- retningslinjer fra OECD	18
2.4.3	Regnskapsloven § 3-3 c)	19
3.	Rettslige utgangspunkt for behandling av personopplysninger	21
3.1	Innledning	21
3.2	Lovens formål jf. poppl. § 1	21
3.3	Grunnleggende vilkår for behandling av personopplysninger	22
3.3.1	”Saklig begrunnet i behandlingsansvarliges virksomhet” – formålet med behandlingen jf. poppl. § 11, b)	22
3.3.2	Behandling av personopplysninger jf. poppl. § 8.....	22
3.3.3	Behandling av sensitive personopplysninger jf. poppl. § 9	23
3.4	Konsesjonsmyndighet og vaktbikkje - Datatilsynet.....	24
3.4.1	Datatilsynets todelte funksjon – ombud og tilsynsorgan.....	24
3.4.2	Datatilsynets og behandling av sensitive personopplysninger	24
3.4.3	Unntak fra konsesjonsplikt – personopplysningsforskriften	25
4.	Hjemmelsgrunnlag ved behandling av sensitive personopplysninger	28
4.1	Innledning	28
4.2	”Hjemmel i lov” jf. poppl. § 8, første ledd og §9, første ledd, b)	28
4.2.1	Særregulering av opplysninger angitt i poppl. § 2 nr.8, b) jf. poppl. §10.....	28
4.3	Opplysninger om at en person har vært mistenkt, siktet, tiltalt eller dømt for en straffbar handling jf. poppl. § 2, nr.8, b)	29
4.3.1	Særlovgivning for utstedelse av politi/vandelsattest – Politiregisterloven 28.mai, 2010 nr. 16	29
4.3.2	Politiattest og hvilke formål som berettiger bruk av denne	29
4.3.3	Politiregisterforskriften 2013	32
4.4	”Samtykke” jf. poppl. § 2 nr.7 jf. poppl. § 9, første ledd, a) som hjemmelsgrunnlag	32
4.4.1	Hva er et samtykke etter poppl.?	32
4.4.2	Samtykke til fremleggelse av politiattest i ansettelsesprosessen	34

4.5	”Nødvendig for å gjennomføre arbeidsrettslige plikter eller rettigheter” jf. poppl. § 9, første ledd, f)	36
4.6	Oppsummering	38
5.	EUs personvernforordning – ikrafttredelse 2018	39
5.1	Bakgrunn og formål	39
5.2	Virkninger for næringslivet	39
5.2.1	Artikkel 88	39
5.2.2	Fremtiden til personopplysningsforskriften – melde og konsesjonsplikt	40
5.2.3	Skjerpet samtykkekrav	41
5.2.4	”One- stop shop”	41
6.	Avslutning	42
7.	Kilde og litteraturliste	43

1. Innledning

1.1 Oppgavens tema og problemstilling

Tema for oppgaven er bakgrunnssjekk i ansettelsesprosessen , nærmere bestemt arbeidsgivers behov for et forsvarlig ansettelsesgrunnlag og kandidatens rett til vern av integritet.

Oppgavens overordnede problemstilling er arbeidsgivers behandling av kandidatens personopplysninger i ansettelsesprosessen. Problemstillingen reiser spørsmål om avveiningen av hensynene for at arbeidsgiver får en utvidet adgang til informasjon mot at kandidaten har en lovfestet rett til vern av personlige opplysninger og integritet. Oppgavens hovedfokus er på arbeidsgivers adgang til å behandle opplysninger om kandidaten tidligere har vært mistenkt, siktet, tiltalt eller dømt i en tidligere straffesak¹. Disse opplysningene fremgår av en politiattest, og innsyn i denne vil være gjenstand for behandling i oppgaven. Det overordnede hensynet her er at arbeidsgiver i kraft av innsyn kan forebygge og minimere risikoen for at virksomheten blir rammet av økonomisk kriminalitet.

Arbeidsmiljøloven inneholder ingen spesifikke bestemmelser vedrørende bakgrunnssjekk av kandidater i ansettelsesprosessen. De alminnelige reglene for behandling av personopplysninger i personopplysningsloven kommer imidlertid til anvendelse for arbeidsgiver og kandidat. Avhandlingen er ment som et bidrag til redegjøring og avklaring av en rettstilstand som i dag oppleves som fragmentarisk.

EUs nye personvernforordning trer i kraft i 2018. Derfor vil oppgaven også fokusere på hvilke endringer forordningen kan innebære på det aktuelle rettsområdet.

1.2 Bakgrunn og aktualitet

Arbeidsrett i kombinasjon med personvernrett er svært aktuelt. Den teknologiske delen av samfunnet holder et høyt tempo, og dette inkluderer informasjonsteknologi. Dette er både positivt og negativt. På den ene siden er en økt tilgang på informasjon en nyttig ressurs. Det bidrar til et sikrere, mer åpent og tilgjengelig samfunn. På den andre siden er utfordringer vedrørende kvalitet og troverdighet til stede når man har en fri flyt av informasjon i samfunnet. En naturlig konsekvens av at utviklingen går fort er at lovgivningen i noen tilfeller sliter med å holde følge.

¹ Lov om behandling av personopplysninger 14.april 2000 nr. 31, heretter poppl. § 2 nr.8, b)

² Ep/Rdir. 95/46/EF

Behovet for et forsvarlig ansettelsesgrunnlag er alltid aktuelt for arbeidsgiver. Det er fordi en feilansettelse er ressurskrevende på mange områder. De potensielle konsekvensene i sammenheng med arbeidsgivers omdømme, økonomi, hensynet til andre arbeidstakere og samfunnet generelt kan bli store dersom feil kandidat blir ansatt i en stilling. En bakgrunnssjekk av kandidaten er derfor et viktig verktøy for arbeidsgiver når beslutningen skal tas. Spørsmålet er imidlertid i hvor stor utstrekning virksomheten kan kontrollere den potensielle arbeidstageren og om lovgivningen gir arbeidsgiver adgang til å utføre en utvidet bakgrunnssjekk hvor det behandles opplysninger om kandidaten tidligere har vært involvert i strafferettsystemet.

1.3 Metode

Avhandlingen gjør rede for gjeldende norsk rett, og tar utgangspunkt i regler for behandling av personopplysninger som nedfelt i personopplysningsloven og politiregisterloven med tilhørende forskrifter. Annen særlovgivning på området blir det ikke tatt stilling til, og det tas høyde for at det kan foreligge bestemmelser som kan gi en spesifisert type privat virksomhet andre rettigheter enn det personopplysningsloven og politiregisterloven gjør. Metodisk tar oppgaven sikte på analysere og anvende bestemmelsene som er aktuelle for temaet og anvende de på problemstillingen. Dette vil bli gjort ved å tolke de aktuelle bestemmelsene i lys av ordlyd, forarbeider og andre rettskilder som har relevans. Oppgaven har en teoretisk tilnærming til redegjørelsen for fenomenet bakgrunnssjekk samt den nye personvernforordningen.

Personopplysningsloven er den primære rettskilden da den regulerer vilkår for behandling av personopplysninger. Den angir også kravene til rettslige grunnlaget for behandling av sensitive personopplysninger. Loven, forskriften og dens forarbeider er de viktigste rettskildene når det skal redegjøres for rettstilstanden ved privat sektors behandling av personopplysninger.

Personopplysningsloven er i stor grad bundet av EUs personverndirektiv 1995². Den 25.6.99 ble direktivet tatt inn i EØS avtalen, hvilket gjorde det folkerettslig bindende for Norge³. Før direktivet trådte i kraft, var det et hinder mot flyt i det indre markedet at medlemslandene hadde forskjellig lovgivning på dette området. Noen land ble ansett for å ha et for sterkt vern av personlige opplysninger, mens andre land ikke hadde tilstrekkelig vern. Direktivet angir et

² Ep/Rdir. 95/46/EF

³ Dag W. Schartum og Lee A. Bygrave, *Personvern i informasjonsamfunnet*, 3.utgave, Bergen 2016 s. 95

minimum av personopplysningsvern som medlemslandene ikke kan fravike⁴. Norges forpliktelse til å gjennomføre direktivet innebærer også at særlovgivning må bygges opp i tråd med de samme begreper og prinsipper som direktivet og personopplysningsloven⁵. Formålet bak nåværende regulering er at det tar sikte på å harmonisere nasjonale lover om personopplysningsvern for å avskaffe hindre mot at personopplysninger skal kunne flyte fritt mellom landene i EU og EØS⁶.

Personopplysningsloven bærer preg av vage bestemmelser, med rom for forholdsmessighetsvurderinger og skjønn. Dette er fordi rettsområdet for personvern er i stadig utvikling, hvilket har sammenheng med en raskt fremskridende utvikling innenfor teknologi og informasjonsteknologi. Muligheten må derfor være til stede for en dynamisk fortolkning av reglene, sett i sammenheng med systemhensynene på rettsområdet.

Politiregisterloven med tilhørende forarbeider og forskrift vil også bli behandlet da det foreligger særregler for innsyn i politi/vandelsattest. Dette drøftes særskilt når det skal gjøres rede for lovhjemmel som hjemmelsgrunnlag.

Temaet bakgrunnssjekk i ansettelsesprosessen er lite berørt i litteraturen. I den grad det nevnes begrenser det seg ofte til arbeidsmiljølovens bestemmelser om hvilke opplysninger arbeidsgiver ikke kan be om i utlysning av stilling og i ansettelsesprosessen. Årsaken til dette er nok at fenomenet bakgrunnssjekk slik det behandles i oppgaven er en relativt fersk problemstilling innenfor områdene arbeidsrett og personvernrett. Ansettelsesprosessen og forholdet mellom arbeidsgiver og kandidat er imidlertid omtalt i større grad, hvilket har betydelig relevans til problemstillingen. Utgangspunktet blir derfor litteratur, statistikk og fagartikler som belyser problemstillingens aktualitet der dette er nødvendig.

1.4 Begreper

1.4.1 Arbeidsgiver

Aml. § 1-8 (2)⁷ definerer en arbeidsgiver slik: ”Med arbeidsgiver menes i denne lov enhver som har ansatt arbeidstaker for å utføre arbeid i sin tjeneste. Det som i denne lov er bestemt om arbeidsgiver, skal gjelde tilsvarende for den som i arbeidsgivers sted leder virksomheten”. Denne definisjonen av en arbeidsgiver er lagt til grunn i oppgaven.

⁴ Dag W. Schartum og Lee A. Bygrave, *Personvern i informasjonssamfunnet*, 3. utgave, Bergen 2016 s.96/97

⁵ Dag W. Schartum og Lee A. Bygrave, *Personvern i informasjonssamfunnet*, 3. utgave, Bergen 2016 s. 125

⁶ Dag W. Schartum og Lee A. Bygrave, *Personvern i informasjonssamfunnet*, 3. utgave, Bergen 2016 s.94

⁷ Arbeidsmiljøloven 2005, 17.juni nr. 62

1.4.2 Kandidat

Begrepet ”kandidat” er ikke legaldefinert i lovgivningen. I personopplysningslovens forstand vil en person være omtalt som ”registrert”⁸, men oppgaven vil benytte seg av begrepet ”kandidat”.

Ordlyden av kandidat antyder at det er tale om en utvalgt person som kan være aktuell for stillingen. Oppgaven er altså avgrenset mot å omhandle en bred krets av arbeidssøkere til en stilling, og videre om det er adgang til innsyn i politiattest i en slik situasjon. Det er også avgrenset mot begrepet ”arbeidstaker” da vedkommende ikke er ansatt i virksomheten på tidspunktet for behandling av sensitive personopplysninger. Arbeidsmiljøloven kommer følgelig ikke til anvendelse ved løsning av problemstillingen.

1.4.3 Personopplysning

Etter poppl. § 2, nr.1 fremgår det at en personopplysning er opplysninger og vurderinger som kan knyttes til en enkeltperson. Forarbeidene legger til grunn at med en ”enkeltperson” menes en person som direkte eller indirekte kan identifiseres, for eksempel ved hjelp av navn, identifikasjonsnummer eller annet kjennetegn som er spesielt for fysiologiske, psykiske, fysiske, økonomiske, kulturelle eller sosiale identitet, jf. direktivet art. 2 a⁹. Uttrykket «personopplysning» favner videre enn opplysninger om noens «personlige forhold», jf. forvaltningsloven § 13 første ledd nr. 1 om taushetsplikt. Eksempler på personopplysninger som faller utenfor forvaltningslovens begrep er opplysninger om fødested, fødselsdato og personnummer, statsborgerforhold, sivilstand, yrke, bopel og arbeidssted, jf. forvaltningsloven § 13 annet ledd¹⁰.

1.4.4 Sensitive personopplysninger

Personopplysningsloven definerer sensitive personopplysninger som opplysninger av en særskilt sensitiv karakter jf. poppl. § 2, nr.8. Dette er opplysninger om rasemessig eller etnisk bakgrunn, eller politisk filosofisk eller religiøs oppfatning. Videre er opplysninger om at en person har vært mistenkt, siktet, tiltalt eller dømt for en straffbar handling en sensitiv personopplysning. Helseforhold, seksuelle forhold og medlemskap i fagforeninger er også nedfelt som ekstra beskyttelsesverdige opplysninger. Bestemmelsen lovfester sammen med poppl. § 9 regelen i direktivet artikkel 8 nr.1. Definisjonen ”sensitiv personopplysning” har

⁸ Poppl. § 2, nr.6

⁹ Ot.prp.nr. 92, (1998-1999) s. 102

¹⁰ Ot.prp.nr. 92 (1998-1999) s. 103

også betydning med tanke på bestemmelsen om konsesjonsplikt i § 33.¹¹ Det kommer videre frem at angivelsen av de sensitive personopplysningene har fått en noe annen utforming enn de tilsvarende beskrivelsene i direktivet, men innholdet er det samme¹².

Når ”sensitivt” benyttes i personvernsammenheng, er det for å uttrykke allmenne antakelser om sammenhengen mellom en opplysningstype og mulige virkninger av opplysningen for de registrerte personene det siktes til¹³. Det foreligger imidlertid et språk mellom allmennhetens ønske om hvilke opplysninger som bør bli lovfestet som sensitive, og direktivet/lovgivers oppfatning av hva som skulle få et lovfestet vern. En rapport fra Transportøkonomisk institutt fra 2005 tok for seg folks holdninger til hvilke opplysninger som er mest beskyttelsesverdige¹⁴. Rapporten viser at 52% av de som ble spurt mente at opplysninger om personlig økonomi var særlig viktig å beskytte. Det samme gjelder opplysninger om personnummer, med en prosentandel på hele 74%. Ingen av disse opplysningene er i pol. angitt som sensitive personopplysninger jf. § 2, (8). Til forskjell mener de spurte i undersøkelsen at opplysninger om medlemskap i fagforeninger og om religiøs tilhørighet, er de minst viktige opplysningene å beskytte. Disse er imidlertid nedfelt i poppl. § 2, (8) jf. bokstav a) og e)¹⁵.

Forarbeidene legger til grunn at begrepet ”sensitiv” ikke må overvurderes. Med dette mener de at det er andre opplysninger som etter omstendighetene også kan oppfattes som følsomme. Her tar forarbeidene til orde for at opplysninger om privatøkonomi, eller opplysninger som gir et så tydelig bilde av den registrerte at det oppleves som ubehagelig, også kan anses som sensitive. I tilknytning til dette blir Datatilsynets mulighet til å pålegge konsesjonsplikt jf. poppl § 33, 2.ledd fremhevet. Her vil vurderingen alltid være knyttet opp mot det bestemte formålet med bruk av opplysningene jf. poppl § 11¹⁶.

Oppgavens hovedfokus er på opplysningene angitt i poppl. § 2, (8) b) om at en person har vært mistenkt, siktet, tiltalt eller dømt for en straffbar handling. Etter direktivets art 8, nr.5 fremgår det at ” Behandling av opplysninger om lovovertridelser, straffedommer eller sikkerhetstiltak kan utføres bare under kontroll av en offentlig myndighet eller dersom det gis tilstrekkelig og spesifikke garantier i henhold til nasjonal lovgivning, med forbehold for

¹¹ NOU 1997:19, kapittel 21, kapittel 1

¹² NOU 1997:19, kapittel 21, kapittel 1

¹³ Schartum/Bygrave: Personvern i informasjonssammenheng, s. 144

¹⁴ Transportøkonomisk institutt; Setter vår lit til storebror, og alle småbrødre med, rapport nr. 789, s.13.

¹⁵ Transportøkonomisk institutt; Setter vår lit til storebror, og alle småbrødre med, rapport nr. 789, s.13.

¹⁶ Ot.prp.nr. 92 (1998-1999) s. 104

unntak som medlemsstaten kan fastsette på grunnlag av nasjonale bestemmelser som gir tilstrekkelige, spesifikke garantier¹⁷”. Bestemmelsen fastsetter at det må føres kontroll av en offentlig myndighet ved behandling av denne type opplysninger, og i personopplysningsloven har lovgiver valgt å gjøre dette ved å oppstille et vilkår om konsesjon fra Datatilsynet ved behandling av sensitive opplysninger. Det er sannsynlig at dette er grunnen til at disse opplysningene er med i oppramsingen av sensitive personopplysninger i poppl. § 2, nr.8.

1.4.5 Behandlingsansvarlig jf. poppl. § 2, nr.4.

Begrepet ”behandlingsansvarlig” er definert i poppl. § 2, nr.4 hvor det fremgår at behandlingsansvarlig er ”(...) den som bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som skal brukes”. Behandlingsansvar betegner en formell posisjon og innebærer krav til etterlevelse av en rekke plikter i loven. Etter forarbeidene fremgår det at det i utgangspunktet bare er rettssubjekter med prosessuell partsevne som kan være behandlingsansvarlig. Med partsevne menes det i denne sammenheng å kunne bli saksøkt under en prosess for domstolene¹⁸Forarbeidene presiserer at kravet til sivilprosessuell partsevne er begrunnet blant annet i at det kan være nødvendig å bruke rettsapparatet for å gjennomføre krav mot den som er behandlingsansvarlig¹⁹. Der den behandlingsansvarlige er en juridisk person, vil den juridiske personen representert ved dens ledelse være behandlingsansvarlig. Funksjonen bør knyttes til en lederstilling slik at stillingsinnehaveren har reell daglig innflytelse på behandlingene som foretas²⁰.

1.4.6 Databehandler

Etter poppl. § 2 nr.5 er databehandler definert som ”...den som behandler personopplysninger på vegne av den behandlingsansvarlige”. Behandlingsoppdraget skal være avtaleregulert, hvilket begrenser databehandlerens rådighet over opplysningene.²¹ Databehandleren er også pålagt et selvstendig ansvar for at informasjonssikkerheten er tilfredsstillende²². En databehandler er typisk en juridisk person, for eksempel et firma, men kan også være en fysisk person. Databehandler er bare aktuell dersom det oppstår et oppdragsforhold mellom

¹⁷ Ep/Rdir. 95/46/EF art.8 nr.5

¹⁸ NOU 1997:19 s. 133

¹⁹ NOU 1997:19 s.133

²⁰ Ot.prp.nr.92 s. 103

²¹ Poppl. § 15

²² Poppl. § 13

behandlingsansvarlig og databehandler hvor behandlingsansvarlig er oppdragsgiver og databehandler er oppdragstaker²³.

1.5 Avgrensninger

1.5.1 Virksomheter i privat sektor

Bakgrunnssjekk i ansettelsesprosessen kan være aktuelt innenfor både offentlig og privat sektor. Oppgaven er avgrenset til private virksomheters innsyn i politiattest i ansettelsesprosessen, og det er flere grunner til dette. Først og fremst vil det for offentlige stillinger ofte foreligge særregler knyttet til ansettelse. I tillegg til dette vil forvaltningsrettslige normer gjelde for ansettelsesprosessen og kan videre tenkes å ha betydning for bruk av bakgrunnssjekk. Personopplysningsloven begrenser i tillegg ikke offentlige virksomheters rett til innsyn etter offentleglova²⁴. Forvaltningsorganer har i flere tilfeller lovfestet rett i særlovgivning til å behandle opplysninger som angitt i poppl. § 2, nr. 8 b). I disse tilfellene vil man kunne søke støtte i forvaltningspraksis rundt praktiseringen av reglene. Det bidrar til at det er en mer avklart og regulert rettstilstand innenfor offentlig sektor og det foreligger følgelig ikke et tilsvarende behov for kartlegging og redegjørelse som det gjør for privat sektor.

1.5.2 Tidspunkt for innhenting og bruk av informasjon

Oppgaven avgrenser seg til ansettelsesprosessen. Det er i dette tidsrommet bakgrunnssjekk blir utført og trer inn som et hjelpemiddel for virksomheten ved rekruttering.

1.5.3 Innsyn i politiattest

Oppgaven er avgrenset til å omhandle behandling av opplysninger om en kandidat har vært mistenkt, siktet, tiltalt eller dømt for en straffbar handling²⁵. Dette valget er tatt på bakgrunn av at de andre opplysningene som er angitt i bestemmelsen om sensitive personopplysninger er av en annen karakter. Opplysninger om graviditet, helseforhold, politisk oppfatning etc er beskyttet i aml. § 13-4²⁶.

Vi lever i en tid hvor eksponering på sosiale medier blir stadig mer utbredt. Opplysninger om graviditet og politisk engasjement er det en lavere terskel for å dele fordi denne måten å

²³ Dag W. Schartum og Lee A. Bygrave, *Personvern i informasjonssamfunnet*, 3. utgave, Bergen 2016 s.173

²⁴ Poppl. § § 6

²⁵ Poppl. § 2, nr. 8 b).

²⁶ Aml § 13-4 om opplysninger arbeidsgiver som hovedregel ikke kan be kandidaten om i ansettelsesprosessen.

formidle nyheter på er praktisk all den tid det når ut til mange på en gang. Det tilhører imidlertid sjeldenhetene at en person legger ut en statusoppdatering på Facebook om at vedkommende er mistenkt eller siktet i en straffesak. Slike opplysninger har en annen karakter av sensitivitet, og en annen betydning for individets integritet. Dette vil også vise seg i redegjørelse for hjemmelsgrunnlagene og hvilke krav som stilles til dette. Behandling av disse opplysningene i ansettelsesprosessen kan samtidig være svært viktig for en virksomhet som av et tungtveiende behov for et forsvarlig ansettelsesgrunnlag. Det foreligger derfor et behov for kartlegging av disse opplysningenes stilling i en ansettelsesprosess.

1.5.4 Diskriminering

Aml. § 13-4 har regulert hvilke hensyn det er lov å vektlegge i en ansettelsesprosess, og hvilke det ikke er adgang til å vektlegge. Dette er regler som beskytter kandidaten mot diskriminering i ansettelsesprosessen. Oppgaven er avgrenset mot dette, og eventuelle problemstillinger i tilknytning til at virksomheten aktivt bruker informasjonen som ledd i avgjørelsen om hvem som blir ansatt vil ikke bli drøftet.

1.6 Den videre fremstillingen

Det vil først bli gitt en redegjørelse for ansettelsesprosessen som er det aktuelle tidsrommet oppgaven befinner seg i. Etter dette følger det i kapittel 2 en fremstilling av bakgrunnssjekk som fenomen og hensynene som legitimerer arbeidsgivers behov for et forsvarlig ansettelsesgrunnlag. Kapittel 3 omhandler de rettslige utgangspunktene for behandling av personopplysninger, samt Datatilsynets funksjon som tilsyn og ombud. Kapittel 4 gjør rede for og drøfter de relevante hjemmelsgrunnlagene innsyn i politiattest i personopplysningsloven og politiregisterloven med tilhørende forskrifter.

Personvernregelverket er under endring, og i 2018 vil EUs nye personvernforordning tre i kraft. Kapittel 5 tar for seg noen forordningens viktigste virkninger for næringslivet.

Avslutning følger i kapittel 6 og kildeliste fremgår i kapittel 7.

2. Bakgrunnssjekk i ansettelsesprosessen

2.1 Innledning

Utgangspunktet i privat sektor er at arbeidsgiver kontrollerer virksomheten. Vedkommende bestemmer derfor hvilke kvalifikasjoner ansatte skal ha og avgjør i en ansettelsesprosess hvem som passer best til stillingen. Krav til kvalifikasjoner kan dreie seg om formell bakgrunn/utdanning og personlig egnethet og arbeidsgiveren vurderer søkeren på grunnlag av intervju, vitnemål og referanser mv.

I offentlig sektor foreligger det regler²⁷, forvaltningspraksis og normer for ansettelse. Arbeidsgivere i privat sektor opplever større frihet i ansettelsesprosessen og er for eksempel ikke bundet av kvalifikasjonsprinsippet²⁸. Den eneste lovregulerte skranken i ansettelsesprosessen private virksomheter må forholde seg til er at det ikke må foreligge diskriminering av kandidater jf. aml. § 13-4²⁹. Arbeidsgiver er allikevel bundet av de skranker som følger av personvernregelverket.

2.2 Bakgrunnssjekk

2.2.1 Fenomenet bakgrunnssjekk

Bakgrunnssjekk er et viktig verktøy for virksomheten i ansettelsesprosessen. Ved å utføre en bakgrunnssjekk av kandidatene som søker på den aktuelle stillingen, vil man kunne kvalitetssikre og verifisere opplysningene vedkommende har gitt i søknad og CV. Det er flere aktører på markedet som tilbyr å foreta denne bakgrunnssjekken for virksomhetene slik at de bare får tilgang til opplysninger de har lov å vektlegge. Det siktes her til opplysninger som gjerne deles i sosiale medier, men som er av sensitiv karakter i henhold til personopplysningsloven. Eksempler på dette er opplysninger om graviditet, helseforhold og politisk tilhørighet. NOU 2009:1³⁰uttaler:

” De fleste av oss protesterer ikke på at legen skal ha opplysninger om helsen vår, at banken skal ha kredittopplysninger når vi søker lån, eller at læreren skal ha relevant informasjon om barna våre.

²⁷ Tjml. § 5

²⁸ Prop. 94 L (2016-2017), pkt. 9.1 s.70: ”Et ulovfestet prinsipp som innebærer at det er den best kvalifiserte søkeren som skal ansettes i en ledig stilling. Prinsippet har lovs rang og gjelder hele offentlig sektor.”

²⁹ Aml. § 13-4 om Innhenting av opplysninger ved ansettelse

³⁰ NOU 2009:1 Individ og integritet, Personvern i det digitale samfunn

Problemet oppstår dersom vi blir avkrevd informasjon som vi ikke oppfatter som *relevant*³¹ for den aktuelle situasjonen eller relasjonen”.³²

Utsagnet fokuserer på *relevansen* av bruken av personopplysninger, og om behandling av opplysningene er en forutsetning for at en ansettelse skal kunne foretas på et forsvarlig grunnlag. En bakgrunnssjekk kan nemlig ha to sider. På den ene siden består den i å verifisere opplysningene som kandidaten har avgitt i søknadsprosessen. Dette er for å forsikre seg om at kandidaten ikke har avgitt falske opplysninger. Forfalskning av kompetansebevis kan innebære konsekvenser for både virksomhet og potensiell arbeidstager. På den andre siden ønsker man å danne seg et helhetlig bilde av kandidaten. Gjennom en søknad og CV, samt kompetansebevis, forteller kandidaten arbeidsgiver det han eller hun selv ønsker å formidle.

2.2.2 Utvidet bakgrunnssjekk

Dette er imidlertid ikke alltid nok for å danne seg et fullstendig bilde av kandidaten. Momenter av relevans som ikke blir nevnt kan være kandidatens økonomiske historie, og hvor mange tidligere arbeidsforhold kandidaten har innrapportert til skattemyndighetene. For enkelte virksomheter kan det også være viktig å kartlegge om kandidaten har et kriminelt rulleblad. Her kan det være av særskilt stor relevans om kandidaten tidligere har vært involvert i økonomisk kriminalitet, som for eksempel bestikkelser og innsidehandel. Dersom stillingen innebærer at vedkommende ofte blir eksponert for situasjoner hvor etikk og moral i tilknytning til dette blir satt på prøve, er arbeidsgiver svært avhengig av å foreta ansettelser på et så forsvarlig grunnlag som mulig.

Et relevant eksempel for problemstillingen fremgår av dom avsagt i Oslo Tingrett i 2012³³. Saken omhandlet en KRIPOS-ansatt som hjalp en tidligere kollega og venn med å sjekke vandelen til i alt 19 personer i forbindelse med jobbsøknader. Siktete i saken fikk eposter fra B, som var daglig leder i Statoil, som spurte om vedkommende kunne sjekke vandel til ulike personer B anmodet om i forbindelse med ansettelsessaker. Tilbakemeldingen siktete ga var om de aktuelle personene var «rene», dvs. om de var oppført i det sentrale straffe- og politiopplysningsregisteret (SSB) eller ikke. Siktete opplyste at B var en tidligere kollega i KRIPOS, og de hadde jobbet sammen fra om lag 1998 til om lag 2006. Personene det ble bedt om opplysninger om søkte jobb hos Statoil. Siktete søkte i SSB og noen ganger også i Strasak. Alle søkene knyttet seg til forespørsler fra B om navngitte personer i forbindelse med

³¹ Min uthevning

³² Dag W. Schartum og Lee A. Bygrave, *Personvern i informasjonssamfunnet*, 3. utgave, Bergen 2016 s.33

³³ TOSLO- 2012- 47498

ansettelser³⁴. Saken omhandlet brudd på taushetsplikten hos siktede på bakgrunn av at vedkommende hadde utlevert disse opplysningene til sin tidligere kollega. Faktum i saken sier ingenting om B og eventuelle følger for virksomheten av saken, men det er på det rene at B har tilegnet seg disse opplysningene på grovt uetisk vis.

Det vises til saken av to grunner. For det første illustrerer den en virksomhets behov for denne kunnskapen om kandidatene i en ansettelsesprosess. For det andre er den et godt eksempel på hvordan en utvidet bakgrunnssjekk ikke skal foregå, og hvor integritetskrenkende den potensielt kan være dersom den foretas på ulovlig vis. Tilegnelse av sensitive personopplysninger på denne måten er atskillig mer integritetskrenkende enn om kandidaten på forhånd er klar over hvorfor virksomheten ønsker innsyn i disse opplysningene, og hvordan de tilegner seg informasjonen. Tilfellet ble fanget opp i politiet sitt system og straffeforfulgt, men det må kunne legges til grunn at det på dette området høyst sannsynlig foreligger mørketall på lignende tilfeller som ikke blir fanget opp.

Oppgaven omhandler arbeidsgivers innsyn i politiattest i ansettelsesprosessen. I den forbindelse vises det til Næringslivets sikkerhetsråd som har som formål å forebygge kriminalitet i og mot næringslivet. Hvert oddetallsår utfører de en undersøkelse om Kriminalitets- og sikkerhetstilstanden i Norge, med vekt på privat og offentlig næringsliv (KRISINO)³⁵. Undersøkelsen fra 2015 omhandlet blant annet kontrolltiltak i ansettelsesperioden og var konsentrert om identitetssjekk, referansesjekk, ekthetskontroll av vitnemål og søk etter opplysninger om jobbsøker på internett. Undersøkelsen viser en økning av private virksomheters bruk av kontrolltiltakene innenfor samtlige kategorier siden forrige undersøkelse i 2013³⁶. I undersøkelsen ble også deltagerne spurt om hvor godt de kjente til korrupsjon i form av bestikkelser i egen bransje. Det var her avgrenset mot korrupsjonssaker deltagerne eventuelt hadde lest om i media. Resultatet viste at det var i private virksomheter at kjennskapen var størst³⁷.

Økokrims trendrapport for 2015/2016 har som oppgave å kartlegge og orientere om trusselnivået rundt økonomisk kriminalitet. På tross av et stort fokus på bekjempelsen av økonomisk kriminalitet, forventer ØKOKRIM at den generelle trusselen for økonomisk og

³⁴ TOSLO- 2012- 47498

³⁵ <http://www.nsr-org.no/krisino/>

³⁶ KRISINO rapport 2015 s.13

³⁷ KRISINO rapport 2015 s.16

miljøkriminalitet vil øke³⁸. Rapporten viser til tre typer næring som er særskilt utsatt for økonomisk kriminalitet, og her er finansnæringen fremhevet. Det er lite kunnskap om omfanget av økonomisk kriminalitet i den norske delen av denne næringen, men det er på det rene at dette er et marked som er egnet for å bli utnyttet av kriminelle aktører.³⁹ I en omfattende studie av holdninger og omfang av kriminalitet i finansnæringen i New York og London i 2015, svarte hele 47 prosent av respondentene at de tror at deres konkurrenter har deltatt i uetiske eller ulovlige aktiviteter for å få konkurransefortrinn. Undersøkelsen er ikke direkte overførbar til norsk finansbransje da det ikke finnes en tilsvarende undersøkelse foretatt her til lands. Denne bransjen er imidlertid utpreget internasjonal og undersøkelsen indikerer at den er preget av høy lovbrudds risiko⁴⁰.

2.2.3 Rolledeling i en bakgrunnsjekk

Partsforholdet ved behandling av personopplysninger er i de fleste tilfeller tredelt. Dette forholdet består av kandidaten, behandlingsansvarlig og databehandler.

Kandidaten eier retten til sine personopplysninger, og iboende i dette er en selvbestemmelsesrett til hvem som skal få tilgang til denne informasjonen. Vedkommendes sensitive personopplysninger er beskyttet av loven slik at de ikke er tilgjengelige for behandling uten at det foreligger et rettslig grunnlag. Kandidaten setter derfor sin tillit til at de sensitive personopplysningene blir forvaltet med behørig omtanke og under sikre rammer.

Behandlingsansvarlig⁴¹ er parten som har ansvaret for behandling av personopplysningene. Ordlyden av begrepet behandlingsansvarlig antyder at det er tale om den som har det overordnede ansvaret for behandlingen av personopplysningene, og at det er vedkommende som skal holdes ansvarlig dersom noe går galt. Personopplysningsloven pålegger den behandlingsansvarlige en rekke plikter i forbindelse med behandling av personopplysninger⁴². Her fremgår det at den behandlingsansvarlige har et betydelig ansvar i forbindelse med blant annet etterlevelsen av at behandlingen av opplysningene skjer i tråd med det formålet som er oppgitt⁴³. Det stilles også krav til behandlingsansvarlig ettersom at kravene til

³⁸ Trendrapport 2015/2016 ØKOKRIM s. 6

³⁹ Trendrapport 2015/2016 ØKOKRIM s. 6

⁴⁰ Trendrapport 2015/2016 ØKOKRIM s. 6

⁴¹ Poppl. § 2, nr. 4

⁴² Ot.prp.nr. 92 (1998-1999) s. 104

⁴³ Poppl. § 11, b)

informasjonssikkerhet overholdes⁴⁴, og behandlingsansvarlig plikter å etterkomme lovens bestemmelser om rett til innsyn⁴⁵

Databehandleren er parten som behandler opplysningene for behandlingsansvarlig. I den tidligere personregisterloven var denne parten definert som databehandlingsforetak, og begrepet ”databehandler” gir derfor bestemmelsen et videre anvendelsesområde.

Databehandleren skal sikre at personopplysningene ikke blir behandlet på noen annen måte enn det som fremgår av avtalen med behandlingsansvarlig⁴⁶, og et av de viktigste ansvarene en databehandler har er å ivareta kravene til informasjonssikkerhet jf. poppl. § 13⁴⁷.

2.3 Hvilke behov legitimerer innsyn i politiattest?

2.3.1 Effektivitet og økonomi

En feilansettelse stjeler tid og ressurser som kunne vært rettet inn mot andre områder. En undersøkelse foretatt av bemanningsbyrået Proffice fra november 2006 viser at feilansettelser koster norske bedrifter 2,4 millioner kroner. I tillegg kommer de ikke- kvantifiserbare kostnadene en feilansettelse fører med seg. Ni av ti norske bedrifter innrømmet at de hadde feilansatt medarbeidere⁴⁸. En feilansettelse innebærer at hele ressursapparatet innenfor ansettelse må iverksettes på nytt, og dette tar tid og koster penger. Hvis virksomheten har et bedre grunnlag for ansettelse enn det en CV, søknad og referanser kan gi, vil dette bidra til å minimere risikoen for feilansettelser. Behovet for ivaretagelse av effektivitet og økonomi i virksomheten vil ikke alene legitimere et behov for innsyn i politiattest, men det vil være en del av en helhetlig vurdering av hvorfor det er nødvendig.

2.3.2 Beskyttelse av omdømme

Noen virksomheter forvalter store økonomiske forpliktelser og ressurser på vegne av andre og de vil måtte foreta ansettelser til stillinger som krever en høy grad av tillit. Dette er ikke bare for å forsikre seg om at avtaleparter er godt ivaretatt; det er også for å kunne opprettholde et forretningsmessig rykte som sikrer at virksomheten holder seg flytende økonomisk. Dersom en virksomhet med dette ansvaret ikke innfrir kundens forventninger og tilliten blir brutt er det et stort potensiale for svikt i omdømmet. Dette vil videre kunne påvirke eksisterende

⁴⁴ Poppl. § 13, første, andre og tredje ledd

⁴⁵ Poppl. § 16 jf. kap. III Informasjon om behandling av personopplysninger

⁴⁶ Poppl. § 15

⁴⁷ Ot.prp.nr. 92 (1998-1999) s. 104

⁴⁸ Dagens Næringsliv <http://www.dn.no/karriere/2009/12/22/sa-mye-koster-en-feilansettelse>

kundeforhold og også rekruttering av nye avtaleparter. Økt bevissthet om kandidatens tidligere arbeidsforhold og om kandidaten tidligere har vært innblandet i bestikkelser eller innsidehandel vil her kunne være avgjørende i en ansettelsesprosess for å hindre at feil person blir ansatt i stillingen. Her vil stillingens art spille inn i vurderingen sammen med hvilken del av næringslivet virksomheten driver innenfor. Dersom virksomheten i tillegg har internasjonale avtaleparter hvor synet på etikk og moral i arbeidslivet kan være variere, stiller dette ytterligere krav til tillit hos kandidater som ønsker å tiltre stillingen.

2.3.3 Sikkerhet for virksomhet og ansatte

Hensynet til sikkerhet for virksomhet og ansatte knyttes særskilt opp mot de tilfellene hvor en feilansettelse kan bidra til at hemmelig informasjon kommer på avveie. Det er her tale om virksomheter som for eksempel håndterer økonomiske opplysninger av hemmeligstemplett art, bedriftshemmeligheter og informasjon om forestående transaksjoner og oppkjøp. Dersom kandidaten blir ansatt i stillingen og misbruker sin betrodde posisjon til å lekke denne type opplysninger for egen eller andres vinning, påvirker dette sikkerheten til andre ansatte i virksomheten, avtaleparter og virksomheten selv. Her vil behovet for innsyn i politiattest i ansettelsesprosessen kunne legitimeres for å kunne utelukke kandidater som tidligere har vært involvert i innsidehandel og lignende hvitsnippskriminalitet.

2.4 Hensynene til sikkerhet i næringslivet – et globalt perspektiv

2.4.1 Etablering av virksomhet i Norge og forholdet til avtaleparter

Dette hensynet gjør seg gjeldende ovenfor selskaper som har internasjonale avtaleparter og forbindelser. I EU-land vil avtaleparten være bundet av det samme direktivet som Norge. I ”Google- dommen”⁴⁹ slo EU- domstolen fast at søkemotoren Google gjennom etableringen av sitt datterselskap Google Spain SL i Spania var omfattet av EUs personverndirektiv og videre at Google Inc. var behandlingsansvarlig for personopplysningene den behandlet i kontekst av den spanske delen av Googles virksomhet⁵⁰. Datatilsynets vurdering som er sitert i PVN-2015-06 Google⁵¹ legger til grunn at det samme må gjelde for Googles etablering i Norge. Den behandlingen av personopplysninger som har naturlig tilknytning til den virksomheten

⁴⁹ Sak C-131/12 av 13. mai 2014

⁵⁰ PVN- 2015-06 Google saken

⁵¹ Klagesaken omhandlet en privatperson klage til Google på at et portrettbilde av privatpersonen brukt i forbindelse med mediedekningen av en drapssak som personen var involvert i ikke ble slettet. Vedkommende påberopte seg retten til å bli glemt. Datatilsynets vedtak ble opphevet grunnet anførsel av feil rettslig grunnlag, men tolkningen av EU-dommen har overføringsverdi til den aktuelle problemstillingen.

Google Inc. har etablert i Norge, herunder indeksering av personopplysninger om norske borgere, må derfor følge personopplysningsloven⁵². Dette innebærer at et selskap som etablerer seg i Norge må følge norsk personvernlovgivning og med dagens regelverk som hovedregel må søke om konsesjon for å behandle sensitive personopplysninger i ansettelsesprosessen. Problemet oppstår dersom virksomhetens avtaleparter gjennomfører utvidet bakgrunnsjekk på sine kandidater og virksomheten selv ikke kan vise til det samme. Dette kan bli sett på som en svikt i sikkerhetsrutinene for internasjonale avtaleparter hvor disse reglene ikke kommer til anvendelse. I dette tilfellet vil begrunnelsen være at man må ta høyde for og beskytte seg selv for enhver risiko knyttet til feilansettelse.

2.4.2 Kriminalitetsforebyggende tiltak og retningslinjer fra OECD

I en jubileumshilsen til Økokrim i anledning deres 25- års jubileum tar advokatforeningens leder Erik Keiserud til orde for hvordan økonomisk kriminalitet påvirker samfunnet. Han legger vekt på at denne typen kriminalitet truer hele samfunnsmodellen. Den truer konkurransevnen til lovlydige bedrifter, den underminerer det offentliges inntektsgrunnlag, den svekker tryggheten for investeringer og arbeidsplasser, skader tilliten til organisasjoner og myndigheter og dersom denne type kriminalitet får utvikle seg vil den kunne true velferdsstaten⁵³.

OECD⁵⁴ står på norsk for Organisasjonen for økonomisk samarbeid og utvikling. De har som oppgave å fremme økonomisk vekst i medlemslandene og å samarbeide om å stabilisere økonomien og å bidra til å utvide verdenshandelen⁵⁵. Norge er medlem av OECD, hvilket innebærer at næringslivet retter seg etter OECDs retningslinjer. Utgangspunktet er at retningslinjene er veiledende og ikke rettslig bindende⁵⁶. I 1980 vedtok de retningslinjer for beskyttelse og utveksling av personopplysninger over landegrenser⁵⁷. Disse skal veilede medlemsland i deres utarbeidelse av nasjonal politikk om personopplysningsvern⁵⁸. Retningslinjene inneholder blant annet to formål som kan ha en noe motstridende karakter.

⁵² PVN- 2015-06 Google

⁵³ ØKOKRIMs årsrapport 2013, Erik Keiserud, Jubileumshilsen, s.13

⁵⁴ Organisation for Economic Co-Operation and Development <http://www.oecd.org/about/>

⁵⁵ Store norske leksikon <https://snl.no/OECD>

⁵⁶ Når retningslinjer fra OECD skal plasseres i en rettskildekategori, blir det omtalt som soft law. OECD definerer soft law som ” *Co- operation based on instruments that are not legally binding, or whose binding force is somewhat ”weaker” than of traditional law, such as codes of conduct, guidelines, roadmaps, peer reviews*”⁵⁶. Videre viser de til at deres egne retningslinjer er et eksempel på softlaw.

⁵⁷ Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data

⁵⁸ Dag W. Schartum og Lee A. Bygrave, *Personvern i informasjonssamfunnet*, 3.utgave, Bergen 2016 s. 93.

Det ene formålet er å forbedre personopplysningsvernet, og det andre er å fremme internasjonal handel og økonomisk vekst ved å lette flyt av personopplysninger mellom land⁵⁹. Innbakt i formålet om å fremme internasjonal handel og økonomisk vekst er et mandat om å bekjempe korrupsjon og økonomisk kriminalitet innenfor næringslivet. Det oppfordres til at ”Private sector and civil society initiatives also help enterprises to design and implement effective anti bribery policies”⁶⁰. I tråd med OECDs grunnleggende dagsorden er oppnåelsen av sistnevnte formål den viktigste drivkraften bak retningslinjene⁶¹. For virksomheter i privat sektor vil disse retningslinjene kunne spille en viktig rolle i angivelse av formålet for behandling av personopplysninger.

2.4.3 Regnskapsloven § 3- 3 c)

Regnskapsloven av 1998, 17.juli nr. 56 kommer til anvendelse på de fleste regnskapspliktige foretak, både innenfor offentlig og privat sektor⁶². Rskl. § 3-3 c) inneholder en lovfestet plikt for foretaket til å gi en redegjørelse om samfunnsansvar i årsberetningen⁶³. Etter første ledd kommer det frem at ”... Store foretak skal redegjøre for hva foretaket gjør for (...) bekjempelse av korrupsjon i sine forretningsstrategier, i sin daglige drift og i forholdet til sine interessenter⁶⁴”. Etter rskl. § 1-5 er store foretak blant annet definert som allmennaksjeselskap⁶⁵. Bestemmelsens ordlyd slår fast at regelen gjelder store foretak, og at de har en plikt til å redegjøre for hva foretaket gjør jf. ”skal”. Forarbeidene til bestemmelsen angir ikke dette som et argumentasjonsgrunnlag i forbindelse med adgang til innsyn i politiattest i ansettelsesprosessen. Bestemmelsen, og plikten den gir uttrykk for, vil imidlertid kunne benyttes i en formålsargumentasjon dersom regnskapsloven kommer til anvendelse på virksomheten. Dette vil kunne være en del av hva foretaket gjør i sin daglige drift for å ivareta sin plikt til å bekjempe korrupsjon, og det vil utgjøre en del av virksomhetens prosedyrer i kraft av at de får innsyn i politiattest på kandidater som er aktuelle for stillingen og derav har mulighet til å luke ut kandidater som kan ha vært involvert i økonomisk kriminalitet tidligere.

Hensynene som er nevnt ovenfor er basert på virksomheter innenfor privat sektor og deres behov for innsyn i politiattest i ansettelsesprosessen. Det vil derfor måtte være tale om virksomheter med et utpreget ansvar og behov for lojalitet i henhold til økonomi og verdifull

⁵⁹ Dag W. Schartum og Lee A. Bygrave, *Personvern i informasjonssamfunnet*, 3.utgave, Bergen 2016 s. 93.

⁶⁰ OECD Guidelines for Multinational Enterprises <http://www.oecd.org/daf/inv/mne/48004323.pdf> s. 50, pkt. 78

⁶¹ Dag W. Schartum og Lee A. Bygrave, *Personvern i informasjonssamfunnet*, 3.utgave, Bergen 2016 s. 93.

⁶² Rskl. § 1-2

⁶³ Rskl. § 3-3 c) , femte ledd

⁶⁴ Rskl. § 3-3 c), første ledd, første setning.

⁶⁵ Rskl. § 1-5, nr.1.

informasjon hos kandidaten. Dette begrunnes i sensitiviteten av opplysningene og at det som et grunnleggende prinsipp må være forholdsmessighet mellom virksomhetens behov for opplysningene og kandidatens rett til vern av integritet og sensitive personopplysninger. Det vil i ytterste konsekvens være nødvendig å måtte vise til risiko for tilbakefall i tilfeller hvor vedkommende har vært innblandet i økonomisk kriminalitet tidligere. Da det foreligger lite konkret forskning på dette nasjonalt sett, vil dette kunne være en utfordring for arbeidsgiver. Samtidig er det viktig å ha i mente at de mange aktører i næringslivet innenfor privat sektor har tette bånd til det internasjonale markedet, hvor utspring av økonomisk kriminalitet og forskning på dette foreligger i større grad.

3. Rettslige utgangspunkt for behandling av personopplysninger

3.1 Innledning

Personopplysningsloven har et bredt nedslagsfelt da den i utgangspunktet kommer til anvendelse på all elektronisk behandling av personopplysninger og på (manuelle) personregistre. Loven fungerer i samordning med personopplysningsforskriften⁶⁶.

3.2 Lovens formål jf. poppl § 1

Formålsbestemmelsen i personopplysningsloven fremgår av § 1 hvor det står at ”Formålet med denne loven er å beskytte den enkelte mot at personvernet blir krenket gjennom behandling av personopplysninger. Loven skal bidra til at personopplysninger blir behandlet i samsvar med grunnleggende personvern hensyn, herunder behovet for personlig integritet, privatlivets fred og tilstrekkelig kvalitet på personopplysninger⁶⁷”.

Forarbeidene påpeker at bestemmelsen har flere funksjoner. Den gir først og fremst uttrykk for at personopplysninger skal behandles på en måte som er i samsvar med personvern hensyn. Bestemmelsen signaliserer ikke at personopplysninger skal behandles i minst mulig grad, men at de skal behandles på best mulig måte. Lovens formål derfor vil være et moment ved tolkning av andre relevante bestemmelser for oppgaven da den viser til ”grunnleggende personvern hensyn”. Grunnleggende personvern hensyn må kunne tenkes å ha samme mening som grunnleggende prinsipp på området for personvern. Blant disse prinsippene finner vi rettferdighet og rettmessighet, formålsbestemthet, minimalitet, opplysningskvalitet, medbestemmelse, informasjonssikkerhet og sensitivitet . Flere av disse prinsippene har sitt utspring i direktivet og Europarådskonvensjonen⁶⁸. Formålsbestemmelsen ses på som et utslag av festnede oppfatninger om personvern, slik det vil bli nedfelt i praksis fra domstolene, rettsteori og administrative avgjørelser.⁶⁹

⁶⁶ FOR-2000-12-15-1265

⁶⁷ Poppl. § 1

⁶⁸ Dag W. Schartum og Lee A. Bygrave, *Personvern i informasjonssamfunnet*, 3.utgave, Bergen 2016 s. 114,115,116 og 117

⁶⁹ NOU 1997:19 om poppl § 1.

3.3 Vilkår for behandling av personopplysninger

3.3.1 ”Saklig begrunnet i behandlingsansvarliges virksomhet” - formålet med behandlingen jf. poppl § 11, b)

Etter poppl. § 11, første ledd, b) kommer det frem at ”(Den behandlingsansvarlige skal sørge for at personopplysningene som behandles) ... Bare nyttes til uttrykkelig angitte formål som er saklig begrunnet i den behandlingsansvarliges virksomhet⁷⁰”.

Ordlyden i bestemmelsen indikerer at den slår fast at behandlingsansvarlige skal fastsette et formål for hver behandling av personopplysninger, og at behandling bare kan skje dersom det er saklig begrunnet i behandlingsansvarliges virksomhet. Forarbeidene presiserer at kravet til uttrykkelige og saklige formål gjelder både når opplysningene samles inn fra den registrerte og når opplysningene hentes fra andre kilder⁷¹. Videre må behandlingsansvarlige fastsette et formål som er tilstrekkelig konkret og avgrenset til at det skaper åpenhet og klarhet om hva behandlingen skal tjene til. Formålsbeskrivelsen må være mer presise enn de formål som angis i poppl. §§ 8 og 9, og jo større fare behandlingen kan medføre for personvernet, desto viktigere er det at formålet er presist definert slik at den registrerte kan gjøre sine rettigheter gjeldende⁷². Dette innebærer at det er lovstridig å behandle personopplysninger uten at et formål er uttrykkelig fastlagt, og at det er forbudt å behandle personopplysninger utenfor et eller flere angitte formål⁷³. Det stilles som vilkår at formålet skal være ”saklig begrunnet” i tilknytning til den behandlingsansvarliges virksomhet. Dette betyr at en arbeidsgiver ikke kan starte med behandling av personopplysninger som ligger utenfor deres forretnings- og virksomhets område⁷⁴. Formålet til arbeidsgiver vil i denne sammenhengen være å oppnå et så forsvarlig grunnlag for ansettelse som mulig sett i sammenheng med virksomhetens arbeidsoppgaver.

3.3.2 Behandling av personopplysninger jf. poppl. § 8

Den alminnelige regelen for behandling av personopplysninger fremgår av poppl. § 8, som inneholder en uttømmende opplisting av rettsgrunnlagene for behandling av personopplysninger. Her kommer det frem at ”... Personopplysninger (...) kan bare behandles dersom den registrerte har samtykket, eller det er fastsatt i lov at det er adgang til slik

⁷⁰ Poppl. § 11, første ledd, første setning ,b)

⁷¹ Ot.prp.nr.92 (1998-1999) s.114

⁷² Ot.prp.nr.92 (1998-1999) s. 114

⁷³ Dag W. Schartum og Lee A. Bygrave, *Personvern i informasjonssamfunnet*, 3. utgave, Bergen 2016 s. 185

⁷⁴ Dag W. Schartum og Lee A. Bygrave, *Personvern i informasjonssamfunnet*, 3. utgave, Bergen 2016 s. 185

behandling, eller at behandlingen er nødvendig for (...)”. Videre følger det alternativer som kan begrunne at behandlingen er nødvendig. Etter alternativet i bokstav f) fremgår det at ”(behandlingen er nødvendig for)... at den behandlingsansvarlige eller tredjepersoner som opplysningene utleveres til kan vareta en berettiget interesse, og hensynet til den registrertes personvern ikke overstiger denne interessen”. Ordlyden i bokstav f) tilsier at det skal foretas en forholdsmessighetsvurdering av vedkommendes interesse i personopplysningene mot hensynet til den registrertes vern av de personlige opplysninger. Dette er en bred skjønnsmessig vurdering hvor flere hensyn spiller inn, og rekkevidden er uklar.

Rettsgrunnlagene for behandling av personopplysninger etter poppl. § 8 er følgelig hjemmel i lov, samtykke eller at det er nødvendig for å ivareta en berettiget interesse.

3.3.3 Behandling av sensitive personopplysninger jf. poppl § 9

Poppl. § 9 inneholder ytterligere vilkår som må være tilstede for at behandling av sensitive personopplysninger kan finne sted. Bestemmelsen viser til at et av vilkårene i poppl. § 8 må være oppfylt, og at det må foreligge et rettslig grunnlag i form av samtykke, lovfestet adgang eller nødvendighet. I denne bestemmelsen er alternativene vedrørende nødvendighet tydeligere definert enn i poppl. § 8. Etter bokstav f) fremgår alternativet ” (at) behandlingen er nødvendig for at den behandlingsansvarlige kan gjennomføre sin arbeidsrettslige plikter eller rettigheter”. Av forarbeidene fremgår det at poppl. § 9 begrenser mulighetene til å behandle sensitive personopplysninger elektronisk eller innta slike i et manuelt personregister. Adgangen til å behandle sensitive personopplysninger begrenses ved å oppstille en uttømmende oppregning av når slike opplysninger kan behandles⁷⁵.

Det kommer imidlertid også frem at bestemmelsen inneholder nødvendige, men ikke alltid tilstrekkelige vilkår for å behandle sensitive personopplysninger. Dersom personopplysningene skal benyttes til å treffe visse former for kvalifiserte beslutninger, må det i tillegg søkes om konsesjon etter poppl. § 33⁷⁶.

⁷⁵ NOU 1997:19 Et bedre personvern, note til § 9.

⁷⁶ NOU 1997:19 Et bedre personvern, note til § 9.

3.4 Konesjonsmyndighet og vaktbikkje: Datatilsynet

3.4.1 Datatilsynets todelte funksjon – ombud og tilsyn

Datatilsynet er et uavhengig forvaltningsorgan administrativt underordnet Kongen og Kommunal og moderniserings departementet⁷⁷. Det kjennetegnes ved at det har en todelte funksjon; det fungerer både som tilsynsorgan og som ombud. Det ble opprettet som følge av personregisterloven som trådte i kraft i 1980. På den ene siden er Datatilsynet gitt generell kompetanse til å gi pålegg og stille vilkår for å sikre etterlevelse av loven jf. pol. § 46, siste ledd⁷⁸. På den andre siden er de gitt en rekke funksjoner som folkeopplyser og rådgiver jf. poppl. § 42, 2.ledd, nr. 1 og nr. 4-8. Datatilsynet har brukt mye tid på å utvikle ordningen med personvernombud, og utvikling av bransjenormer for personvern fremstår dessuten som en mulighet som delvis kan redusere behovet for tilsyn og kontroll med bransjene⁷⁹.

3.4.2 Datatilsynet og behandling av sensitive personopplysninger

Etter poppl. § 33 fremgår det i første ledd at "...Det kreves konsesjon fra Datatilsynet for å behandle sensitive personopplysninger. Dette gjelder likevel ikke for behandling av sensitive personopplysninger som er avgitt uoppfordret.⁸⁰" Ordlyden tilsier at det kreves tillatelse ved behandling av sensitive personopplysninger, med mindre disse er avgitt uoppfordret. Hva som ligger i begrepet uoppfordret er ikke gjenstand for videre redegjørelse i denne sammenhengen.

Forarbeidene gir ikke en særskilt veiledning utover ordlyden av § 33, første ledd, men det er på det rene at det er tale om opplysninger som ved behandling av sensitivitetsgrunner har et større behov for tilsyn og kontroll. Schartum og Bygrave nevner imidlertid at det i utgangspunktet bare er behandling av sensitive personopplysninger som er konsesjonspliktige. Det er nok at en opplysningstype har denne karakteren for at hele behandlingen av personopplysninger må ha forhåndsgodkjenning⁸¹. Av Datatilsynets hjemmesider fremgår det at man ved tildelt konsesjon får tillatelse til å behandle sensitive personopplysninger innenfor tidsrammen som vedtaket angir⁸².

Poppl. § 34 angir vurderingstemaet for om konsesjon skal tildeles eller ikke. Her kommer det frem at "... Ved avgjørelsen av om konsesjon skal gis, skal det klarlegges om behandlingen

⁷⁷ www.datatilsynet.no : Om Datatilsynets oppgaver

⁷⁸ Dag W. Schartum og Lee A. Bygrave, *Personvern i informasjonssamfunnet*, 3.utgave, Bergen 2016 s. 225

⁷⁹ Dag W. Schartum og Lee A. Bygrave, *Personvern i informasjonssamfunnet*, 3.utgave, Bergen 2016 s. 226

⁸⁰ Poppl. § 33, første ledd

⁸¹ Dag W. Schartum og Lee A. Bygrave, *Personvern i informasjonssamfunnet*, 3.utgave, Bergen 2016 s. 229

⁸² www.datatilsynet.no : "Slik søker du konsesjon"

av personopplysninger kan volde ulemper for den enkelte som ikke avhjelpes gjennom bestemmelsene i kapitlene II-V og vilkår etter § 35. I så fall må det vurderes om ulempene blir oppveid av hensyn som taler for behandlingen”.

Ordlyden legger til grunn forholdsmessighetsvurderingen som går igjen i flere bestemmelser i personopplysningsloven, herunder § 8, f). Av forarbeidene fremgår det at bestemmelsen angir den interesseavveiningen som må foretas når det skal vurderes om konsesjon skal gis. Som ledd i vurderingen av om det skal gis konsesjon må det først klarlegges om personopplysningsbehandlingen vil volde problemer for den enkelte, og om problemene eventuelt avhjelpes ved lovens regler for behandlingen. Hvis behandlingen ikke volder problemer for den enkelte, vil det som regel ikke være aktuelt å nekte konsesjon. En rekke ulike interesser vil måtte veies opp mot hverandre – økonomiske så vel som ideelle⁸³.

Schartum og Bygrave stiller spørsmålet om ”ulemper for den enkelte” bare kan gjelde ulemper i form av personvernkrænkelser, eller om også andre ulemper for de registrerte kan telle med. De konkluderer med at det klart nok er ulemper knyttet til personvernet det siktes til her, men at det også er rom for å trekke inn andre ulemper⁸⁴. Videre fremheves det at det ikke er noen begrensninger i hvilke argumenter konsesjonssøker kan anføre, og at argumentene kan være av politisk, økonomisk eller strategisk art⁸⁵. Dette indikerer at arbeidsgivers adgang til å argumentere for begrensninger i personvernet er åpen.

3.4.3 Unntak fra konsesjonsplikt – personopplysningsforskriften

Slik redegjørelsen ovenfor viser, er det alminnelige utgangspunktet at det må søkes om konsesjon ved behandling av sensitive personopplysninger. Etter personopplysningsloven § 33, femte ledd kan det i forskrift nærmere bestemmes at «visse behandlingsmåter eller behandlingsansvarlige» ikke krever konsesjon. I medhold av poppl. § 33, femte ledd er det i personopplysningsforskriften § 7-16 gitt en bestemmelse om arbeidsgivers behandling av personopplysninger om nåværende eller tidligere ansatte⁸⁶. Etter pof. § 7-13, første ledd fremgår det at ”... Behandlinger som omfattes av dette kapitlet, er unntatt fra konsesjonsplikten etter personopplysningsloven § 33 første ledd og fra meldeplikten etter § 31 første ledd.” Bestemmelsen legger altså til grunn at dersom behandlingen av opplysningene er omfattet av dette kapitlet, er den unntatt fra henholdsvis konsesjons og meldeplikt.

⁸³ Ot.prp.nr.92 (1998-1999) s. 130

⁸⁴ Dag W. Schartum og Lee A. Bygrave, *Personvern i informasjonssamfunnet*, 3.utgave, Bergen 2016 s.232

⁸⁵ Dag W. Schartum og Lee A. Bygrave, *Personvern i informasjonssamfunnet*, 3.utgave, Bergen 2016 s. 232

⁸⁶ Bing, Jon: Samtykke til behandling av personopplysninger i arbeidsforhold, FEST-2009-hj-45 s.61

Pof. § 7-16 omhandler personalregistre. I første ledd fremgår det frem at bestemmelsen kommer til anvendelse på "...Arbeidsgivers behandling av ikke- sensitive personopplysninger om (...) samt søkere til en til en stilling er unntatt meldeplikt etter pol. § 31, første ledd." Videre kommer det i andre ledd frem at "... Dersom det behandles sensitive personopplysninger, er behandlingen unntatt fra konsesjonsplikten etter personopplysningsloven § 33 første ledd, men underlagt meldeplikten etter § 31 første ledd." Unntaket fra konsesjonsplikten kommer til anvendelse så fremt tre kumulative vilkår er oppfylt. Den registrerte må ha samtykket i behandlingen eller at behandlingen er fastsatt i lov, opplysningene må være knyttet til arbeidsforholdet og personopplysningene må behandles som ledd i personaladministrasjonen⁸⁷.

Bestemmelsens første ledd forutsetter klart at en arbeidsgiver som behandler personopplysninger i ansettelsesprosessen er fritatt meldeplikt. Spørsmålet er om unntaket fra konsesjonsplikt i andre ledd også kommer til anvendelse på en arbeidsgiver som ønsker å behandle sensitive personopplysninger i ansettelsesprosessen. Etter ordlyden i andre ledd kommer ikke dette eksplisitt til uttrykk. Utover bestemmelsen og dens ordlyd foreligger det lite eller ingen ytterligere presisering av bestemmelsens innhold og formål i forarbeider eller praksis. At bestemmelsen er uklar på dette området er negativt fordi det kan bidra til forvirring rundt praktisering av når det er fritak fra konsesjonsplikt og når det ikke er det.

I mangel av andre rettskilder må det foretas en kontekstuell tolkning hvor andre bestemmelser av relevans for spørsmålet nyttes som tolkningsverktøy. Poppl. §§ 33 og 34 viser at avgjørelsen om konsesjon skal tildeles kan være ressurskrevende. Dette begrunnes i vurderingene som skal foretas for om forholdsmessighet mellom inngrep og vern av integritet er oppfylt. Dette understøttes også av at det i poppl. § 33 femte ledd er gitt hjemmel for ytterligere regulering i forskrift. Det er derfor naturlig å tenke seg at formålet med bestemmelsen i pof. § 7-16 er å bidra til en mer effektiv og ressurs sparende behandling av personopplysninger for arbeidsgiver. I tillegg til dette vil det lette arbeidsbyrden til Datatilsynet ved at arbeidsgiver ved meldeplikt er gitt adgang til å behandle sensitive personopplysninger, under forutsetning av at det foreligger hjemmel i lov eller et gyldig samtykke. Det ville forøvrig også bydd på praktiske utfordringer dersom det måtte søkes om

⁸⁷ Pof. § 7-16, andre ledd.

konsesjon hver gang virksomheten skulle foreta ansettelser jf. kravene som stilles til konsesjonssøknad⁸⁸.

Det er imidlertid verdt å bemerke at ”nødvendighet” som hjemmelsgrunnlag ikke kan benyttes ved unntak fra konsesjonsplikten. Dette kan henge sammen med at vurderingen av hva som er ”nødvendig” for en virksomhet er en konkret skjønns- og forholdsmessighetsvurdering, og har et større behov for å bli forhåndkontrollert av Datatilsynet enn det samtykke og hjemmel i lov har.

På bakgrunn av dette konkluderes det med at arbeidsgiver er unntatt konsesjonsplikt ved behandling av sensitive personopplysninger, under forutsetning at de tre kumulative vilkårene i pof. § 7-16, andre ledd er oppfylt.

⁸⁸ Poppl. § 34 om avgjørelsen om konsesjon skal gis.

4. Hjemmelsgrunnlag for behandling av sensitive personopplysninger

4.1 Innledning

Dette kapittelet tar for seg de ulike hjemmelsgrunnlagene poppl. oppstiller for behandling av personopplysninger. Oppgaven tar utgangspunkt i behandling av opplysninger som angitt i poppl. § 2, nr.8 b), og kapittelet tar sikte på å kartlegge hvilke krav som stilles til hjemmel for private virksomheter som ønsker innsyn i politiattest i ansettelsesprosessen.

4.2 ”Hjemmel i lov” jf. poppl. § 8, første ledd og § 9, første ledd b)

Både poppl. §§ 8 og 9 angir hjemmel i lov som et rettsgrunnlag for behandling av personopplysninger. Om behandlingen har tilstrekkelig lovhjemmel må avgjøres ved å tolke den aktuelle loven, eller å ta utgangspunkt i hvilke opplysninger som skal behandles. Forarbeidene gir ikke noen særskilt veiledning på hvilke opplysninger det kreves hjemmel i lov for å behandle etter poppl. § 9 utover at den angir et av de grunnleggende vilkårene for behandling av personopplysninger. Hjemmelskravet er ikke statisk, men vil til en viss grad variere avhengig av hvor inngripende behandlingen er for den enkelte. Jo mer inngripende behandlingen er for den enkelte, jo strengere krav må settes til klar lovforankring⁸⁹. I dette tilfellet er det tale om opplysninger som er tett knyttet til individets integritet, og dette indikerer at det vil kunne foreligge et strengt krav til en klar lovhjemmel.

4.2.1 Særregulering av opplysninger angitt i poppl. § 2, nr.8 b) jf. poppl. § 10

Etter poppl. § 10 fremgår det at ” Et fullstendig register over straffedommer kan bare føres under kontroll av offentlig myndighet”.

Bestemmelsen har bakgrunn i direktivet artikkel 8 nr. 5 som krever at fullstendig registre over straffedommer bare kan føres under kontroll av offentlig myndighet. I dette ligger det at private ikke kan bygge opp slike registre – verken manuelt eller elektronisk. Annen form for behandling av denne type opplysninger vil i utgangspunktet kreve konsesjon⁹⁰.

Problemstillingen omhandler arbeidsgivers bruk av opplysningene i ansettelsesprosessen. Det vil i denne situasjonen være aktuelt å benytte opplysningene som et ledd i et forsvarlig ansettelsesgrunnlag og formålet vil således ikke være å opprette et register over straffedommer på kandidater i ansettelsesprosessen. Denne bestemmelsen er derfor ikke til

⁸⁹ NOU 1997:19 s.140

⁹⁰ Ot.prp.nr.92 (1998-1999) 16 Merknader til de enkelte paragrafene, til § 10

hinder for at en privat virksomhet kan behandle opplysninger som angitt i poppl. § 2 nr.8 b) i ansettelsesprosessen.

4.3 Opplysninger om en at en person har vært mistenkt, siktet, tiltalt eller dømt for en straffbar handling jf. poppl. § 2,nr.8 b)

4.3.1 Særlovgivning for innsyn i politi/vandelsattest – Politiregisterloven 28.mai, 2010 nr.16

Politiregisterloven regulerer politiets behandling av personopplysninger. Personopplysninger som blir behandlet i henhold til rettspleielovene, er delvis unntatt fra personopplysningsloven jf. pof § 1-3 og pol. § 3⁹¹. Dette unntaket fra individuell rett til opplysninger er, i henhold til strafferettspleien, begrunnet i at det ville være ødeleggende i etterforskningsøyemed. Det individuelle unntaket kommer altså til anvendelse er i den grad opplysningene brukes i politiarbeid. Politiregisterloven inneholder enkelte bestemmelser som har stor betydning for personvernet. Dette gjelder særlige vilkår for opprettelse av politiregistre, utferdigelse av politiattester og taushetsplikt⁹².

Av poppl. § 2, nr.8 b) fremgår det at opplysninger om at en person har vært mistenkt, siktet, tiltalt eller dømt for en straffbar handling er en sensitiv personopplysning og at konsesjon derfor er en forutsetning for behandling av opplysningene. Det er tidligere slått fast at arbeidsgiver vil være unntatt fra konsesjonsplikten jf. pof. § 7-16, andre ledd, men en forutsetning for unntakets anvendelse er at det foreligger enten hjemmel i lov eller samtykke. Personopplysningsloven inneholder ikke en klar lovhjemmel for private virksomheters rett til innsyn i politiattest i ansettelsesprosessen. Spørsmålet er om politiregisterloven inneholder en bestemmelse som hjemler denne adgangen, og på hvilke premisser hjemmel anses oppnådd.

4.3.2 Politiattest og hvilke formål som berettiger bruk av denne

I bestemmelsen om vandelskontroll og attester kommer det i politiregisterloven § 36, første ledd nr.1 frem at ”Vandelskontroll kan bare foretas når den har *hjemmel i lov* eller *i forskrift gitt i medhold av lov*⁹³.” Videre legger bestemmelsen til grunn at vandelskontroll kan *utstedes*⁹⁴ som politiattest, hvor dokumentet utstedes til bruk i mottakers interesse og kan inneholde opplysninger om hvorvidt en fysisk eller juridisk person har vært ilagt straff eller

⁹¹Dag W. Schartum og Lee A. Bygrave, *Personvern i informasjonssamfunnet*, 3.utgave, Bergen 2016 s.280

⁹² Dag W. Schartum og Lee A. Bygrave, *Personvern i informasjonssamfunnet*, 3.utgave, Bergen 2016 s.283

⁹³ Min kursivering

⁹⁴ Min kursivering

andre strafferettslige reaksjoner eller andre tiltak som følge av lovbrudd, eller er under straffeforfølgning (...). Bestemmelsen fastsetter at politiet kan utlevere opplysninger i forbindelse med vandelskontroll, når det er hjemmel i lov eller forskrift gitt i medhold av lov⁹⁵. Felles for vandelskontrollene er at de må karakteriseres som en særlig form for unntak fra taushetspliktreglene, der det gis ut opplysninger om en persons vandel, som oftest i mottakers interesse⁹⁶.

Bestemmelsen i politiregisterloven § 37 angir formålene som berettiger bruk av politiattest. I første ledd, nr.1 og nr.6 kommer det frem at en ”politiattest bare kan brukes for å utelukke fysiske og juridiske personer fra stilling, virksomhets, aktivitet eller annen funksjon dersom (...) 1. lovbruddet gjør en person uegnet, og manglende utelukkelse vil kunne medføre betydelige skadevirkninger”, eller,” (nr.6.) det er fare for at personen på ny vil begå lovbrudd”. I denne drøftelsen er det tatt stilling til alternativene i nr. 1 og nr. 6 da det er disse som er mest relevante for problemstillingen. Bestemmelsen gir anvisning på de formål som kan begrunne bestemmelser om krav om politiattest. Bestemmelsen gir således ikke alene hjemmel for utstedelse av politiattest, men indikerer til hvilke formål attesthjemler bør utstedes⁹⁷.

Forarbeidene utdyper et stykke på vei hvilken reell betydning bestemmelsene har. Første ledd, nr.1 kommer til anvendelse i de tilfellene hvor det foreligger samfunnsmessige hensyn som gjør det nødvendig at vedkommende er skikket. Her kan lovbrudd i forbindelse med rus og narkotika spille en rolle for vedkommendes skikkethet, og forarbeidene eksemplifiserer med at det ved utstedelse av transportløyver og sertifikater innenfor luftfart foreligger samfunnsmessige hensyn som legitimerer innsyn i politiattest. Selv om lovbruddene kan ha blitt begått en stund tilbake i tid og det ikke er noen holdepunkter for at de vil bli begått på ny, vil det kunne gis hjemmel til innsyn dersom det foreligger samfunnsmessige hensyn i henhold til dette⁹⁸.

Etter første ledd nr. 6 kan politiattest brukes for å hindre at personer som tidligere er straffet får stillinger hvor det er fare for at de på nytt vil begå straffbare handlinger. Her tas det sikte på å utelukke personer som bevisst ønsker seg et yrke eller en posisjon hvor de kan videreføre sin kriminelle virksomhet, men også på tilfeller hvor det på grunn av vedkommendes tidligere

⁹⁵ Ot.prp.nr.108 (2008-2009) s.311

⁹⁶ Ot.prp.nr.108 (2008-2009) 12.2.1 Innledning

⁹⁷ Ot.prp.nr.108(2008-2009) s. 312

⁹⁸ Ot.prp.nr.108 (2008-2009) til nr. 312

kriminelle adferd vil utgjøre en risiko å plassere personen i en arbeidssituasjon hvor en ny straffbar handling kan bli begått⁹⁹. Bestemmelsene viser at det er gitt relativt vide rammer for hvilke hjemler som kan utstedes. Forarbeidene peker også på at bestemmelsen ikke er en skranke for lovgiver med tanke på hvilke konkrete formål og situasjoner man i fremtiden kan gi hjemmel for å utstede politiattest til¹⁰⁰.

I arbeidet med politiregisterloven ble det pekt på noen essensielle momenter i tilknytning til utlevering av politiattest. Utvalget fremholdt at EMK artikkel 8 setter naturlige ytre rammer for vurderingen av hvilke formål som berettiger politiattest, herunder at det må fremme et av de legitime formålene i EMK og være nødvendig i et demokratisk samfunn. Innenfor disse rammene ble det oppstilt noen typetilfeller hvor bruk av politiattest er berettiget. Adgangen til å kreve politiattest ble opprinnelig brukt ved ansettelse i stillinger eller posisjoner hvor det var særlig viktig å ha tillit til den personen som skulle ansettes. Et av hovedformålene synes i følge utvalget å ha vært behovet for å sikre seg mot å ansette personer som på grunn av sin fortid kunne representere en risiko for virksomheten som sådan. I arbeidet med politiregisterloven pekte utvalget også på et økende behov for å beskytte samfunnsmessige og økonomiske interesser¹⁰¹. I vurderingen av om det var nødvendig med et nytt hjemmelsgrunnlag for å utstede politiattest, måtte det i følge utvalget også tas hensyn til risikoen forbundet med at det ville bli begått nye straffbare forhold. Som eksempel ble det nevnt at personer som tidligere har begått vinningskriminalitet eller økonomisk kriminalitet ofte kunne ha økonomiske problemer og at sannsynligheten for nye lovbrudd sannsynligvis er stor¹⁰².

Basert på denne redegjørelsen vil private virksomheters behov for et forsvarlig ansettelsesgrunnlag ha forutsetninger for å kunne hjemles i politiregisterloven § 36, første ledd jf. §37, nr.1 og nr.6. Formålet til arbeidsgiver vil være å skjerme virksomheten fra ansettelser som kan ha et skadepotensial, hvilket harmonerer med forarbeidenes uttalelser om dette. Bestemmelsen i § 36, første ledd er imidlertid for vag til at det er forsvarlig å innfortolke et grunnlag for hjemmel, og det fremgår også at bestemmelsen ikke kan benyttes som hjemmel på selvstendig grunnlag. Forarbeidene legger opp til en streng fortolkning av hjemmelskravet om klar hjemmel i lov eller forskrift for rett til utstedelse av politiattest i ansettelsesprosessen. Slik det fremgår av dagens politiregisterlov inneholder ikke denne en

⁹⁹ Ot.prp.nr.108 (2008-2009) til nr. 312

¹⁰⁰ Ot.prp.nr. 108 (2008-2009) s.312

¹⁰¹ Ot.prp.nr.108 (2008-2009) s.149

¹⁰² Ot.prp.nr.108 (2008-2009) s.150

klar hjemmel for utstedelse av politiattest i ansettelsesprosessen til private virksomheter. Det må derfor ses til politiregisterforskriften om tilstrekkelig hjemmel er nedfelt der.

4.3.3 Politiregisterforskriften 2013

Politiregisterforskriften¹⁰³ fungerer i samordning med politiregisterloven og den angir konkrete hjemler for utstedelse av politiattest. Etter forskriftens § 28-2 om ”Generelt om politiattest” fremgår det at ”... Politiattest kan bare utstedes når det er hjemlet i lov eller i forskrift gitt i medhold av lov”.

Forskriftens kapittel 34 angår politiattest på områder uten lovregulering. Kapittelet kommer til anvendelse fordi det ikke foreligger en uttrykkelig hjemmel i politiregisterloven om at private virksomheter har rett til utstedelse av politiattest i ansettelsesprosessen. I dette tilfellet angir heller ikke forskriften en uttrykkelig hjemmel til innsynsrett, selv i kapittelet for områder uten lovregulering.

Etter en tolkning av personopplysningsloven, politiregisterloven og politiregisterforskriften sett i lys av forarbeidene og systemhensyn på rettsområdet er det kommet frem at det ikke foreligger hjemmel i lov eller forskrift som gir private virksomheter rett til utstedelse av politiattest i ansettelsesprosessen etter personopplysningsloven eller politiregisterloven med tilhørende forskrift. Dette kan derfor ikke benyttes som hjemmelsgrunnlag ved behandling av sensitive personopplysninger.

I mangel av hjemmel av lov som grunnlag for rett til utstedelse må det derfor ses til andre bestemmelser i personopplysningsloven for oppfylling av kravet om hjemmelsgrunnlag for behandling av sensitive personopplysninger i ansettelsesprosessen.

4.4 ”Samtykke” jf. pol § 2, nr.7 jf. § 9, første ledd, a) som hjemmelsgrunnlag

4.4.1 Hva er et samtykke etter personopplysningsloven?

Legaldefinisjonen av samtykke fremgår av poppl. § 2 nr.7 hvor det står at ” (samtykke er)... en frivillig, uttrykkelig og informert erklæring fra den registrerte om at han eller hun godtar behandling av opplysninger om seg selv,”¹⁰⁴. Bestemmelsen gir uttrykk for at utgangspunktet er at det er individet som selv bestemmer over sine personlige opplysninger og hvem som skal få behandle de i kraft av at behandlingen godtas av vedkommende.

¹⁰³ FOR-2013-09-20-1097

¹⁰⁴ Poppl. § 2 nr.7.

Forarbeidene legger til grunn at samtykket i utgangspunktet må gis av den registrerte selv. Det stilles ikke noe formkrav til samtykket, som kan gis skriftlig eller muntlig. Det må imidlertid klart og utvetydig fremgå at det samtykkes, hvilke behandlinger samtykket omfatter og hvilke behandlingensvarlige det er rettet til jf. kravet til at samtykket skal være ”uttrykkelig”. Det holder ikke med et passivt eller stilltiende samtykke, og heller ikke samtykke gjennom såkalt konkludent atferd er tilstrekkelig¹⁰⁵. Da det er den behandlingsansvarlige som vil måtte sannsynliggjøre at det foreligger et samtykke, kan skriftlighet med signatur være en fornuftig løsning, spesielt i forbindelse med behandling av sensitive personopplysninger jf. § 9¹⁰⁶.

Samtykket må være frivillig. I dette ligger det at et samtykke ikke er gyldig dersom det er påvirket av tvang eller trusler¹⁰⁷. Videre stilles det krav om at erklæringen må være ”informert”. I dette ligger at den registrerte må forstå hva en erklæring om samtykke gjelder, og hvilke konsekvenser denne får eller kan få. Det legges i denne forbindelse til at den registrerte når som helst kan trekke tilbake sitt samtykke. I så fall kan behandlingen som samtykket bygger på ikke lenger foretas¹⁰⁸.

Datatilsynet legger i sin lovtolkning til grunn at samtykke er hovedregelen i både poppl. §§ 8 og 9¹⁰⁹. Dette innebærer at dersom en kandidat samtykker til at sensitive personopplysninger blir behandlet, er dette et rettslig grunnlag for adgang til behandling av sensitive personopplysninger i henhold til personopplysningsloven¹¹⁰. Det eksisterer ikke en eksplisitt prioriteringsrekkefølge mellom de tre grunnlagene for å behandle sensitive personopplysninger, men samtykke som hjemmelsgrunnlag er følgelig et viktig ideologisk og systematisk utgangspunkt for både personverndirektivet og de norske personopplysningsreglene¹¹¹.

Under drøftelsen av om det foreligger hjemmel i lov for private virksomheter til å kreve utstedelse av politiattest i ansettelsesprosessen, ble det konkludert med at det ikke foreligger en tilstrekkelig klar lovhjemmel for dette. En arbeidsgiver i privat sektor er derfor avskåret fra å kreve utstedelse av politiattest i ansettelsesprosessen etter politiregisterloven med tilhørende forskrift.

¹⁰⁵ NOU 1997:19 s.134

¹⁰⁶ Ot.prp.nr. 92 (1998-1999) s. 104

¹⁰⁷ Ot.prp.nr.92 (1998-1999) s. 104 og 105

¹⁰⁸ Ot.prp.nr. 92 (1998-1999) s. 105

¹⁰⁹ PVN-2004-1 pkt. 5 ”Datatilsynets vurdering”

¹¹⁰ Ot.prp.nr.92 1998-1999 s.110

¹¹¹ Dag W. Schartum og Lee A. Bygrave, *Personvern i informasjonssamfunnet*, 3.utgave, Bergen 2016 s. 183

Spørsmålet er derfor om et samtykke til å vedlegge politiattest i ansettelsesprosessen er et gyldig samtykke i henhold til personopplysningsloven.

4.4.2 Samtykke til fremleggelse av politiattest i ansettelsesprosessen

Det er på det rene at det i ansettelsesprosessen hersker et ujevnt styrkeforhold. Situasjonen bærer preg av at det er arbeidsgiver som sitter med godet, og kandidaten som må ”bevise” at det er han eller hun som bør bli tildelt muligheten til å jobbe for virksomheten. Dette settes på spissen ved behandling av personopplysninger i ansettelsesprosessen, og utfordrer forutsetningene for at et fullgodt samtykke i henhold til lov er avgitt. Det er imidlertid arbeidsgiver som har bevisbyrden for at et gyldig samtykke er gitt.

Peter Blume har i dansk personvernrett tatt til orde for den ujevne styrkeforholdet som oppstår i en situasjon med arbeidsgiver og en kandidat eller arbeidstager. Han viser til at personvernspørsmålene som oppstår i en slik situasjon, bærer preg av å være hierarkisk og som karakteriseres ved ulikhet. Det foreligger derfor på denne bakgrunn et særlig beskyttelsesbehov¹¹². Han legger videre til grunn at arbeidsplassen representerer et miljø hvor det kan være risiko for at personopplysninger misbrukes, og hvor det kan være vanskelig å oppnå et effektivt integritetsvern. Dette kan begrunne en tilbakeholdenhet med å benytte samtykke som hjemmelsgrunnlag, særlig i henhold til sensitive personopplysninger, ikke minst i situasjoner hvor det reelt sett ikke er noen mulighet for å samtykke¹¹³.

Kandidatens selvbestemmelsesrett og frivillighet i forbindelse med samtykke til innsyn i personopplysninger er imidlertid et viktig moment på flere måter. Samtykke er ansett som det ideologisk sett viktigste grunnlaget for behandling av personopplysninger i kraft av denne selvbestemmelsesretten. Dette innebærer at dersom kandidaten samtykker til å vedlegge politiattest og gi arbeidsgiver innsyn i denne i ansettelsesprosessen, så spiller det en mindre rolle om arbeidsgiver ikke har hjemmel i lov for rett til utstedelse. Kandidaten har i kraft av sin selvbestemmelsesrett bestemt at det er i orden. Dette er et viktig moment i balanseringen av samtykkedrøftelsen da det er kandidaten som eier retten til sine personopplysninger.

¹¹² Blume, Peter ” Databeskyttelsesret” 3. utgave, 1. opplag 2008 s. 255

¹¹³ Blume, Peter ” Databeskyttelsesret” 3. utgave, 1. opplag 2008 s. 255

Jon Bing har også uttalt seg om problemstillingen i artikkelen ” Samtykke til behandling av personopplysninger i arbeidsforholdet”¹¹⁴. Selv om artikkelen primært omhandler arbeidstagers samtykke i arbeidsforholdet, har han flere poeng som berører problemstillingen på et overordnet plan. I forbindelse med at samtykket må være frivillig, understreker han at tvang per definisjon sjelden vil være noe problem i et arbeidsforhold. Problemet er heller at arbeidsgiver i kraft av sin styringsrett alltid vil ha mulighet til myke sanksjoner eller belønninger i forbindelse med samtykke¹¹⁵. Her vil potensielle konsekvenser av manglende samtykke ha stor betydning for om det foreligger et gyldig samtykke. Dette har overføringsverdi til ansettelsesprosessen og kandidatens ønske om å oppfylle alle arbeidsgivers ønsker, og om det reelt sett foreligger et samtykke til å legge ved politiattest.

Et samtykke, og hva som legges i dette, er samtidig også individuelt. For noen kandidater kan det å legge frem en politiattest oppleves som helt legitimt såfremt arbeidsgiver har informert tilstrekkelig om formålet. For andre kandidater kan det oppleves som svært inngripende og integritetskrenkende å måtte legge dette frem, selv om vedkommende skulle ha plettfri vandel. Hva som er et samtykke i henhold til loven baseres på hvilken personlig oppfatning kandidaten har, og dette kan det være utfordrende å føre bevis for. Et moment som for øvrig bør nevnes er at et samtykke når som helst kan trekkes tilbake i kraft av den registrertes selvbestemmelsesrett. Dette vil potensielt gjøre samtykke til et noe upraktisk hjemmelsgrunnlag for arbeidsgiver all den tid kandidaten kan trekke samtykke, og derav hjemmelsgrunnlag, tilbake.

Vurderingen av samtykke som hjemmelsgrunnlag er utfordrende og jo dypere man trer inn i samtykkets materie og vurderingen av hva som er et gyldig samtykke, dess mer utfordrende blir det. Dette underbygges av at samtykkebestemmelsene har vanskeligheter med å definere hva som kvalifiserer til et fullgodt samtykke. Det springende punkt later til å være om frivillighetskriteriet er oppfylt når dette ses sammenheng med situasjonen kandidaten befinner seg i. Her er det utvilsomt et viktig poeng at det er tale om en ansettelsesprosess, som igjen kan tale for at samtykke ikke skal kunne benyttes som hjemmelsgrunnlag.

Viktigheten av et fullt ut frivillig samtykke sett i sammenheng med situasjonen kandidaten befinner seg i, vil resultere i at det må legges til grunn en høy terskel for å godta et samtykke som hjemmel ved krav om fremleggelse av politiattest i ansettelsesprosessen. Det konkluderes

¹¹⁴ Bing, Jon: Samtykke til behandling av personopplysninger i arbeidsforhold, FEST-2009-hj-45

¹¹⁵ Bing, Jon: Samtykke til behandling av personopplysninger i arbeidsforhold, FEST-2009-hj-45 s.59

derfor med at samtykke, under tvil, kan benyttes som hjemmelsgrunnlag for behandling av sensitive personopplysninger i ansettelsesprosessen. En konkret vurdering vil i alle tilfelle måtte legges til grunn ved avgjørelse om samtykket er gyldig i henhold til poppl. § 2 nr.7.

4.5 ”Nødvendig for å gjennomføre arbeidsrettslige plikter eller rettigheter” jf. poppl. § 9, første ledd, f)

Av poppl. § 9, første ledd, f) fremgår det at sensitive personopplysninger kan behandles dersom ”... behandlingen er nødvendig for at den behandlingsansvarlige⁵ kan gjennomføre sine arbeidsrettslige plikter eller rettigheter,”¹¹⁶.

Selv om det verken foreligger samtykke eller hjemmel i lov, åpner personopplysningsloven for at opplysningene kan behandles dersom dette er ”nødvendig” for å realisere visse formål eller virkninger som er konkret angitt i loven¹¹⁷. Ordlyden av ”nødvendig” indikerer at behandlingen av opplysningene anses som en forutsetning for at formålet skal kunne realiseres.

Verken lovteksten eller forarbeidene gir særskilt veiledning på hvordan begrepet ”nødvendig” bør tolkes i denne sammenhengen. Dette er fordi ”nødvendig” tolkes konkret i tilknytning til hvilken type opplysninger som skal behandles. Flere av nødvendighetsalternativene er imidlertid så løst formulert at minst ett alternativ kan hevdes å passe de fleste situasjoner¹¹⁸. Noe veiledning kan imidlertid hentes fra en klagesak i personvernemnda. Nemnda uttaler seg her om hva som skal til for å fravike ”hovedregelen” samtykke og det fremgår da at:

For at man skal kunne gjøre et avvik fra hovedprinsippet(les. samtykke)¹¹⁹, må det derfor foreligge en begrunnelse. Denne begrunnelsen kan, som nevnt ovenfor, ikke bare være en ren hensiktsmessighetsbetraktning, f eks å unngå kostnader, spare tid eller lignende – selv om slike begrunnelser selvsagt også må vurderes konkret i forhold til den enkelte sak.¹²⁰

Uttalelsen indikerer at det må foreligge noe mer enn en hensiktsmessighetsbetraktning. Den helgarderer seg imidlertid ved å tilføye at hvis det skulle være hensiktsmessighetsbetraktninger som lå til grunn så må det allikevel vurderes konkret i den

¹¹⁶ Poppl. § 9, f).

¹¹⁷ Dag W. Schartum og Lee A. Bygrave, *Personvern i informasjonssamfunnet*, 3.utgave, Bergen 2016 s. 181

¹¹⁸ Dag W. Schartum og Lee A. Bygrave, *Personvern i informasjonssamfunnet*, 3.utgave, Bergen 2016 s. 183

¹¹⁹ Min referering

¹²⁰ PVN-2004-1 pkt.6 ”Personvernemndas vurderinger”

enkelte sak. Bestemmelsen angir en form for terskel, men beholder samtidig fleksibiliteten og vagheten som er karakteristisk for flere av bestemmelsene i personopplysningsloven.

Det første spørsmålet er om bestemmelsen kommer til anvendelse på ansettelsesprosessen jf. ”arbeidsrettslige rettigheter og plikter”. Den naturlige språklige forståelsen av ”arbeidsrettslige rettigheter og plikter” gir uttrykk for å være forhold som blir aktualisert i selve arbeidsforholdet. Etter forarbeidene fremgår det at uttrykket «arbeidsrettslige plikter eller rettigheter» omfatter alle plikter og rettigheter som hviler på et arbeidsrettslig grunnlag, uansett om grunnlaget er lovgivning, avtale mellom partene i arbeidslivet, eller individuelle arbeidsavtaler (ansettelseskontrakter)¹²¹. En ansettelseskontrakt er, med de begrensninger aml. uttrykker, det primære juridiske grunnlaget for ansettelsesforholdet. Forarbeidene tar ikke stilling til om bestemmelsen kommer til anvendelse i ansettelsesprosessen, og det er ingen andre rettskilder som tar stilling til bestemmelsens anvendelsesområde.

Bestemmelsen må derfor tolkes utfra systematiske betraktninger og hva som kan sies å gi det beste resultatet. Slik det fremgår av øvrig personvernlovgivning vedrørende politiattest, er terskelen høy for innsyn i denne typen opplysninger. Personopplysningsforskriften § 7-16 andre ledd angir for eksempel ikke nødvendighet som et gyldig grunnlag for unntak fra konsesjonsplikten.

På den ene siden foreligger ingen uttrykkelig hjemmel i lov for private virksomheters innsynsrett, og samtykke har vist seg å være et hjemmelsgrunnlag som byr på utfordringer gitt konteksten det avgis i. Dette oppfordrer til å vise forsiktighet med en utvidende fortolkning av bestemmelsens anvendelsesområde, da denne tolkningen ikke kan sies å inneha den samme rettskildemessige tyngden som hjemmel i lov og samtykke har. På den andre siden er det i poppl. § 9 tale om alternative hjemmelsgrunnlag som alle kan komme til anvendelse dersom vilkårene er oppfylt. Rettsgrunnlaget i poppl. § 9, første ledd f) kan derfor ikke kategoriseres som mindreverdige fordi det ikke er hjemmel i lov eller samtykke. Det er like fullt lagt til grunn som et hjemmelsgrunnlag for behandling av sensitive personopplysninger.

Utgangspunktet er at arbeidsgiver i privat sektor står friere enn arbeidsgiver i offentlig sektor på mange områder. Til en viss utstrekning gjelder dette også arbeidsavtaler, og det er tidligere redegjort for behovet næringslivet har for å gjøre tilpasninger i henhold til internasjonale avtaleparter, samt hensynet til kriminalitetsforebyggende arbeid og sikring av virksomheten.

¹²¹ Ot.prp.nr. 92 (1998-1999) s. 111 og 112

Bestemmelsens uklarhet i henhold til anvendelsesområde er en svakhet som gjør det vanskelig å konkludere i dette tilfellet. Dette er imidlertid ikke ukjent på dette området hvor flere av bestemmelsene er vage av hensyn til stadige endringer og behov for fleksibilitet. Dersom det legges til grunn at bestemmelsen også kommer til anvendelse i ansettelsesprosessen vil virksomheten kunne nedfelle det i ansettelseskontrakten og derav kunne kreve at politiattest fremlegges i ansettelsesprosessen. Dette tilfellet bærer imidlertid preg av såpass mye tvil at det er vanskelig å lande på en konkret konklusjon.

Det konkluderes derfor, under tvil og gitt at bestemmelsen kommer til anvendelse i ansettelsesprosessen, med at arbeidsgiver kan hjemle innsyn i politiattest i ansettelsesprosessen med at det er ”nødvendig for å gjennomføre sine arbeidsrettslige plikter eller rettigheter” i henhold til poppl. § 9, første ledd, bokstav f).

4.6 Oppsummering

Redegjørelsen og drøftelsen av de aktuelle hjemmelsgrunnlagene i tilknytning til problemstillingen, viser at det foreligger mange vanskelige og utfordrende vurderinger knyttet til hvilket grunnlag som kommer til anvendelse. Dette er begrunnet i at personopplysningsloven er utpreget vag på flere av de aktuelle områdene. Det er imidlertid slått fast at det ikke foreligger en klar hjemmel i lov som gir private virksomheter rett til utstedelse av politiattest i ansettelsesprosessen jf. politiregisterloven med tilhørende forskrift. Samtykke kan i utgangspunktet anvendes som hjemmelsgrunnlag, men det er flere hindre knyttet til dette gitt konteksten samtykket skal avgis i. Bestemmelsen i poppl. § 9, første ledd bokstav f) har et uklart anvendelsesområde og det kan derfor ikke med sikkerhet slås fast at dette kan benyttes som hjemmelsgrunnlag. Systemhensyn taler også mot en utvidende fortolkning av bestemmelsen.

5. EUs personvernforordning – ikrafttredelse 25.mai 2018

5.1 Bakgrunn og formål

EU- kommisjonen og EU- parlamentet kom i desember 2015 til enighet om nye personvernregler. Det nye regelverket gjennomføres som en forordning i mai 2018. I kraft av at det er en forordning med et formål om rettsenhet i medlemsstatene, er det lite rom for nasjonale tilpasninger¹²². Forordningen vil by på mange endringer, og dette vil bli merkbart i form av at en god del av dagens lovgiving i form av lov eller forskrift kan tenkes å falle bort. Det er fremdeles mye som er usikkert, og ytterligere avklaringer er forventet når Justisdepartementet og beredskapsdepartementet sender ut et høringsnotat som er forventet å komme i løpet av sommeren 2017¹²³. Det er allikevel relevant for problemstillingen å ta for seg noen av virkningene forordningen etter all sannsynlighet vil ha for næringslivet.

5.2 Virkninger for næringslivet

5.2.1 Artikkel 88

Forordningens artikkel 88 omhandler behandling av personopplysninger i forbindelse med ansettelsesforhold. Etter art. 88, nr.1 fremgår det at ”Medlemsstaterne kan ved lov eller i medfør av kollektive overenskomster fastsette mer spesifikke bestemmelser for at sikre beskyttelse av rettighederne og firhesrettighederne (...), navnlig med henblik på ansættelse(...)”. I nr. 2 kommer det videre frem at ”Disse bestemmelser skal omfatte passende og specifikke foranstaltninger til beskyttelse af den registreredes menneskelige værdighed, legitime interesser og grundlæggende rettigheder(...)”¹²⁴.

Artikkel 88 viser at området for behandling av personopplysninger i ansettelsesforhold er et av områdene hvor det er rom for nasjonale tilpasninger i det nye regelverket. Dette innebærer at det er knyttet større usikkerhet til hvilke regler som kommer til anvendelse på arbeidsrettens område i tilknytning til personopplysninger og behandlingen av disse i et ansettelsesforhold.

¹²² Øystein Flagstad, Carsten L Mowinckel og Inger-Anne Folkestad Tornes, ”Nytt personvernregelverk fra EU” LoD-2015-122-24

¹²³ www.regjeringen.no ”Personvernforordning” EØS-notat

¹²⁴ EP/Rf (EU) 2016/679 27.april 2016 (dansk utgave)

5.2.2 Fremtiden til personopplysningsforskriften – melde og konsesjonsplikt

Etter TFEU art.288 fremgår det at et direktiv er bindende for alle land som det retter seg mot sett i sammenheng med resultatet direktivet vil oppnå, men at det er de nasjonale myndighetenes oppgave å bestemme form og tilnærming for gjennomføringen¹²⁵. Da ny lovgivning skulle erstatte den gamle personregisterloven¹²⁶, skjedde dette i form av personopplysningsloven med den tilhørende personopplysningsforskriften. Lovgiver valgte altså å legge visse særreguleringer til forskriften, blant annet unntaket fra konsesjonsplikt i pof. § 7-16 som er tidligere drøftet i oppgaven.

Fremtiden til personopplysningsforskriften er imidlertid usikker med tanke på at en forordning stiller krav til at lovgivningen skal gjennomføres likt i alle EU/EØS medlemsstater¹²⁷. Rommet for nasjonale tilpasninger forsvinner derfor, og dette innebærer at forskriften også etter all sannsynlighet ikke videreføres.

Dette kan imidlertid avhjelpest ved at dagens melde- og konsesjonsplikt i hovedsak ikke videreføres¹²⁸. Etter forordningens art. 35 legges det større vekt på at virksomheten foretar en konsekvensanalyse forut for behandlingen av personopplysninger i form av risikovurdering og dokumentasjonsplikt¹²⁹. Dersom konsekvensanalysen avdekker høy personvernrisiko i forbindelse med behandlingen, skal de konsultere og rådføre seg med tilsynsmyndighetene¹³⁰. Bestemmelsens siktemål er etter all sannsynlighet å lette arbeidsbyrden til tilsynsorganene, og samtidig bidra til en mindre byråkratisk og mer smidig behandling av personopplysninger.

I arbeidslivet kan det imidlertid tenkes at det på noen områder vil foreligge et behov for å opprettholde en konsesjonsplikt, eller en utvidet tilsynsplikt. Det siktes her til arbeidsgivers adgang til å kameraovervåking, kredittopplysningsvirksomhet og lignende inngripende behandlinger av personopplysninger. Hvordan dette vil bli løst uten at det foreligger en eksplisitt konsesjonsplikt i forordningen, gjenstår å se når høringsnotatet blir offentlig og når forordningen trer i kraft i 2018.

¹²⁵ TFEU art. 288, 3.linje (oversatt fra engelsk)

¹²⁶ Opphevet da den nye personopplysningsloven trådte i kraft 1.januar 2001

¹²⁷ TFEU art. 288, 2.linje (oversatt fra engelsk)

¹²⁸ www.regjeringen.no ”Personvernforordning” EØS-notat

¹²⁹ www.regjeringen.no ”Personvernforordning” EØS-notat

¹³⁰ EP/Rf (EU) 2016/679 27.april 2016 art. 35 og 36

5.2.3 Skjerpet samtykkekrav

I de innledende betraktningene til forordningen omhandler nr. 42 og nr. 43 utgangspunktene for krav til samtykke. I nr. 42, siste setning fremgår det at ” Samtykke bør ikke anses for at være givet frivilligt, hvis den registrerede ikke har et reelt eller frit valg eller ikke kan avvise eller tilbaketrække sit samtykke, uden at det er til skade for den gågældende¹³¹”. Videre kommer det i nr. 43, 1.setning frem at ”Med henblik på at sikre, at der frivilligt er givet samtykke, bør samtykke ikke udgjøre et gyldigt retsgrundlag for behandling af personoplysninger i et specifikt tilfælde, hvis der er en klar skævhed mellem den registrerede og den dataansvarlige (...) ¹³²”. Punktene løfter frem og setter ord på situasjoner hvor gyldigheten av et samtykke kan være gjenstand for tvil, slik det også er fremhevet i drøftelsen om samtykke. Art. 7 fremhever i nr. 3 at det også skal være like lett å trekke tilbake sitt samtykke, som å gi det¹³³. De skjerpede kravene til samtykke i forordningen er relevant i den utstrekning at oppgaven har vist at samtykke er det grunnlaget arbeidsgiver i mange tilfeller faller ned på som hjemmel for behandling av personopplysninger i ansettelsesprosessen.

5.2.4 ”One- stop shop”

Forordningens kapittel VI omhandler uavhengige tilsynsmyndigheter. I Norge er dette som tidligere nevnt Datatilsynet. Etter art. 56 fremgår det at ”(...) (er) tilsynsmyndigheden for den dataansvarliges eller databehandlerens hovedvirksomhed eller eneste etablering kompetent til at fungere som ledende tilsynsmyndighed for den grænseoverskridende behandling(...) ¹³⁴”. Det er dette som betegnes som ”one stop shop”. Det opprettes en sentral europeisk tilsynsmyndighet, European Data Protection Board(EDPB), som skal bestå av representanter fra nasjonale tilsynsmyndigheter¹³⁵. Dette innebærer at dersom en virksomhet ønsker å behandle personopplysninger i flere land innenfor EU, trenger virksomheten i utgangspunktet bare å forholde seg til Datatilsynet i Norge da dette representerer det sentrale tilsynet i EU/EØS. Det vil med dette blir enklere for norske aktører i næringslivet å operere internasjonalt i EU/EØS med ett harmonisert regelsett å forholde seg til¹³⁶.

¹³¹ EP/Rf (EU) 2016/679 27.april 2016 nr. 42

¹³² EP/Rf (EU) 2016/679 27.april 2016 nr. 43

¹³³ EP/Rf (EU) 2016/679 27.april 2016 art.7, nr.3

¹³⁴ EP/Rf (EU) 2016/679 27.april 2016 art. 56, nr.1

¹³⁵ www.regjeringen.no ”Personvernforordning” EØS-notat

¹³⁶ www.regjeringen.no ”Personvernforordning” EØS-notat

6. Avslutning

Oppgaven har løftet frem problemstillinger knyttet til arbeidsgivers behov for behandling av sensitive personopplysninger i ansettelsesprosessen. I den forbindelse har det kommet frem at virksomheter i privat sektor kan ha et reelt og legitimt behov et forsvarlig ansettelsesgrunnlag hvor innsyn i politiattest er et element i ansettelsesprosessen. Dette ses i sammenheng med utviklingen av økonomisk kriminalitet i næringslivet, og virksomhetens økende behov for å minimere risiko ved ansettelse.

Fremstillingen har også belyst spørsmål om kandidatens personvern i ansettelsesprosessen. Innsyn i politiattest i ansettelsesprosessen kan oppleves som både inngripende og integritetskrekkende. Behandlingen av denne type opplysninger må derfor ha et legitimt formål for at det skal være forholdsmessig, og loven stiller strenge krav til hjemmel for behandling av denne type opplysninger.

Oppgaven har samtidig illustrert at en vag, uklar og til tider uoversiktlig personopplysningslov gjør løsning av problemstillingene utfordrende. Mangel på relevant praksis og muligheten til å utlede retningslinjer fra dette gjør at systemhensyn og formålsbetraktninger blir viktige tolkningsmomenter når det skal redegjøres for rettstilstanden. Dette genererer spørsmålet om en lovfestet adgang for private virksomheter til utstedelse av politiattest i ansettelsesprosessen vil være et godt alternativ som vil fremme forutberegnelighet for både arbeidsgiver og kandidat. Slik rettstilstanden er i dag er den uoversiktlig og byr på en kronglete sti i søken på hvilket hjemmelsgrunnlag som kommer til anvendelse. Samtidig må det vurderes i hvor stor utstrekning arbeidsgiver skal kunne kontrollere kandidatene som søker på en stilling, og om lovgiver skal gi etter for dette kontrollbehovet. Jakten på den ”ufeilbarlige” arbeidstaker kan utlede i usunne tendenser i arbeidsmarkedet og forhindre at godt kvalifiserte kandidater velger å ikke søke fordi de vet at det innebærer blottstillelse overfor arbeidsgiver i ansettelsesprosessen.

Det er en spennende tid i vente i forbindelse med personvernforordningens ikrafttredelse i 2018. Slik det norske personvernregelverket fremstår i dag, vil forordningen kunne bidra til en klarere og mer oversiktlig fremstilling av reglene på området for personvern. Den vil også kunne legge bedre til rette for utvikling av bransjepraksis og retningslinjer i forbindelse med næringslivets behandling av personopplysninger i alle EU/EØS landene. Dette vil forhåpentligvis veie opp for de ressursene som vil kreves for å implementere nye personvernrutiner i virksomheten.

7. Kildeliste

Lover og traktater

Personopplysningsloven	Lov om behandling av personopplysninger 14.april 2000 nr. 31
Politiregisterloven	Lov om behandling av opplysninger i politiet og påtalemyndigheten 28.mai 2010 nr. 16
Arbeidsmiljøloven	Lov om arbeidsmiljø, arbeidstid og stillingsvern mv. 17.juni 2005 nr. 62
Regnskapsloven	Lov om årsregnskap mv. 17.juli 1998 nr. 56
Tjenestemannsloven	Lov om statens tjenestemenn m.m. 4.mars 1983 nr. 3
Consolidated version of the treaty of the functioning of the European Union (TFEU) OJ C 326 26/10/2012	

Forskrifter

Personopplysningsforskriften	Forskrift om behandling av personopplysninger (personopplysningsforskriften) 15.desember 2000 nr. 1265
Politiregisterforskriften	Forskrift om behandling av opplysninger i politiet og påtalemyndigheten (politiregisterforskriften) 20.september 2013 nr. 1097

Forarbeider

NOU 1997:19	Et bedre personvern
NOU 2009:1	Individ og integritet: Personvern i det digitale samfunn
Ot.prp.nr.92 (1998-1999)	Om lov om behandling av personopplysninger (personopplysningsloven)
Ot.prp.nr.108 (2008-2009)	Om lov om behandling av opplysninger i politiet og påtalemyndigheten (politiregisterloven)
Prop. 94 L (2016-2017)	Lov om statens ansatte mv. (statsansattloven)

Underrettsdommer

TOSLO-2012-47498	Dom fra Oslo Tingrett avsagt 28.mars 2012 nr. 47498
------------------	---

Vedtakspraksis fra Personvernemnda

PVN-2015-06 Vedtak fra Personvernemnda 8. desember 2015 nr. 6

PVN-2004-1 Vedtak fra Personvernemnda 19. august 2004 nr. 1

Rettspraksis fra EU-domstolen

Sak C131/12 Domstolens dom (stor avdeling) 13. mai 2014 – Google Spain SL og Google Inc. mot Agencia de Proteccion de Datos (AEPD) og Mario Costeja Gonzalez

Forordninger

Europaparlamentets- og Rådets forordning (EU) 2016/679 27. april 2016 om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av sådanne opplysninger og om opphevelse av direktiv 95/46/EF (generel forordning om databeskyttelse) (dansk utgave)

Direktiver

Europaparlamentets- og Rådetsdirektiv 95/46/EF 24. oktober 1995 om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger.

Bøker

Schartum, Dag Wiese og Bygrave, Lee A., *Personvern i informasjonsfunnet- en innføring i vern av personopplysninger*, 3. utgave (Bergen 2016)

Blume, Peter, *Databeskyttelsesret*, 3. utgave (København 2008)

Artikler

Bing, Jon, ”Samtykke til behandling av personopplysninger i arbeidsforhold” i *Arbeid og rett: Festskrift til Henning Jakhellns 70-års dag 2009* s. 45-64, Cappelen Akademiske forlag

Flagstad, Øystein, Mowinckel, Carsten L. og Folkestad Tornes, Inger-Anne, ”Nytt personvernregelverk fra EU”, *LoD- 2015-122-24* (Lovdata 2015)

Andre kilder

ØKOKRIM Trendrapport/ Trusselvurdering 2015/2016 (sist sjekket 31.5.17):
[http://www.okokrim.no/www/okokrim/resource.nsf/files/207516847-trusselvurdering_okokrim_15-16/\\$FILE/trusselvurdering_okokrim_15-16.pdf](http://www.okokrim.no/www/okokrim/resource.nsf/files/207516847-trusselvurdering_okokrim_15-16/$FILE/trusselvurdering_okokrim_15-16.pdf)

Dagens Næringsliv, ”Så mye koster en feilansettelse” , publisert 22.12.2009, oppdatert 7.2.2014 (sist sjekket 31.5.17):

<http://www.dn.no/karriere/2009/12/22/sa-mye-koster-en-feilansettelse>

www.regjeringen.no , ”Personvernforordning” EØS-notat publisert 24.3.2017 (sist sjekket 31.5.17):

<https://www.regjeringen.no/no/sub/eos-notatbasen/notatene/2014/avg/forslag-til-personvernforordning/id2433856/>

Transportøkonomisk institutt; Setter vår lit til storebror, og alle småbrødre med, rapport nr. 789 2005 (sist sjekket 31.5.17):

<https://www.toi.no/getfile.php?mmfileid=913>

Kriminalitets og sikkerhetsundersøkelsen i Norge (KRISINO), presentert 23. og 24.september 2015 (sist sjekket 31.5.17):

https://www.nsr-org.no/getfile.php/Dokumenter/NSR%20publikasjoner/Krisino/krisino_2015_utskrift.pdf

Om OECD og retningslinjer fra OECD (sist sjekket 31.5.17):

<http://www.oecd.org/about/>

<http://www.oecd.org/daf/inv/mne/48004323.pdf>

Stor norske leksikon om OECD (sist sjekket 31.5.17):

<https://snl.no/OECD>

ØKOKRIMs årsrapport 2013, Jubileumshilsen ved Erik Keiserud (leder i avdokatforeningen) (sist sjekket 31.5.17):

http://www.hvitvasking.no/globalassets/okokrim_arsrapport_2013_norsk.pdf

Om Datatilsynets oppgaver og hvordan man søker konsesjon (sist sjekket 31.5.17):

<https://www.datatilsynet.no/Om-Datatilsynet/Oppgaver/>

<https://www.datatilsynet.no/personvern/Melding-og-konsesjon/soke-konsesjon/>