Utredning av personvernkonsekvenser: Lovhjemmel for behandling av personopplysninger i Samordna opptak og studieadministrative systemer

Bestilling fra departementet

Det vises til departementets e-post av 06.06.2017 hvor CERES ble bedt om å vurdere de personvernmessige konsekvensene av behandling av personopplysninger i hhv. Samordna opptak og studieadministrative systemer.

Presiseringer

Etter departementets ønske er konsekvensutredningen skrevet i henhold til den malen som fremgår av veileder til utredningsinstruksen «Vurdering av personvernkonsekvenser». Veilederen er utarbeidet av KMD (tidligere Fornyings- og administrasjonsdepartementet).

I den videre fremstillingen brukes begrepet «den registrerte» om de søkere og studenter personopplysningene er knyttet til. I de tilfeller det henvises til både søkere og studenter, omfatter dette også doktorgradskandidater.

De deler av fremstillingen som omtaler institusjonens rolle og plikter når det gjelder behandling av personopplysninger om «søkere», gjelder også Kunnskapsdepartementet ved behandling av personopplysninger i Samordna opptak. Dette fordi departementet er behandlingsansvarlig for personopplysninger om søkere som blir behandlet i opptakssystemet til Samordna opptak.

A. Kartleggingsfasen

1. Innebærer tiltaket behandling av personopplysninger?

Forslaget om lovhjemmel regulerer behandling av personopplysninger om søkere, studenter og doktorgradskandidater. Dette er behandling av personopplysninger som institusjonene utfører i forbindelse med opptak og studieadministrasjon.

Lovforslaget går ut på at det rettslige grunnlaget for behandlingen av personopplysninger (behandlingsgrunnlaget) i opptaks- og studieadministrative systemer følger direkte av en lovhjemmel i universitets- og høyskoleloven. Både offentlige og private utdanningsinstitusjoner er omfattet av virkeområdet til universitets- og høyskoleloven, jf. uhl. § 1-2.

Det er foreslått én lovhjemmel for «Samordna opptak», og en egen lovhjemmel for institusjonenes studieadministrative systemer. Per i dag bruker de fleste utdanningsinstitusjonene det studieadministrative systemet «Felles studentsystem».

I Samordna opptak behandles det kun personopplysninger om søkere til høyere utdanning, mens det i studieadministrative systemer (som f.eks. Felles studentsystem) behandles personopplysninger om både søkere, studenter og doktorgradskandidater.

2. Hvilke endringer innebærer tiltaket i forhold til nåværende situasjon?

Rettslig grunnlag for behandling av personopplysninger

Personopplysninger om hhv. søkere, studenter og doktorgradskandidater blir også i dag behandlet elektronisk både i Samordna opptak og institusjonenes studieadministrative systemer.

Behandlingen i Samordna opptak hjemles per i dag i personopplysningsloven § 8 bokstav e, idet behandlingen er nødvendig for å utøve offentlig myndighet. Det vil si treffe enkeltvedtak som er bestemmende for rettighetene eller pliktene til den som har søkt om opptak til høyere utdanning.

I studieadministrative systemer skjer det også per i dag en elektronisk behandling av personopplysningene til søkere og studenter. Behandlingen hjemles i personopplysningsloven § 8. Det rettslige grunnlaget er mer sammensatt når det gjelder behandling i studieadministrative systemer. De fleste behandlinger er nødvendige for å utøve offentlig myndighet, det vil si treffe enkeltvedtak og avgjørelser som er bestemmende for rettighetene eller pliktene til den enkelte søker, student eller doktorgradskandidat. Andre behandlinger er nødvendige for å oppfylle en avtale med den enkelte søker, student eller doktorgradskandidat. Noen behandlinger hjemles også i et samtykke fra den enkelte personen, f.eks. innhentes det samtykke ved bruk av personbilder i Fagpersonweb.

Med utgangspunkt i det forslaget til lovbestemmelser som er foreslått, vil endringen gå ut på at det rettslige grunnlaget for behandling av personopplysningene til søkere, studenter og doktorgradskandidater vil følge direkte av universitets- og høyskoleloven.
Endringen vil også innebære at det tillates elektronisk behandling av opplysninger om helse og sosiale forhold. Opplysninger om helse er alltid å anse som sensitive og taushetsbelagte opplysninger, mens opplysninger om sosiale forhold i stor grad er taushetsbelagte.

Digitale politiattester

Det er også foreslått lovhjemmel for at utdanningsinstitusjoner som tilbyr utdanninger hvor det stilles krav om politiattest, kan behandle politiattestene til studentene elektronisk.

Etter gjeldende personopplysningslov vil politiattester med merknader inneholde sensitive personopplysninger, jf. pol. § 2 nr. 8 bokstav b, og derfor må ett av tilleggsvilkårene i pol. § 9 være oppfylt. Denne definisjonen blir ikke videreført i den nye personvernforordningen(GDPR), men forordningen vil stille krav om lovhjemmel for behandling av opplysninger om straff og lovovertredelser, jf. GDPR art. 10.

Forslaget om lovhjemmel for elektronisk behandling av politiattester er begrunnet i at det er nødvendig å innføre en elektronisk løsning for innlevering av politiattester til institusjonen, fordi politiet har begynt å utstede digitale politiattester (signerte PDF-filer) til de studentene som har digital postkasse. For å sikre at de politiattestene som blir levert til utdanningsinstitusjonen er autentiske, er det derfor nødvendig å åpne for at digitalt utstedte attester kan leveres elektronisk til institusjonene.

Per i dag leverer alle studenter politiattester på papir til utdanningsinstitusjonen. Studenter som får tilsendt digital politiattest til sin digitale postkasse må skrive den ut på papir, og levere den til institusjonen. Det er relativt enkelt å manipulere en slik papirutskrift, og det oppstår dermed en fare for dokumentfalsk. Hverken utdanningsinstitusjonene eller politiet har i dag kapasitet til å utføre en manuell verifisering av politiattesten etter at den er levert til institusjonen. Det er likevel viktig at det innføres tiltak for å påse at den innleverte politiattesten er autentisk, og ikke er blitt endret på.

Det minnes om at ordningen med kontroll av politiattester på enkelte utdanninger er nødvendig for å beskytte sårbare grupper (mindreårige) som studentene kommer i kontakt med under praksis på utdanningen, jf. universitets- og høyskoleloven § 4-9. Dagens situasjon innebærer en risiko for at hensynet til sårbare grupper ikke blir godt nok ivaretatt. Siden utdanningsinstitusjonene ikke har en lovhjemmel for elektronisk behandling av politiattester på plass, har de ikke mulighet til å be studentene om å levere attestene elektronisk, og derfor kan de heller ikke være sikre på at den digitale politiattesten blir levert i sin autentiske form.

Når det gjelder politiattester er det ikke tilstrekkelig at kravet om politiattest følger av universitets- og høyskoleloven § 4-9, eller at det forutsetningsvis følger av uhl. § 4-9 at institusjonene bør kunne ta imot politiattester elektronisk. For at behandlingen skal være lovlig, må det fremgå eksplisitt av loven at institusjonene kan behandle slike politiattester elektronisk.

Automatisert saksbehandling

Videre innebærer lovforslaget at muligheten for automatisert saksbehandling i Samordna opptak og studieadministrative systemer hjemles i lov. Det siktes da til tilfeller hvor institusjonene ved hjelp av automatisert saksbehandling fatter enkeltvedtak og avgjørelser som er bestemmende for rettighetene eller pliktene til en søker eller student.

Automatisert saksbehandling innebærer at et datasystem fatter beslutninger som er avgjørende for rettighetene og pliktene til en enkeltperson. Ved automatisert saksbehandling er rettsreglene blitt formalisert og programmert i datasystemet. Rettsanvendelsen skjer altså gjennom datasystemet.

Automatisert saksbehandling kan bidra til å sikre den enkeltes rettssikkerhet på en bedre måte, siden automatisert saksbehandling bidrar til effektivitet, kvalitet og likebehandling i saksbehandlingen. Slik kan automatisert saksbehandling på en bedre måte ivareta rettsikkerheten til den person avgjørelsen eller enkeltvedtaket retter seg mot, sammenlignet med manuell saksbehandling.

Som et eksempel på automatisert saksbehandling i opptakssystemet til Samordna kan det nevnes automatisk beregning av poengsum av elektroniske vitnemål. Når det gjelder studieadministrative systemer, kan det nevnes at innvilgelse av eksamens- og undervisningsmeldinger foregår etter automatisert saksbehandling (gjennom FS-applikasjonen Studentweb).

Det blir også i dag fattet enkeltvedtak og avgjørelser etter automatisert saksbehandling i Samordna opptak og Felles studentsystem, men dette er ikke alltid like synlig for den enkelte søker, student eller kandidat. Ved å hjemle muligheten til automatisert saksbehandling i universitets- og høyskolesektoren vil det skape forutsigbarhet for både søkere, studenter, kandidater og allmennheten for øvrig. Det vil bli mer synlig at automatisert saksbehandling foregår i universitets- og høyskolesektoren, og det kan også legges føringer på i hvilke tilfeller automatisert saksbehandling kan og bør anvendes.

Forvaltningslovens regler om saksbehandling vil alltid gjelde i tilfeller hvor det fattes vedtak ved bruk av automatisert saksbehandling. Den enkelte personen som vedtaket retter seg mot vil derfor ha rettigheter både som «den registrerte» etter personvernregelverket, og «part» etter forvaltningslovens. F.eks. vil kravene om veiledning, utredning, begrunnelse og klagerett i forvaltningsloven gjelde også ved automatisert saksbehandling.

Den kommende personvernforordningen som trer i kraft i mai 2018, vil gi den registrerte personen rett til å motsette seg automatisert saksbehandling, med mindre behandlingsgrunnlaget følger av en konkret lovhjemmel som ivaretar rettighetene og

interessene til den registrerte, jf. GDPR art. 22. For å sikre en effektiv ressursbruk og kvalitet i saksbehandlingen, er det ikke ønskelig at den registrerte uten videre kan motsette seg automatisert saksbehandling.

For å ivareta rettighetene og interessen til den registrerte foreslås det derfor at den personen avgjørelsen eller vedtaket retter seg mot skal kunne kreve at avgjørelsen eller vedtaket blir overprøvd manuelt. Gjeldende personopplysningslov har en lignende bestemmelse i § 25 (Rett til å kreve manuell behandling). En rett til manuell overprøving, som supplerer den alminnelige klageretten etter forvaltningsloven, vil tilstrekkelig ivareta rettighetene og interessene til den registrerte, selv om den registrerte ikke kan motsette seg automatisert saksbehandling. Alternativt kan det vurderes om den alminnelige klageretten som følger av forvaltningsloven, som vil innebære at vedtaket vil bli overprøvd av en klageinstans, er tilstrekkelig for å ivareta rettighetene til den registrerte. I så fall er det nødvendig å presisere at det overprøvingen må utføres manuelt av en fysisk person i klageprosessen. Klageinstansen kan ikke automatisk legge til grunn at systemet har fattet et riktig vedtak.

Mulighet for manuell overprøving av vedtak fattet ved automatisert saksbehandling, er å foretrekke fremfor situasjoner hvor alle personopplysningene må bli behandlet manuelt under hele saksprosessen.

3. Hvilke typer personopplysninger skal behandles

Ordinære personopplysninger

Opplysninger om navn, adresse, telefonnummer, e-post og fødsels- og personnummer er i utgangspunktet å anse som ordinære eller åpne personopplysninger. Disse opplysningene er ikke å anse som sensitive etter personopplysningsloven. I utgangspunktet er de heller ikke taushetsbelagte etter fvl. § 13 første ledd nr. 1, men unntak kan forekomme. For enkelte personer kan opplysninger om adresse og telefonnummer være taushetsbelagte etter fvl. § 13 første ledd nr. 1. F.eks. hvis noen personer har et beskyttelsesbehov, eller har en adresse som kan avsløre taushetsbelagte opplysninger om personen. Adressen kan for eksempel tilhøre et fengsel eller en psykiatrisk institusjon.

Utgangspunktet er at opplysninger om bestått utdanning, herunder avlagte eksamener og prøver, gjennomførte kurs, oppnådde grader, ikke er taushetsbelagte opplysninger. For karakterer kan saken stille seg annerledes, og her skilles det også mellom karakterer fra grunnskolen/videregående opplæring og karakterer fra høyere utdanning. Se omtale av dette under hhv. «Taushetsbelagte personopplysninger» og «Andre beskyttelsesverdige personopplysninger».

Taushetsbelagte personopplysninger

Ved opptak til høyere utdanning vurderes generell studiekompetanse med bakgrunn i vitnemål og kompetansebevis fra videregående opplæring. Karakterer fra videregående opplæring er å anse som taushetsbelagte opplysninger etter fvl. § 13 første ledd nr. 1. Karakterer fra grunnskolen er også taushetsbelagte, men det er sjelden nødvendig å fremlegge dokumentasjon på grunnskole ved opptak til høyere utdanning.

Opplysninger om orden og fravær på vitnemål er også å anse som taushetsbelagte opplysninger. Elektroniske vitnemål i Nasjonal vitnemålsdatabase inneholder ikke opplysninger om orden og fravær, men i de tilfeller hvor en søker legger frem kopi av sitt papirvitnemål, vil dokumentasjonen også inneholde opplysninger om orden og fravær.

Ved vurdering av generell studiekompetanse etter 23/5 regelen eller realkompetanse, kan det være nødvendig for en søker å dokumentere arbeidspraksis. Det er også utdanninger som har arbeidspraksis som et spesielt opptakskrav. Erfaring viser at mange søkere

dokumenterer dette ved å sende inn arbeidsattester som også inneholder opplysninger om deres personlige egenskaper. Opplysninger om personlige egenskaper er å anse som opplysninger om «noens personlige forhold», og er derfor taushetsbelagte etter fvl. § 13 første ledd nr. 1.

Fullført militærtjeneste kvalifiserer til to tilleggspoeng ved opptak til høyere utdanning. Enkelte søkere fremlegger også dokumentasjon på militærtjeneste for å dokumentere arbeidspraksis i forbindelse med opptak. Tjenesteuttalelser kan inneholde taushetsbelagte opplysninger etter fvl. § 13 første ledd nr. 1. For eksempel kan de inneholde opplysninger om søkerens personlige egenskaper..

Opplysninger om helse og sosiale forhold er taushetsbelagte opplysninger etter fvl. § 13 første ledd nr. 1.

Opplysninger om sosiale forhold kan være opplysninger om personens familie, økonomi og livssituasjon, og kan også omfatte dokumentasjon fra NAV og PPT-tjenesten. Opplysninger om sosiale forhold blir oppfattet som beskyttelsesverdige av folk flest, og av personvernhensyn bør de behandles på samme måte som sensitive opplysninger.

Sensitive personopplysninger

Opplysninger om helse er å anse som sensitive personopplysninger, jf. pol. § 2 nr. 8 bokstav c. I den nye forordningen er helseopplysninger definert som «special category of personal data», jf. GDPR art. 9. Dette kan være opplysninger om sykdom, funksjonshemming, lyte, uførhet, nedsatt arbeidsevne o.l. Dokumentasjon som kan inneholde opplysninger om helse er f.eks. legeattester, dokumentasjon fra NAV eller PPT-tjenesten, og også egenerklæringer fra den enkelte personen.

Opplysninger om merknader på politiattesten til en student er etter dagens personopplysningslov sensitive personopplysninger, jf. pol. § 2 bokstav. Etter den nye personvernforordningen (GDPR) vil det stilles det krav om lovhjemmel for behandling av opplysninger om straff og lovovertredelser, jf. GDPR art. 10.

Andre beskyttelsesverdige personopplysninger

Fødsels- og personnummer er ikke en sensitiv personopplysning, og er heller ikke taushetsbelagt etter fvl. § 13 første ledd nr. 1. Dette er likevel en opplysning som folk flest anser som beskyttelsesverdig, og skal derfor kun brukes der det er nødvendig for å oppnå sikker identifisering. Søkernummer og studentnummer kan også bli oppfattet som beskyttelsesverdige opplysninger. Ved konkrete innsynsbegjæringer «kan» disse opplysningene unntas med hjemmel i offl. § 26 femte ledd.

Vitnemål og karakterer fra *høyere utdanning* er ikke taushetsbelagte etter fvl. § 13 første ledd nr.1. Folk flest vil trolig anse karakterer fra høyere utdanning som beskyttelsesverdige personopplysninger. Ved konkrete innsynsbegjæringer «kan» karakterer fra høyere utdanning unntas med hjemmel i offl. § 26 første ledd.

Enkeltvedtak og avgjørelser

De opplysningene det er redegjort for ovenfor er personopplysninger som kan inngå i beslutningsgrunnlaget til en avgjørelse eller enkeltvedtak. De avgjørelsene og enkeltvedtak som institusjonene fatter er å anse som «nye» personopplysninger om en søker, student eller kandidat. I hvilken grad disse opplysningene er sensitive, taushetsbelagte eller åpne (ikke beskyttelsesverdige) må vurderes konkret.

For eksempel kan et vedtak om generell studiekompetanse være en «åpen personopplysning». En avgjørelse om innvilgelse av permisjonssøknad på grunn av familiære årsaker vil som regel være taushetsbelagt etter fvl. § 13 første ledd nr. 1.

Et vedtak om tilrettelegging på eksamen grunnet sykdom vil være en «sensitiv personopplysning».

4. Hvis tiltaket ikke direkte omfatter ny behandling av personopplysninger, har det likevel personvernkonsekvenser?

Dette punktet er ikke aktuelt siden endringene vil innebære ny elektronisk behandling av sensitive personopplysninger og behandling av flere taushetsbelagte opplysninger enn tidligere: Opplysninger om helse og sosiale forhold, og politiattester.

5. Hvem, herunder hvor mange, blir berørt av tiltaket?

Personer som søker om opptak til høyere utdanning, eller er studenter eller doktorgradskandidater ved utdanningsinstitusjoner som er omfattet av universitets- og høyskoleloven, vil bli berørt av endringene. Under gis det en oversikt over omfanget på antall berørte personer, med utgangspunkt i tall fra 2016.

Antall aktive studenter i Felles studentsystem

I Felles studentsystem, som er det mest brukt studieadministrative systemet i universitets- og høyskolesektoren i dag, var det høsten 2016 registrert ca. 250 000 aktive studenter. Dette utgjør ca. 92 prosent av alle studenter i Norge. Felles studentsystem er i bruk ved alle statlige universiteter og høyskoler i dag, og også ved mange av de private utdanningsinstitusjonene. Systemet er ikke i bruk ved Handelshøyskolen BI.

Antall søkere ved lokale opptak til institusjonene

I 2016 fikk 103 000 søkere *tilbud* om opptak gjennom lokalt opptak i Felles student system, mens 114 000 søkere fikk *tilbud* om opptak gjennom Samordna opptak (Den nasjonale opptaksmodellen/NOM-opptak).

I statistikk om søknadstall i DBH er det ikke skilt på om det er søkere fra lokalt opptak eller Samordna opptak. De fleste som tas opp til grunnutdanninger tas opp gjennom Samordna opptak. Enkelte høyskoler har inntak til grunnutdanninger to ganger i året, og tar opp søkere gjennom Samordna opptak for studier med oppstart på høsten, men gjennomfører lokalt opptak for studier med oppstart på våren.

Antall søkere ved Samordna opptak (NOM)

I det samordnede opptaket til høyere grunnutdanning som ble gjennomført i 2016, ble det registrert 132 021 *søkere* (registrerte søknader).

Antall søkere som ble tatt opp til utdanninger med krav om politiattest (gjennom Samordna opptak)

I 2016 var det registrert 360 utdanninger som hadde krav om politiattest. 32 613 personer som søkte minst én av disse utdanningene fikk tilbud om studieplass, og av disse var det 20 426 personer som møtte opp.

Antall søkere og studenter som fremla opplysninger om helse

Når det gjelder tall på antall søkere eller studenter som fremla dokumentasjon med opplysninger om helse (på papir) i 2016, er det vanskelig å anslå eksakte tall på dette. Dette fordi det ikke blir registrert eller behandlet sensitive opplysninger i dagens systemer, hverken i Samordna opptak eller Felles studentsystem.

Når det gjelder antall studenter som søker om tilrettelegging på studiestedet i forbindelse med undervisning, eksamen o.l., blir dette ikke registrert i Felles studentsystem i dag.

Årsaken er at slik tilrettelegging ofte skyldes sykdom, funksjonshemming eller lignende, og dette er sensitive personopplysninger.

Det registreres kun behov for *konkret* tilrettelegging i Felles studentsystem. Hvis det er ønskelig fra departementets side og utdanningsinstitusjonene samtykker, kan det være mulig for CERES å hente tall på antall studenter med registrert person- eller eksamenstilpasning.

Når det gjelder Samordna opptak kan man få en viss pekepinn ved å ta utgangspunkt i antall søkere som søkte om hhv. betinget opptak og særskilt vurdering, jf. forskrift om opptak til høgre utdanning (opptaksforskriften) § 5-1 og § 7-13. Både dokumentasjon på helse og andre sosiale forhold er aktuelt ved vurdering av søknader etter disse bestemmelsene. I 2016 søkte 1187 personer om særskilt vurdering. I tillegg var det 516 personer som krysset av for særskilt vurdering i søknaden, men valget ble annullert på grunn av manglende grunnlag. Når det gjelder betinget opptak iht. opptaksforskriften § 5-1, møtte 75 personer opp til utdanninger hvor de fikk et betinget opptak.

6. Planlagt bruk (formål), risiko for misbruk

Lovforslaget innebærer at formålet med behandlingen av personopplysninger i Samordna opptak og studieadministrative vil gå direkte frem av universitets- og høyskoleloven.

Formålet med behandlingen i Samordna opptak er å behandle søknader om opptak til høyere utdanning i et nasjonalt og samordnet opptak. Formålet med behandlingen i studieadministrative systemer er å ivareta rettighetene til en søker, student eller doktorgradskandidat, eller oppfylle institusjonenes oppgaver og plikter etter universitets- og høyskoleloven, herunder opptak til høyere utdanning.

At formålet defineres i universitets og høyskoleloven vil bidra til bedre forutberegnelighet for de registrerte personene, og også bidra til lik praksis i sektoren. I dag er den enkelte utdanningsinstitusjon selv ansvarlig for å definere formålet med behandling av personopplysninger i studieadministrative systemer. Dagens praksis innebærer at institusjonene i dag kan ha ulike vurderinger av hvilken nødvendig grunn i pol. § 8 behandlingen skal hjemles i, og det er også varierende i hvilken grad institusjonene informerer de registrerte om hva som er formålet med behandlingen.

Lovforslaget innebærer at institusjonene kan innhente nødvendige personopplysninger elektronisk fra andre offentlige organer, når dette er nødvendig for å oppfylle det angitte formålet. Andre organer vil først og fremst være Folkeregisteret, Kontakt- og reservasjonsregisteret, andre utdanningsinstitusjoner og Nasjonal vitnemålsdatabase som inneholder elektroniske vitnemål fra videregående opplæring. Eksemplene er ikke uttømmende.

Hjemmelen for elektronisk innhenting av personopplysninger fra andre organer vil ikke gjelde for sensitive personopplysninger. Når det gjelder sensitive personopplysninger må det alltid fremgå eksplisitt av lovens ordlyd at behandlingen er tillatt. I lovforslaget er det ikke lagt opp til at sensitive personopplysninger skal kunne innhentes elektronisk fra andre organer uten at den registrerte aksepterer det. Lovbestemmelsen åpner kun for at visse sensitive personopplysninger kan behandles elektronisk, etter at den registrerte selv har lagt dem frem. I tilfeller hvor det er nødvendig å dokumentere helseopplysninger, er det altså søkeren eller studenten selv som er ansvarlig for å fremlegge dokumentasjon på dette. Lovhjemmelen vil tillate at søkeren kan levere slik dokumentasjon til institusjonen via en elektronisk løsning.

En tilsvarende løsning er også tenkt for digitale politiattester. Det vil si at politiet sender politiattesten til studenten, og studenten leverer den selv til utdanningsinstitusjonen. Dette sikrer også at studenten får muligheten til å kontrollere innholdet i politiattesten, før den legges frem for institusjonen. Hvis det i fremtiden tilbys en løsning gjennom Vitnemålsportalen, vil også den sikre at studenten først får se attesten og får mulighet til å kontrollere innholdet, før studenten aksepterer at den sendes videre til institusjonen.

Risikoen for evt. misbruk av personopplysninger må elimineres med tilfredsstillende informasjonssikkerhet og rutiner for internkontroll. Det må iverksettes sikkerhetstiltak som ivaretar hensynet til konfidensialitet, integritet og tilgjengelighet ved behandling av personopplysninger, f.eks. tilgangskontroller og kryptering. Institusjonene må foreta jevnlige risikovurderinger for å identifisere fare og sannsynlighet for evt. misbruk av personopplysninger, og det må iverksettes nødvendige tiltak for at risikoen skal være på et akseptabelt nivå. Både gjeldende personopplysningslov og den nye personvernforordningen har bestemmelser om ivaretakelse av informasjonssikkerhet og internkontroll. Dette er bestemmelser som behandlingsansvarlig er pliktig til å overholde. Det vises til personopplysningsloven § 13 og 14, og personvernforordringen art. 24, 25, 30, 32 og 35. Se også «Sikring av personopplysninger» under pkt. 14.

Konfidensialitet vil også bli ivaretatt gjennom bestemmelsene om taushetsplikt som følger av forvaltningsloven. Både offentlige og private utdanningsinstitusjoner som er omfattet av virkeområdet til universitets- og høyskoleloven, er pålagt lovbestemt taushetsplikt etter fvl. § 13 første ledd nr. 1 om noens personlige forhold, jf. universitets- og høyskoleloven § 7-6 første ledd.

Andre formål

Utgangspunktet er at personopplysningene ikke kan behandles til andre formål enn det de er hentet inn for. Dette fremgår av grunnkravene i pol. § 11. Tilsvarende begrensning vil også følge av den nye personvernforordningen, jf. personvernforordringen art. 5.

Offentlige myndigheter som kan dokumentere at de har rettslig grunnlag for å få utlevert personopplysninger om søkere, studenter og doktorgradskandidater vil likevel kunne få utlevert opplysningene. Behandlingsgrunnlag slike myndigheter kan påberope seg kan følge av både særlovgivningen eller personopplysningsloven direkte. For eksempel har Statistisk sentralbyrå og Lånekassen hjemmel i særlovgivningen, som tillater at de kan få utlevert personopplysninger, jf. statistikkloven og lov om utdanningsstøtte. Andre organer eller systemer som kan påberope seg rettslig grunnlag for utlevering av personopplysninger er f.eks. Norsk senter for forskningsdata (NSD), BIBSYS, Nasjonal database for godkjenning av utenlandske studier (GAUS) og Register for utestengte studenter (RUST).

På dette området må utdanningsinstitusjonene sørge for å etablere rutiner for gjennomgang av formålet og det rettslige grunnlaget behandlingen, før utlevering tillates til andre organer eller myndigheter.

Bruk av personopplysninger til historiske, statistiske og vitenskapelige formål blir normalt ansett som lovlige, men det må foretas en konkret vurdering av både formål og rettslig grunnlag i slike tilfeller. Etter gjeldende personopplysningslov må det dessuten gjøres en vurdering av om samfunnets interesse i at behandlingen finner sted, klart overstiger ulempene behandlingen kan medføre for den enkelte, jf. personopplysningsloven § 11 andre ledd. Tilsvarende bestemmelser er gitt i personvernforordringen, jf. art. 5 nr. 1 bokstav e. Her må det vurderes om slike formål kan oppfylles ved bruk av anonymisering, avidentifisering eller pseudonymisering av personopplysningene.

I det kommersielle markedet er det stor etterspørsel etter kontaktinformasjonen til privatpersoner, særlig studenter. Utdanningsinstitusjonene må etablere rutiner for å hindre at

det skjer en utlevering av personopplysninger til kommersielle aktører, som kan krenke personvernet til deres søkere, studenter eller doktorgradskandidater.

Institusjonene må også være oppmerksomme på at postadressen og telefonnummeret til en søker, student eller kandidat kan være omfattet av lovbestemt taushetsplikt etter fvl. § 13 første ledd nr. 1. Dette gjelder ikke dersom personen selv har gjort informasjonen offentlig tilgjengelig, f.eks. i offentlige tilgjengelig telefonkataloger, eller evt. samtykker til utlevering.

På dette området må det også tas i betraktning at kommersielle aktører kan fremme innsynsbegjæring i personopplysninger i medhold av bestemmelser i offentleglova. Dagens personvernregelverk er utformet slik at den ikke begrenser allmennhetens innsynsrett etter offentleglova, med mindre lovbestemt taushetsplikt er til hinder for dette eller en unntaksbestemmelse kan gjøres gjeldende. I universitets- og høyskolesektoren har det vært flere tilfeller hvor private aktører har bedt om personopplysninger, herunder kontaktinformasjonen til uteksaminerte studenter. I slike tilfeller har de ikke fått utlevert postadressen og telefonnumrene til disse personene, men det er blitt lagt til grunn at de kan få innsyn i navnelister over uteksaminerte studenter, siden opplysninger om bestått høyere utdanning og oppnådd grad ikke anses som taushetsbelagte opplysninger.

7. Rettslig grunnlag for behandlingen

Lovforslaget innebærer at det rettslige grunnlaget for behandling av personopplysninger vil følge direkte av en lovhjemmel i universitets- og høyskoleloven.
Gjeldende personopplysningslov krever at det rettslige grunnlaget for behandlingen (behandlingsgrunnlaget) enten er en lovhjemmel (i en særlov), samtykke fra den registrerte, eller en nødvendig grunn som angitt personopplysningsloven § 8 bokstav a til f. Ovenfor er det redegjort for hva som er gjeldende praksis når det gjelder rettslig grunnlag for behandling av personopplysninger i Samordna opptak og studieadministrative systemer, jf. pkt. 1. De fleste behandlingene hjemles i en eller flere av de nødvendige grunnene som fremgår av pol. § 8.

Den nye personvernforordningen angir også utøving av offentlig myndighet som en nødvendig grunn, som behandlingen av personopplysninger kan hjemles i, jf. personvernforordringen art. 6. personvernforordringen stiller samtidig krav til at grunnlaget for utøving av offentlig myndighet skal fremgå av medlemsstatens nasjonale rett.

Samtykke har tradisjonelt blitt ansett som det rettslige grunnlaget som best ivaretar den registrertes personvern. Det stilles imidlertid krav om at samtykke skal være avgitt ved en frivillig, uttrykkelig og informert erklæring fra den registrerte. Personvernnemnda har tidligere lagt til grunn at samtykke er hovedregelen når det gjelder rettslig grunnlag, men har senere gått bort fra dette. I dag anerkjenner Personvernnemnda samtlige rettslige grunnlag i personopplysningsloven § 8 som likestilte. Dette er også i tråd med det som følger av EU-retten.

Når offentlige myndigheter behandler personopplysninger vil det ikke sjelden være problematisk å oppfylle kravet om frivillighet i en samtykke-erklæring. Kravet om frivillighet innebærer at det ikke skal knytte seg noen negative sanksjoner til manglende samtykke. Hvis en student f.eks. ikke samtykker til innlevering av en politiattest, vil det knytte seg sanksjoner til manglende innlevering av attesten, idet studenten da ikke vil ha rett til å delta i praksisundervisningen, jf. forskrift om opptak til høgre utdanning, § 6-6.
Behandlingsgrunnlaget for offentlige myndigheters behandling av personopplysninger bør derfor følge av en lovhjemmel i særlovgivningen.

Når det gjelder behandling av sensitive personopplysninger etter gjeldende personopplysningslov, må ett av tilleggsvilkårene i § 9 være oppfylt. § 9 bokstav b sier at sensitive personopplysninger kan behandles dersom det er fastsatt i lov at det er adgang til slik behandling. Dersom en lovhjemmel for behandling av sensitive personopplysninger foreligger, vil dette tilleggsvilkåret være oppfylt, og det vil heller ikke være nødvendig å søke om konsesjon fra Datatilsynet. Det presiseres at det ikke er meningen at sensitive personopplysninger skal kunne innhentes fra andre organer, dette er opplysninger som skal innhentes direkte fra søkeren eller studenten.

Etter gjeldende personopplysninglov er opplysninger om helse og merknader på politiattest å anse som sensitive personopplysninger. Etter den nye personvernforordningen vil opplysninger om helse fortsatt være sensitive. Opplysninger om straff og lovovertredelser er ikke klassifisert som sensitive personopplysninger i personvernforordringen, men behandlingen av slike opplysninger må likevel være hjemlet i lov, jf. personvernforordringen art. 10.

Når den nye personvernforordningen trer i kraft, vil konsesjonsplikten (for sensitive opplysninger) erstattes av regler om utredning av personvernkonsekvenser og forhåndsdrøftelser med Datatilsynet, jf. personvernforordringen art. 35 og 36.

Det er ikke blitt utredet hvorvidt en lovhjemmel i universitets- og høyskoleloven som tillater behandling av sensitive personopplysninger, også vil være tilstrekkelig som behandlingsgrunnlag etter personvernforordringen art. 9. På dette punktet avventes det mer veiledning fra Datatilsynet, men trolig vil behandlingen kunne hjemles i art. 9 nr. 2 (bokstav g). Siden sensitive opplysninger om helse uansett skal innhentes fra søkeren, f.eks. via Søkerportalen, vil det ikke være problematisk å supplere lovhjemmelen med et samtykke eller en aksept fra søkeren. Her vises det likevel til at kravet om frivillighet i en samtykke-erklæring overfor en offentlig myndighet kan bli vanskelig å oppfylle.

8. Informasjon og innsyn til den registrerte

Den enkelte søker, student eller doktorgradskandidat som personopplysningene er knyttet til, vil ha status som «den registrerte» etter personopplysningsloven. Det er behandlingsansvarlig som er ansvarlig for å gi den registrerte informasjon og innsyn i behandlingen av personopplysninger, jf. pkt. 9.

Gjeldende personopplysningslov har bestemmelser om den registrertes rett til innsyn i behandling av personopplysninger, og også informasjonsplikten til behandlingsansvarlig, jf. personopplysningsloven § 18, 19 og 20. Det er vanlig praksis at informasjonsplikten oppfylles ved at behandlingsansvarlig utformer en personvernerklæring for behandlingen.

Den nye personvernforordningen vil pålegge behandlingsansvarlig en mer omfattende informasjonsplikt, og ytterligere styrke den registrertes rettigheter når det gjelder informasjon og innsyn, jf. personvernforordringen art. 13, 14 og 15. Bestemmelsene i personvernforordringen er mer detaljerte enn dagens personopplysningslov, og art. 12 stiller blant annet krav om at informasjonen skal være konsis, transparent, forståelig og lett tilgjengelig.

I de tilfeller hvor personopplysningene inngår i beslutningsgrunnlaget til et vedtak som er bestemmende for rettighetene og pliktene til den registrerte, vil vedkommende også ha status som «part» etter forvaltningsloven, og vedkommende kan da påberope seg retten til partsinnsyn, jf. fvl. § 18. Bestemmelse om forhåndsvarsling, utredning, begrunnelse og underretning av enkeltvedtak vil også bidra til at den registrerte får informasjon og innsyn i hvilke personopplysninger som inngår i beslutningsgrunnlaget til et enkeltvedtak.

Bestemmelsene i personvernregelverket og forvaltningsloven vil sammen sørge for at den enkeltes rett til informasjon og innsyn blir godt ivaretatt.

Løsninger som tar utgangspunkt i prinsippene for «selvbetjent forvaltning» vil også bidra til at den registrerte vil ha innsyn i sine personopplysninger. F.eks. er nettsøknaden til Samordna opptak i stor grad basert på en selvbetjent løsning, hvor søkeren har god oversikt over hvilke personopplysninger som inngår i beslutningsgrunnlaget. I Søkerportalen har søkeren mulighet til å laste opp dokumentasjon for å belyse sin egen sak. Søkeren får se sitt elektroniske vitnemål som ligger i Nasjonal vitnemålsdatabase, og får mulighet til å kontrollere innholdet. Søkeren får også se sine resultater fra høyere utdanning i Vitnemålsportalen før vedkommende samtykker til at de kan brukes ved behandling av søknaden.

Informasjon og innsyn når det gjelder behandling av personopplysninger, er også viktig for at den enkelte skal kunne påberope seg andre rettigheter, f.eks. retten til å få rettet mangelfulle personopplysninger.

9. Hvis endringene knytter seg til én eller flere konkrete behandlinger, hvem er eller skal være behandlingsansvarlig?

Behandlingsansvarlig er den som bestemmer formålet med behandlingen av personopplysninger, og hvilke hjelpemidler som skal brukes ved behandlingen. Behandlingsansvarlig er normalt det organet som har den øverste instruksjonsmyndigheten når det gjelder behandling av personopplysninger.

For Samordna opptak er det Kunnskapsdepartementet som er behandlingsansvarlig. Når det gjelder behandling av personopplysninger i studieadministrative systemer er hver enkelt utdanningsinstitusjon behandlingsansvarlig for personopplysninger om sine søkere, studenter og doktorgradskandidater. Som et eksempel kan det vises til Felles studentsystem som er et studieadministrativt system som er i bruk ved de fleste utdanningsinstitusjoner i universitets- og høyskolesektoren i dag, og hvor den enkelte utdanningsinstitusjonen er behandlingsansvarlig for opplysninger om sine søkere, studenter og kandidater.

I forslaget til lovbestemmelser er det foreslått at det går direkte frem av ordlyden hvem som er behandlingsansvarlig for hhv. Samordna opptak og institusjonenes studieadministrative systemer.

10. Hvor lenge skal opplysninger behandles/lagres?

Utgangspunktet er at personopplysningene skal slettes når formålet med behandlingen er oppfylt. Som nevnt ovenfor skal formålet med behandlingen følge direkte av bestemmelser i universitets- og høyskoleloven.

Vurderinger av når formålet anses for å være oppfylt kan i praksis vise seg å være krevende. Når det gjelder personopplysninger som har inngått i beslutningsgrunnlaget til en avgjørelse eller enkeltvedtak, kan det være aktuelt å ta i betraktning den absolutte klagefristen på ett år, jf. forvaltningsloven § 31 tredje ledd. Når det gjelder selve vedtaket kan det være aktuelt å ta i betraktning om en person er aktiv student ved institusjonen, og om vedtaket har betydning for studentens rettigheter i hele studieperioden.

Studieadministrative systemer kan imidlertid inneholde opplysninger som etter sitt formål må oppbevares for en lenger tidsperiode. Dette gjelder for eksempel opplysninger om oppnåelse av grader, eksamenssensur, og vedtak om generell studiekompetanse.

Det bør imidlertid stilles strengere krav til lagring når det gjelder sensitive personopplysninger. Det kan ikke tillates at sensitive personopplysninger oppbevares i en lang tidsperiode. F.eks. må en legeattest som er fremlagt i forbindelse med en søknad om opptak til høyere utdanning, slettes senest ved utløp av den absolutte klagefristen på ett år. Politiattesten til en student må slettes når vedkommende er ferdig med utdanningen og har oppnådd en evt. autorisasjon.

Historiske, statistiske og vitenskapelige formål kan tillate at personopplysningene lagres også etter at det opprinnelige formålet med behandlingen er oppfylt, jf. personopplysningsloven §§ 11 og 28, og personvernforordringen art. 5 nr. 1 bokstav e. Tiltak som anonymisering, avidentifisering eller pseudonymisering må vurderes hvis opplysningene skal brukes til slike formål.

Den registrerte kan også be om sletting av sine personopplysninger, og hvorvidt henvendelsen etterkommes må avgjøres etter en konkret vurdering, jf. personopplysningsloven § 28 tredje ledd. For øvrig kan den registrerte be om både retting, supplering, sperring eller sletting av personopplysninger, jf. personopplysningsloven § 27 og 28 tredje ledd. Den registrerte personens rettigheter på dette området vil bli ytterligere forsterket når den personvernforordningen (personvernforordringen) trer i kraft i mai 2018. Se personvernforordringen art. 16, 17 og 18.

Det må tas høyde for at bestemmelser i arkivlovgivningen kan innebære at opplysningene må lagres også etter at formålet med behandlingen er oppfylt, men opplysningene bør i så fall lagres i egnede og godkjente arkivsystemer.

B. Analysefasen

11. Er det forholdsmessighet mellom behandling og formål?

Formålet for behandlingen av personopplysningene vil fremgå av universitets- og høyskoleloven, og sette en begrensning for hva personopplysningene kan brukes til. Det er kun adgang til å behandle de personopplysninger som er relevante og nødvendige for å oppfylle formålet med behandlingen. Mange av behandlingene er knyttet til oppfyllelse av søkerens eller studentens rettigheter, men kan også gjelde søkerens eller studentens plikter overfor institusjonen. Det er derfor nødvendig å behandle personopplysninger om den enkelte søker eller student.

Når det gjelder opplysninger om helse og sosiale forhold, vil disse kun bli behandlet når det er nødvendig å dokumentere slike forhold. F.eks. kan det være nødvendig for en student å dokumentere sykdom med legeattest, for å dokumentere gyldig fravær på eksamen og få rett til utsatt eksamen.

Et annet eksempel er universitets- og høyskoleloven § 4-9 som sier at på studier hvor studentene kan komme i kontakt med sårbare grupper under praksis, kan institusjonen kreve at studenten legger frem politiattest som nevnt i politiregisterloven § 39 første ledd. En politiattest vil derfor kun bli behandlet i tilfeller hvor en student er tatt opp på en utdanning hvor det er krav om politiattest.

Det er viktig at den registrerte får nok informasjon om hvordan opplysningene blir behandlet, og har tillit til at de blir behandlet på en sikker og forsvarlig måte. Dersom bestemmelsene om informasjon til den registrerte, og kravene om informasjonssikkerhet og internkontroll

som følger av personvernregelverket blir overholdt av behandlingsansvarlig, vil behandlingen ikke oppleves som integritetskrenkende for den enkelte.

12. Analyse av hvilke personverninteresser som gjør seg gjeldende

Personvern i dagens IKT-samfunn handler i stor grad om å kunne ha kontroll over sine egne personopplysninger. For å ivareta personvernet til den enkelte personen opplysningene er knyttet til, er det viktig at den enkelte både får mulighet til å bestemme over tilgang til sine personopplysninger, og også får tilstrekkelig informasjon om hvordan personopplysningene blir behandlet, jf. den norske personvernteorien. Både i EU og internasjonalt blir det lagt vekt på prinsipper som medbestemmelse og rettferdig behandling når det gjelder vern av personopplysninger.

En gjennomgang av alle personverninteressene i den norske personvernteorien og de internasjonale prinsippene om personopplysningsvern vil ikke bli foretatt her. For en grundig gjennomgang vises det til «Personvern i informasjonssamfunnet. En innføring i vern av personopplysninger» av Dag Wiese Schartum og Lee A. Bygrave.

For å ivareta *interessen om innsyn og kunnskap*, ved behandling av personopplysninger i Samordna opptak og studieadministrative systemer, er det viktig at søkere og studenter får god informasjon om hvordan personopplysningene deres blir behandlet. Både gjeldende personopplysningslov og personvernforordringen har bestemmelser om hvilken informasjon som skal gis til den registrerte. Mye av informasjonen skal gis av behandlingsansvarlig etter eget tiltak. Det vises til bestemmelser i personopplysningsloven § 18, 19 og 20, og personvernforordringen art.13, 14 og 15. Når det gjelder enkeltvedtak vil informasjonsplikten bli supplert med kravene om blant annet begrunnelse, underretning og partsinnsyn som følger av forvaltningsloven.

I tillegg har både personopplysningsloven og personvernforordringen bestemmelser som gir den registrerte rett til å få ytterligere informasjon om behandlingen, hvis vedkommende aktivt ber om dette. Når de registrerte personene får tilstrekkelig kunnskap om og innsyn i hvordan behandlingen av personopplysninger skjer, vil de også bli i stand til å påberope seg andre rettigheter som følger av lovgivningen. Innsyn og kunnskap om behandlingen, vil slik også bidra til å ivareta rettssikkerheten til den enkelte søker eller student.

Når det gjelder *kontroll over egne personopplysninger*, vil dette i stor grad bli ivaretatt ved behandling av sensitive personopplysninger. Søkere og studenter vil i stor grad selv være ansvarlig for å legge frem dokumentasjon på helse og sosiale forhold som kan ha betydning for deres rettigheter. Det samme gjelder ved fremleggelse av politiattester. Ved elektronisk opplasting vil den enkelte søker eller student i større grad ha kontroll over at riktig dokumentasjon blir knyttet til deres sak. Utdanningsinstitusjonen er selvfølgelig ansvarlig for å opplyse en sak så godt som mulig, og etterlyse dokumentasjon der det er nødvendig.

Siden det er søkeren eller studenten selv som vil fremlegge dokumentasjon med sensitivt innhold, og vil vedkommende ha kontroll over hvilke sensitive personopplysninger institusjonen har tilgang til. Der disse opplysningene vil inngå i beslutningsgrunnlaget til et enkeltvedtak, vil vedkommende også bli underrettet om innholdet i enkeltvedtaket, jf. forvaltningsloven. Dersom enkeltvedtaket er av sensitivt innhold vil de dermed ha kontroll og oversikt over dette også.

Når det gjelder opplysninger som vil bli innhentet fra andre organer, til bruk i saksbehandlingen, vil den enkelte ha mindre kontroll over selv innhentingen, men på den annen siden vil slik innhenting ivareta *interessen i opplysningskvalitet.* Når det gjelder opplysningskvalitet kan det nevnes som et eksempel at innhenting av adresse fra

Folkeregisteret vil bidra til bedre opplysningskvalitet når det gjelder adressen til den enkelte. Et annet eksempel er innhenting av elektronisk vitnemål fra Nasjonal vitnemålsdatabase, som vil kunne bidra til bedre opplysningskvalitet på søkerens poengsum. Den registrerte vil selvfølgelig ha rett til informasjon om innhentingen, og innsyn i hvilke opplysninger som blir innhentet fra andre organer.

Bruk av fødselsnummer for sikker identifikasjon vil bidra til bedre opplysnings- og behandlingskvalitet, siden det vil bidra til at de nødvendige opplysningene knyttes til rett person. Se også omtale av fødselsnummer under pkt. 13.

De kravene som stilles til informasjonssikkerhet og internkontroll i personvernregleverket vil også bidra til å ivareta behandlingskvaliteten for opplysninger som blir innhentet fra andre organer. Regler som gir den enkelte rett til å kreve retting eller supplering av sine personopplysninger, vil også bidra til å ivareta opplysningskvaliteten, jf. personopplysningsloven § 28 og personvernforordringen art. 16.

Ved elektronisk opplasting av politiattester, skal man tilby løsninger som både skal sikre at den enkelte har kontroll over innholdet, og at utdanningsinstitusjonen skal kunne legge til grunn at innholdet i attesten er autentisk. Elektronisk innlevering av digitalt utstedte politiattester vil kunne redusere faren for dokumentfalsk.

Når det gjelder innloggingsløsningene som skal benyttes av den enkelte søker eller student, er det viktig at de er *brukervennlige*. For å ivareta brukervennligheten, er det også viktig at institusjonene er lydhøre for tilbakemeldinger fra brukerne, og tilrettelegger for dialog.

Løsningene må ha et tilstrekkelig sikkerhetsnivå, og sikkerhetsnivået må være høyere for løsninger hvor sensitiv dokumentasjon skal kunne opplastes.

Søkere og studenter må kunne ha tillit til at institusjonen kun vil behandle deres personopplysninger til nødvendige formål, og at behandlingen vil være lovlig og forsvarlig.

13. Sammenheng opplysningstyper og formål

Når det gjelder sammenheng mellom opplysningstyper og formål, må minimalitetsprinsippet ivaretas. Det vil si at de personopplysningene (opplysningstypene) som blir innhentet og samlet inn, begrenses til det som er helt nødvendig for å oppfylle formålet med behandlingen.

Når det gjelder eksakt *hvilke* opplysningstyper det er nødvendig å behandle for å oppnå formålet, må det foretas jevnlige vurderinger av dette i lys av det som følger av gjeldende lover, forskrifter og evt. lokale retningslinjer. For eksempel vil de gjeldende regler i universitets- og høyskoleloven som regulerer rettighetene og pliktene til en søker eller student, kunne angi hvilke opplysningstyper det er nødvendig å behandle.

F.eks. går det frem av universitets- og høyskoleloven§ 3-6 annet ledd at søkere som er 25 år eller eldre i opptaksåret kan få opptak til enkeltstudier med grunnlag i realkompetanse. Det følger dermed av bestemmelsen at opplysningstypen «fødselsdato» om søkeren må innhentes.

I de tilfeller hvor en søker eller student skal laste opp dokumentasjon eller avgi opplysninger elektronisk, må institusjonen gi tilstrekkelig veiledning, slik at den enkelte selv kan gjøre en vurdering av hvilke opplysninger som er relevante og nødvendige for formålet med behandlingen. Dette vil også kunne begrense at det blir samlet inn «overskuddsinformasjon».

Fødselsnummer

Når det gjelder opplysningstypen «fødselsnummer», fremgår det av pol. 12 at fødselsnummer kun kan benyttes i behandlingen når det er saklig behov for sikker identifisering, og dette er nødvendig for å oppnå slik identifisering.
I den nye personvernforordningen vil bruk av fødselsnummer være regulert av art. 87, og det er åpnet for nasjonale reguleringer.

I universitets- og høyskolesektoren er det i dag vanlig praksis at fødsels- og personnummer brukes for å oppnå sikker identifikasjon av søkere, studenter og doktorgradskandidater, og det legges til grunn at det foreligger et saklig behov for dette. Bruk av fødselsnummer for å oppnå sikker identifisering vil derfor ikke innebære noen endring fra dagens praksis, da dette allerede er i bruk i Samordna opptak og studieadministrative systemer. Under gis det noen eksempler på det er et saklig behov for bruk av fødselsnummer i disse systemene.

Samordna opptak er et samordnet *nasjonalt* opptak til høyere utdanning. Bruk av fødsels- og personnummeret er nødvendig for å oppnå sikker identifikasjon, det vil si for å knytte personopplysningene til rett person og unngå sammenblanding av søkere. F.eks. er bruk av fødsels- og personnummer nødvendig for å sikre at rett elektronisk vitnemål blir hentet inn fra Nasjonal Vitnemålsdatabase under søknadsbehandlingen. I tillegg er det også et prinsipp i det samordnede opptaket at institusjonene saksbehandler for hverandre, og ved bruk av fødsels- og personnummer unngår man sammenblanding av søkere.

I studieadministrative systemer er det også nødvendig å bruke fødsels- og personnummer for å hindre sammenblanding av personer. Sikker identifikasjon er f.eks. nødvendig hvor personopplysninger skal utveksles mellom utdanninginstitusjonene. En institusjons vedtak om generell studiekompetanse skal gi adgang til åpne studier ved andre institusjoner, jf. universitets og høyskoleloven § 3-6 sjette ledd, og i slike tilfeller er det også nødvendig å bruke fødselsnummer for sikker identifikasjon.

Behovet for sikker identifikasjon er også tilstede hvor det skal innhentes personopplysninger fra andre myndigheter, som f.eks. Folkeregisteret, eller hvor det skal utleveres til andre offentlige myndigheter, som f.eks. Lånekassen. Bruk av fødselsnummer er i slike tilfeller nødvendig for å unngå sammenblanding av personer, sikre at opplysningene er knyttet til rett person, og generelt ivareta opplysningskvaliteten.

14. Fins det alternative opplysningstyper og behandlingsmåter som kan ivareta det definerte formålet, men som representerer en mindre personverntrussel? Vurdere tiltak for å avhjelpe personverntrusler

Behandling av sensitive personopplysninger kan i stedet utføres manuelt, slik praksisen er i dag. Det kan argumenteres for at dette er en løsning som representerer en mindre personverntrussel. Krenkelser av personlig integritet kan likevel forekomme ved f.eks. post som kommer på avveie eller blir åpnet av uvedkommende.

Dagens praksis med manuell behandling av sensitiv dokumentasjon er ressurskrevende og mindre effektiv for forvaltningen. Det medgår tid til postgang, skanning, journalføring og lignende, som fører til at det tar lenger tid før dokumentasjonen når frem til rett saksbehandler.

Innsendelse av sensitiv dokumentasjon på papir oppleves som tidkrevende og tungvint for den enkelte søker eller student. Det tar også lengre tid før de får bekreftelse på at dokumentasjonen er mottatt.

Den yngre gruppen har også mindre forståelse for hvorfor slike opplysninger eller dokumentasjon ikke kan leveres elektronisk til utdanningsinstitusjonene. Siden det ikke tilbys elektroniske løsninger hvor en søker eller student kan sende inn sensitive opplysninger, velger mange å sende det inn til institusjonene per e-post. Sensitive personopplysninger som blir sendt inn per e-post innebærer en større personverntrussel, enn en elektronisk løsning hvor søkere og studenter får muligheten til å levere sensitive personopplysninger på en trygg og sikker måte. Det forutsettes selvfølgelig at en slik løsning har et tilstrekkelig høyt sikkerhetsnivå.

Av hensyn til rettssikkerheten til søkere og studenter bør forvaltningen også tilstrebe å effektivisere og digitalisere saksbehandlingen, slik at den enkelte på en enkel måte kan opplyse sin egen sak, og saksbehandlingstiden ved forvaltningen kan reduseres.

Sikring av personopplysninger

Både gjeldende personopplysningslov og den nye personvernforordningen (personvernforordringen) har bestemmelser som stiller krav til tilfredsstillende informasjonssikkerhet og nødvendig internkontroll. Dette er bestemmelser som behandlingsansvarlig er pliktig til å overholde ved behandling av personopplysninger. Relevante bestemmelser er pol. § 13 og 14, og personvernforordringen art. 24, 25, 30, 32 og 35.

Behandlingsansvarlig må iverksette tiltak for å ivareta tilfredsstillende informasjonssikkerhet. I tillegg må behandlingsansvarlig sørge for å iverksette nødvendige tiltak og rutiner for internkontroll, som blant annet skal sikre kvaliteten på de personopplysningene som blir behandlet.

Behandlingsansvarlig må foreta risikovurderinger for å kartlegge om risikoen er på et akseptabelt (forsvarlig nivå), og evt. iverksettes tiltak for å redusere den til et akseptabelt nivå. Det må iverksettes sikkerhetstiltak som ivaretar hensynet til konfidensialitet, integritet og tilgjengelighet ved behandling av personopplysninger, f.eks. tilgangskontroller og kryptering. Kun ansatte med et nødvendig tjenstlig behov bør få tilgang til personopplysningene. Innebygd personvern må implementeres i informasjons-/datasystemer, og de mest personvernvennlige innstillingene må velges som standardløsninger.

Ved behandling av sensitive personopplysninger må sikkerhetsnivået heves til et tilstrekkelig sikkert nivå. F.eks. må en innloggingsløsning som gir en søker eller student mulighet til å laste opp sensitiv dokumentasjon eller politiattester, være egnet til å autentisere personen på et tilstrekkelig høyt nivå. En innloggingsløsning som krever autentisering i to trinn må brukes, f.eks. MinID eller BankID.

Som nevnt under punkt 6, vil konfidensialitet også bli ivaretatt gjennom bestemmelsene om taushetsplikt som følger av forvaltningsloven. Både offentlige og private utdanningsinstitusjoner som er omfattet av virkeområdet til universitets- og høyskoleloven, er pålagt lovbestemt taushetsplikt etter fvl. § 13 første ledd nr. 1 om noens personlige forhold, jf. universitets- og høyskoleloven § 7-6 første ledd.

C. Vurderinger

15. Avveining av eventuelle motstridende personverntrusler

Se pkt. 12 ovenfor om personverninteressen i opplysningskvalitet vs. personverninteressen i kontroll over tilgang til sine personopplysninger.

16. Avveining mot andre hensyn

Hensynet til sårbare grupper (mindreårige)

Den mest personverninngripende behandlingen som lovforslaget åpner for er elektronisk behandling av politiattester *med merknader*. Kravet om politiattest er lovfestet i universitets- og høyskoleloven § 4-9, og forslaget om elektronisk behandling av politiattester er fremmet av hensynet til beskyttelse av sårbare grupper. Under punkt 2 er det redegjort for at det er nødvendig med elektronisk behandling av politiattester av hensyn til autentisering av innholdet. Det må legges til rette for at digitalt utstedte politiattester kan leveres elektronisk, for å redusere faren for dokumentfalsk.

Selv om politiattesten vil bli lagt frem av studenten selv, etter at innholdet er kontrollert, er kravet om politiattest i realiteten et kontrolltiltak. Dersom studenten er tatt opp på en utdanning hvor det kreves fremleggelse av politiattest, er vedkommende nødt til å legge den frem for å kunne delta i praksisundervisningen. Dersom politiattesten har merknader risikerer man også utestenging fra praksis.

På dette punktet må samfunnets interesse i å beskytte sårbare grupper, og ivaretakelse av den personlige integriteten til de sårbare gruppene, veie tyngre enn hensynet til de studentene som har merknader på politiattesten. Risikoen for at uegnede personer kan komme i kontakt med sårbare grupper under praksis på utdanningen, må elimineres i størst mulig grad. Dette kan først skje når vi vet med sikkerhet at den politiattesten som blir levert til institusjonen, leveres i den form og med det innhold politiet har utstedt den.

Personvernet til studentene skal selvfølgelig ivaretas i størst mulig grad ved innlevering av attestene. Studentene må tilbys en trygg og sikker innloggingsløsning, som kan benyttes ved innlevering av politiattesten til institusjonen. Innloggingen bør skje gjennom en to-trinns innloggingsløsning. I tillegg må institusjonen iverksette nødvendige sikkerhetstiltak (kryptering, tilgangskontroller o.l.).

Gjenbruk av opplysninger

Innhenting av nødvendige personopplysninger fra andre organer og muligheter, vil kunne legge til rette for gjenbruk av personopplysninger. Det vises til regjeringens IKT-politikk, jf. Digital Agenda. Det er en målsetting at forvaltningen skal fremstå som helhetlig og sammenhengende, og at borgerne ikke skal bli spurt om opplysninger som forvaltningen allerede har fått oppgitt eller har tilgjengelig. Ved innhenting av nødvendige personopplysninger fra andre organer, vil også universitets- og høyskolesektoren kunne bidra til å oppnå denne målsettingen.

Opplysningskvalitet og rettssikkerhet

Innhenting av nødvendige personopplysninger fra andre organer vil kunne bidra til å heve kvaliteten på personopplysningene. Når kvaliteten på personopplysningene heves, vil også kvaliteten på beslutningsgrunnlaget til enkeltvedtak og avgjørelser som er bestemmende for rettighetene eller pliktene til en søker eller student heves. Dermed vil rettssikkerheten til den enkelte bli ivaretatt på en bedre måte.

Automatisert saksbehandling og rettssikkerhet

Automatisert saksbehandling, det vil si enkeltvedtak og avgjørelser som blir truffet ved hjelp av et datasystem hvor rettsreglene er blitt formalisert og programmert, kan bidra til å ivareta rettssikkerheten til søkere og studenter Dette fordi automatisert saksbehandling bidrar til likebehandling og effektivitet i saksbehandlingen, og reduserer faren for at det begås menneskelige feil. Forutsatt at rettsreglene er blitt riktig programmert i systemet, vil automatisert saksbehandling bidra til korrekt rettsanvendelse, og dermed likebehandling av søkere og studenter. Automatisert saksbehandling vil også bidra til å korte ned

saksbehandlingstiden, slik at den enkelte slipper å gå rundt i uvisshet og vente på avgjørelser som er bestemmende for vedkommendes rettigheter og plikter.

Samtidig er det viktig å gi de registrerte personene god informasjon om hvordan automatisert saksbehandling foregår, slik at prosessen fremstår som åpen og forutsigbar.

Det må iverksettes tiltak for å sikre at de registrerte får mulighet til å få overprøvd automatiserte avgjørelser ved manuell saksbehandling. Det er viktig å legge til rette for søkere og studenter som kan ha behov for en individuell vurdering, hvor anvendelse av forvaltningsskjønn er nødvendig. Det er viktig med likebehandling for å unngå vilkårlig forskjellsbehandling, men saklig og begrunnet forskjellsbehandling bør likevel være tillatt.

D. Oppsummering og konklusjon

17. Konklusjon av personvernanalysen og begrunnelse for valgene

Det er behov for å innføre lovhjemmel for elektronisk behandling av personopplysningene til søkere og studenter i universitets- og høyskolesektoren for at institusjonene skal kunne utføre sine oppgaver og plikter på en lovlig, effektiv og ressursbesparende måte. Selv om mange av de omtalte personopplysningene om søkere og studenter også i dag blir behandlet med grunnlag i personopplysningsloven § 8, er det nødvendig med en lovhjemmel for behandlingsgrunnlaget i universitets- og høyskoleloven, for å skape åpenhet og forutsigbarhet om hvordan sektoren behandler personopplysninger om søkere og studenter. Dette er viktig for at personvernet og rettssikkerheten til denne gruppen skal bli tilstrekkelig ivaretatt.

Offentlige organer og myndigheter skal sørge for en effektiv utnyttelse av samfunnets ressurser, og samtidig sørge for at rettighetene til den enkelte borger blir ivaretatt. Rettssikkerheten til borgerne skal ivaretas, og de lovhjemlene som er foreslått er begrunnet både i rettsikkerhet- og personvernhensyn.

Åpenhet og forutsigbarhet når det gjelder behandling av personopplysninger om søkere og studenter vil bidra til å ivareta både rettssikkerheten og personvernet til disse gruppene.

Muligheten til å innhente nødvendige personopplysninger fra andre organer vil bidra til bedre kvalitet på personopplysningene og beslutningsgrunnlaget. På denne måten vil kvaliteten i de enkeltvedtak og avgjørelser institusjonen fatter kunne heves, og dette vil også ivareta rettssikkerheten til den enkelte. Bedre opplysningskvalitet på de personopplysningene som blir behandlet, vil også være til fordel for personvernet til den enkelte søker eller student.

Automatisert saksbehandling vil ikke bare sørge for en bedre utnyttelse av samfunnets ressurser og opplysningskvalitet, men vil også bidra til likebehandling, riktig rettsanvendelse og effektivitet i saksbehandlingen.

Muligheten til å sende inn sensitiv dokumentasjon vil gi den enkelte søker eller student mulighet til å opplyse sin sak på en god og effektiv måte, i tillegg til at saksbehandlingstiden vil kunne reduseres.

Både automatisert saksbehandling og muligheten for at den enkelte søker eller student selv kan laste opp dokumentasjon elektronisk, vil sørge for at opplysningene blir knyttet til rett person og sak. Dette vil redusere risikoen for at det blir begått menneskelige feil under saksbehandlingen.

Dersom utdanningsinstitusjonene får mulighet til å behandle studenters politiattester elektronisk, vil det bidra til at hensynet til de sårbare gruppene som studentene kan komme i kontakt med under praksisutdanningen, kan ivaretas på en bedre måte. Dette vil bidra til at innholdet i en digitalt utstedt politiattest blir tilstrekkelig autentisert og verifisert, slik at faren for dokumentfalsk blir redusert.

Muligheten til å levere politiattester elektronisk vil også kunne gi studentene en enkel og effektiv måte å levere politiattesten, og bidra til å korte ned saksbehandlingstiden ved institusjonene når de skal vurdere om studenten har rett til å delta i praksisundervisningen eller ikke.

Når det gjelder Samordna opptak og studieadministrative systemer er det hhv. Kunnskapsdepartementet og utdanningsinstitusjonene som er behandlingsansvarlig. I rollen som en offentlig myndighet og behandlingsansvarlig, har disse institusjonene et stort ansvar når det gjelder ivaretakelse av personvernet til søkere og studenter, ved behandling av deres personopplysninger.

Rettslig grunnlag for behandling av personopplysninger i lov er ikke alene tilstrekkelig for at behandlingen av personopplysninger vil bli ansett som lovlig. Samtlige krav som gjeldende personopplysningslov og den nye personvernforordningen stiller til behandling av personopplysninger må oppfylles. Kravene til tilfredsstillende informasjonssikkerhet, rutiner for internkontroll og sikring av opplysningskvaliteten må også overholdes. Det må iverksettes sikkerhetstiltak for å ivareta hensynet til konfidensialitet, integritet og tilgjengelighet ved behandlingen. Blant annet med det må iverksettes tiltak som tilgangskontroller, kryptering o.l. for å hindre at uvedkommende får tilgang til personopplysningene. Den registrerte personens lovbestemte rettigheter må ivaretas ved behandlingen, og en av forutsetningene for at den registrerte skal kunne påberope seg sine rettigheter er at vedkommende får nok informasjon om behandlingen av sine personopplysninger. Både departementet og institusjonene må sørge for at personvernregelverket blir overholdt, slik at rettighetene til søkere og studenter blir ivaretatt.

Forutsatt at bestemmelsene om behandling av personopplysninger, som fremgår av gjeldende personopplysningslov og den kommende personvernforordningen, blir overholdt, er vår konklusjon at lovforslaget ikke vil få noen negative konsekvenser for personvernet til søkere og studenter.