Helsedirektoratet Direktoratet for e-helse

Helseopplysninger i skyen

Er det behov for en utredning av rettslige problemstillinger ved behandling av helseopplysninger i skytjenester?

1. oktober 2021

Innhold

1. Innledning 3
1.1. Tolkning av oppdraget og avgrensning av svaret 3
2. Overføring av personopplysninger 4
2.1. Arbeidet i det europeiske Personvernrådet (EDPB) 5
2.2. Datatilsynet 5
2.3. Pågående forhandlinger 5
2.4. Arbeid hos norske myndigheter som oppfølging av Schrems II 6
3. Veiledere og pågående aktivitet på området 7
4. Er det behov for ytterligere veiledning? 9
5. Anbefaling om videre oppfølging 10
5.1. Samle lenker til veiledningsmateriale 10
5.2. Ytterligere veiledning 10
5.3. Følge problemstillingene videre i delprosjektet "KI – data og algoritmer" 10

1. Innledning

Dette dokumentet er svar på oppdrag fra Helse- og omsorgsdepartementet. Det er utarbeidet i samarbeid mellom Direktoratet for e-helse og Helsedirektoratet.

1.1. Tolkning av oppdraget og avgrensning av svaret

I rapporten "Helseopplysninger i skyen – Er det behov for en utredning av rettslige problemstillinger ved behandling av helseopplysninger i skytjenester?" som ble levert til Helse- og omsorgsdepartementet høsten 2020 foreslo Helsedirektoratet fire konkrete oppfølgingspunkter:

1. Sørge for at lenker til tilgjengelig veiledningsmateriale om skytjenester samles på ett sted.
2. Utrede om det er behov for ytterligere veiledning om behandling av helseopplysninger i skytjenester.
3. At Helsedirektoratet følger med på arbeidet i Personvernrådet og utreder om det er behov for konkret veiledning om hva som kan være ytterligere tiltak ved overføring av helseopplysninger som samles inn i helse- og omsorgstjenesten. Eventuelle tiltak bør utarbeides i samarbeid med andre etater som har behandling av helseopplysninger innenfor sitt myndighetsområde. Det er naturlig å se hen til vurderingene av skytjenester som gjøres i Helseanalyseplattformen.
4. At NSMs anbefaling om å utrede behov for sterkere nasjonal regulering av skytjenester i helse- og omsorgstjenesten følges opp.

I tildelingsbrevet for 2021 har HOD gitt etatene i koordineringsprosjektet "Bedre bruk av kunstig intelligens" følgende oppdrag:

> *Etatene skal, innen samme frist [1. oktober 2021], utrede hvilke rammebetingelser helsemyndighetene bør justere for å legge til rette for lagring av helseopplysninger i skyen, jf. redegjørelse for problemstillinger knyttet til dette i rapport av oktober 2020. Utredningen skal legge nasjonale og internasjonale rammebetingelser utenfor helsesektoren, herunder sikkerhetsloven, til grunn for sitt arbeid. Helsedirektoratet skal koordinere arbeidet.*

Oppdragsteksten kan synes å gå lenger enn oppfølgingspunktene som Helsedirektoratet foreslo i forrapporten fra høsten 2020. Som følge av at de mest sentrale spørsmålene om bruk av skytjenester ikke berører vårt regelverk, og det samtidig pågår flere prosesser nasjonalt og internasjonalt for å løse den største utfordringen, nemlig overføringsproblematikken, har vi kommet til at vi begrenser vårt svar til oppfølgingspunktene i forrapporten.

2. Overføring av personopplysninger

Som nevnt i forrapporten har vi i møter med aktører som utvikler eller skal anskaffe systemer med kunstig intelligens for bruk i helse- og omsorgstjenesten, diskutert problemstillinger knyttet til skytjenester. I møtene har vi blant annet fått spørsmål om det er lovlig å behandle helseopplysninger i skytjenester og hvilke lovkrav som gjelder dersom det er lovlig. Særlig har de ulike aktørene tatt opp spørsmålet om helseopplysninger lovlig kan overføres til land utenfor EØS-området, såkalte tredjeland.

Aktører som har hatt dialog med leverandører av skytjenester, inkludert leverandører som leverer systemer med kunstig intelligens via skytjenester, opplever at flere av leverandørene enten har servere i tredjeland eller at leverandørene bruker underleverandører i tredjeland, som oftest i USA.

Behandling av personopplysninger i Norge er regulert i personopplysningsloven som også omfatter EUs personvernforordning (GDPR). I tillegg er behandling av helseopplysninger regulert i særlovgivning som utfyller personvernregelverket. Bruk av skytjenester innebærer at det må inngås databehandleravtale, og at underleverandører må kunne følges opp. Aktørene opplever at leverandøren ikke utøver full åpenhet om bruk av underleverandører.

Det er den dataansvarliges ansvar å sikre at behandling av personopplysninger skjer i tråd med de grunnleggende personvernprinsippene og regelverket for øvrig. Dette skal skje etter vurdering av ulike forhold, som behandlingens art, omfang, formål og sammenhengen den utføres i, samt risikoene av varierende sannsynlighets- og alvorlighetsgrad for våre rettigheter og friheter som fysiske personer.

Bruk av skytjenester innebærer ofte overføring av personopplysninger til utlandet. Overføring skal forstås i vid forstand og inkluderer:

- Faktisk overføring til og lagring i et tredjeland (for eksempel lagring av opplysninger på server i USA)
- Lagring og behandling i EU/EØS/godkjent land, men tilgang til personopplysninger for driftspersonell fra tredjeland (for eksempel for oppgradering av teknisk løsning der det er nødvendig å ha tilgang til personopplysninger)
- Lagring og øvrig behandling i EU/EØS/godkjent land, men tilgang til personopplysninger for supportpersonell fra tredjeland

Utgangspunktet for overføring av personopplysninger til utlandet er at det landet overføring skal skje til må ha et tilstrekkelig nivå for ivaretakelse av personvernet. Innenfor EU/EØS gjelder GDPR, og da er det ikke krav om et eget overføringsgrunnlag. Det finnes også noen tredjeland som er forhåndsgodkjente av Kommisjonen, og som man heller ikke behøver å gjøre egne vurderinger av. For overføring av personopplysninger til øvrige land (såkalte tredjeland) må den dataansvarlige forsikre seg om at personvernet vil bli ivaretatt.

Tidligere kunne man overføre personopplysninger til USA basert på en egen ordning, Privacy Shield. Konsekvensene av Schrems II-avgjørelsen fra EU-domstolen[1] er at overføring til USA ikke lenger kan skje basert på Privacy Shield-ordningen (artikkel 45), men må basere seg på et av de andre lovlige grunnlagene.

[1] Avgjørelse i EU-domstolen CJEU C-311/18.

Bortfall av Privacy Shield-ordningen er årsaken til at helse- og omsorgssektoren, i likhet med alle andre som benytter skyløsninger, har fått en utfordrende situasjon med hvordan personopplysninger lovlig skal kunne overføres til USA.

I etterkant av Schrems II-dommen har det vært utgitt ulike nasjonale og europeiske veiledninger.

2.1. Arbeidet i det europeiske Personvernrådet (EDPB)

Etter EU-domstolens avgjørelse i Schrems II har det europeiske Personvernrådet (EDPB) utarbeidet veiledning om overføring av personopplysninger i tredjeland. Veiledningen er publisert i *Guidelines 2/2020 on articles 46 (2) (a) and 46 (3) (b) of Regulation 2016/679 for transfers of personal data between EEA and non-EEA public authorities and bodies*, versjon 2.0.[2]

Videre har EDPB publisert anbefalinger om essensielle europeiske garantier som må være oppfylt også ved overvåkningstiltak. Anbefalingene er publisert i *Recommendations 02/2020 on the European Essential Guarantees for surveillance measures.*[3]

EDPB publiserte den 18. juni 2021 veiledning om ytterligere tiltak ved overføring av personopplysninger til tredjeland. Veiledningen er publisert i *Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data.*[4]

2.2. Datatilsynet

Datatilsynet publiserte 3. september 2021 en veileder for overføring av personopplysninger ut av EØS. Veilederen gir en gjennomgang av hva som skal til for at personopplysninger kan overføres til land utenfor EØS. "Særlige kategorier personopplysninger", som for eksempel helseopplysninger, krever høyere grad av beskyttelse etter personvernforordningen sammenlignet med andre personopplysninger og er omtalt i veilederen.

Når man skal vurdere om det er lov å overføre personopplysninger ut av EØS, kan man ifølge veilederen ta utgangspunkt i følgende sjekkliste:

1. Kjenn overføringene
2. Identifiser overføringsgrunnlag
3. Vurder om overføringsgrunnlaget vil være effektivt i lys av alle omstendighetene ved overføringen
4. Iverksett ytterligere tiltak
5. Re-evaluer med jevne mellomrom

Alle punktene i sjekklisten kommer med en forklaring, og steg 3 (vurdering av beskyttelsesnivå) og 4 (ytterligere tiltak) er spesielt utdypet.

Veilederen inneholder også en liste over såkalte "godkjente land" utenfor EU-/EØS-området.

2.3. Pågående forhandlinger

Det pågår også forhandlinger mellom EU og USA for å få på plass en ny avtale om overføring av personopplysninger til USA under GDPR art. 46. Avhengig av hva avtalen vil omfatte, kan en slik avtale også få betydning for bruk av kunstig intelligens i skytjenester ved ytelse av helsehjelp. Forhandlingene ble intensivert etter at Joe Biden ble innsatt som

[2] edpb_guidelines_202002_art46guidelines_internationaltransferspublicbodies_v2_en.pdf (europa.eu).
[3] edpb_recommendations_202002_europeanessentialguaranteessurveillance_en.pdf (europa.eu)
[4] https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en

president i USA. Blant annet er det utnevnt en ny sjefsforhandler fra USAs side, og i et seminar i regi av IAPP i mai sa både han og EU-Kommisjonens sjefsforhandler at de var optimistiske om muligheten for å komme frem til en god løsning.

2.4. Arbeid hos norske myndigheter som oppfølging av Schrems II

Skate er et strategisk samarbeidsråd som skal gi råd til Digitaliseringsdirektoratet og digitaliseringsministeren. Skate skal bidra til en samordnet digitalisering av offentlig sektor som gir gevinster for innbyggerne, næringslivet, frivillig sektor, og offentlige virksomheter. Våren 2021 ble det gjennomført et koordineringsarbeid for arbeidet med Schrems II, og det er anslått at dette arbeidet vil avsluttes innen høsten 2021. I møtepapirene til Skate-møtet 13. oktober 2021 opplyses det at: *"(…)de offentlige virksomhetene er avhengig av å få på plass en løsning innen rimelig tid for å ivareta sine rettslige forpliktelser. Det er likevel grunn til å tro at arbeidet med Schrems II vil avdekke utfordringer og ulike praksiser i offentlige aktørers bruk av skytjenester. Eksempelvis antar vi at det vil bli avdekket at flere offentlige virksomheter har ulike risikovurderinger for samme utfordringer. Videre antar vi at det skjer ulike juridiske vurderinger for de samme juridiske problemstillingene. I bruken av skytjenester foretas det svært kompliserte vurderinger av teknisk, juridisk, sikkerhetsmessig og økonomisk art. Offentlig sektor benytter de samme skytjenestene og på nesten de samme måtene. Offentlig sektor vil være tjent med at det skjer en koordinering i dette arbeidet. På den måten kan vi sørge for optimale løsninger og god ressursbruk. Det kan være naturlig å se arbeidet opp mot regjeringens strategi for bruk av skytjenester."*

Vi finner også grunn til å nevne at personvernombudene i Helsedirektoratet, Direktoratet for e-helse og Norsk Helsenett har utarbeidet et notat om overføring av personopplysninger til tredjeland etter Schrems II-dommen. Notatet har først og fremst de tre virksomhetene som målgruppe.

3. Veiledere og pågående aktivitet på området

I forrapporten viste vi at det allerede finnes omfattende veiledningsmateriale om skytjenester som er utgitt av forskjellige norske myndigheter. Noen av disse veilederne er nok ikke godt kjent i helse- og omsorgstjenesten.

Norm for informasjonssikkerhet og personvern (Normen) i helse og omsorgstjenesten har krav til bruk av skytjenester. Normen har også mye veiledningsmateriell som kan hjelpe sektoren i vurderinger av skytjenester og generelt om informasjonssikkerhet og personvern.

Normens veileder i bruk av skytjenester til behandling av helse- og personopplysninger gir praktisk hjelp innenfor områdene:

- Fastsette ansvar, inngå avtaler, ivareta kontroll og vurdere risiko
- Belyse fordeler ved teknologien
- Synliggjøre trusler og behov for kontroll
- Ivaretakelse av pasientens rettigheter til samtykke, innsyn, retting sletting mv.
- Eksempler på risikoområder som det er naturlig å belyse
- Etabler databehandleravtale
- Behandling av helse- og personopplysninger under Normens virkeområde

I et vedlegg til denne veilederen har Cloud Security Alliance Norway kartlagt Normens krav til Cloud Controls Matrix (CCM). I tillegg er det utarbeidet en kryssreferanse fra CCM til kapitlene i Normen. CCM-rammeverket gjør det enklere for både kunder og leverandører å snakke samme språk når sikkerheten i en skyløsning skal vurderes.

Foruten Normens veileder om bruk av skytjenester til behandling av helseopplysninger finnes det ingen andre veiledere som spesifikt omhandler bruk av skytjenester ved behandling av helseopplysninger, og det finnes ingen som spesielt omtaler bruk av systemer med kunstig intelligens i skytjenester, etter det vi kjenner til.

Norsk Helsenett har imidlertid en egen temaside om skytjenester på sine nettsider, og de utvider for tiden sitt tjenestetilbud med å bygge opp kompetanse for å tilby tjenester i skyen.

Det finnes også flere mer generelle veiledere som også er svært nyttige for aktører i helse- og omsorgstjenesten. Blant annet omtales anskaffelse, sky og sikkerhet i Nasjonal sikkerhetsmyndighets (NSM) "Grunnprinsipper for IKT-sikkerhet". NSM har også en nettside for ofte stilte spørsmål om sky og tjenesteutsetting, hvor også spørsmål særskilt relatert til sikkerhetsloven omtales.

Digitaliseringsdirektoratet omtaler også skytjenester på sine nettsider. Hovedbudskapet er at virksomheter som etablerer nye eller oppgraderer eksisterende fagsystemer eller digitale tjenester, eller endrer eller fornyer avtaler knyttet til drift, skal vurdere skytjenester på linje med andre løsninger.

Markedsplassen for skytjenester er en del av www.anskaffelser.no som eies av DFØ. Markedsplassen skal være stedet hvor offentlige oppdragsgivere og leverandører møtes når offentlig sektor skal investere i skyteknologi. Markedsplassen skal bidra til økt utbredelse av sikre, lovlige og kostnadseffektive skytjenester. Her skal offentlige virksomheter få en god og strukturert oversikt over leverandører og tjenester tilgjengelig i markedet. Det skal være

mulig å knytte seg til og benytte frivillige fellesavtaler inngått av statens innkjøpssenter. På markedsplassen skal virksomheter også finne veiledning om risiko og råd om sikkerhet.

I tillegg til veiledningsaktivitet er det også flere andre store initiativ som vil få betydning på området. Internasjonale teknologiselskaper jobber med metoder for å kunne tilby plattformer, drift og funksjonalitet i Europa og fra europeisk eierskap. Dette vil ha påvirkning for helse- og omsorgssektoren i Norge.

EU satser på bruk av skytjenester og har flere initiativer for å bidra til økt bruk, Cloud computing | Shaping Europe's digital future (europa.eu). Det er også store investeringer i utvikling av diverse store europeiske skytjenester som for eksempel Gaia-X.

Relevant regelverk fra EU, om blant annet KI og NIS-direktivene, samt sikkerhetsloven vil også kunne ha betydning for vurderinger av lagring i sky.

4. Er det behov for ytterligere veiledning?

Budskapet fra både regjeringen, Direktoratet for e-helse samt tilsynsmyndigheter, er at skytjenester kan benyttes til behandling av personopplysninger, inkludert særlige kategorier av personopplysninger. KI-prosjekter og andre aktører i helse- og omsorgstjenesten som har spørsmål om det er lovlig å behandle helseopplysninger i skytjenester og hvilke lovkrav som gjelder dersom det er lovlig, kan lett henvises til ulike veiledere og informasjon om dette. Vi kan derfor ikke se per i dag at det er behov for ytterligere *generell* veiledning om helseopplysninger i skytjenester.

Det som er et vanskeligere spørsmål, er hva som skal til for at KI-prosjekter og andre aktører i helse- og omsorgstjenesten kan ta i bruk skytjenester som innebærer overføring av personopplysninger til andre land enn et EU/EØS/godkjent land, og om det er behov for konkret veiledning om hva som være ytterligere tiltak ved overføring av helseopplysninger som er samlet inn i helse- og omsorgstjenesten. Til dette er EDPBs veileder fra 18. juni 2021 og Datatilsynets veileder fra 3. september 2021 for ferske. Vi vet lite om hvor avklarende disse veilederne er for aktører i helse- og omsorgstjenesten. I den anledning viser vi også til det pågående arbeidet i Skate om forholdet mellom Schrems II-dommen og offentlige aktørers bruk av skytjenester, som etter planen skal avsluttes i løpet av høsten.

Hva som skal til for at KI-prosjekter og andre aktører i helse- og omsorgstjenesten kan ta i bruk skytjenester som innebærer overføring av personopplysninger til andre land enn et EU/EØS/godkjent land er et vanskelig spørsmål. Behovet for konkret veiledning om hva som vil være ytterligere tiltak ved overføring av helseopplysninger som er samlet inn i helse- og omsorgstjenesten er på det nåværende tidspunkt ikke klart. Det vil være behov for mer veiledning spisset mot helse, selv om vi ikke ennå helt ser rekkevidden av den mer generelle veiledningen som foreligger og det som kommer.

5. Anbefaling om videre oppfølging

Problemstillingene knyttet til bruk av skytjenester for aktører i helse- og omsorgstjenesten berører ikke bare kunstig intelligens og kan som gjennomgangen ovenfor viser, heller ikke løses innenfor prosjektet "Bedre bruk av kunstig intelligens". Vi har imidlertid kommet frem til to oppfølgingspunkter for prosjektet.

5.1. Samle lenker til veiledningsmateriale

Siden forrapporten ble skrevet, er det tilkommet ytterligere veiledninger m.m. innenfor temaet skytjenester. Vi vil derfor legge ut lenker til veiledningsmaterialet om skytjenester som er omtalt i dette dokumentet på temasiden for kunstig intelligens på Helsedirektoratets nettsider, eller den tverretatlige informasjonssiden som etter planen skal lanseres i desember.

5.2. Ytterligere veiledning

Vi vil anbefale at etatene følger situasjonen og følger opp med veiledning når behovet blir klarere. Normen bør følge utviklingen på feltet skytjenester og oppdatere aktuelt veiledningsmateriell ved behov

5.3. Følge problemstillingene videre i delprosjektet "KI – data og algoritmer"

Overføringen av personopplysninger må ha et lovlig overføringsgrunnlag uavhengig av hvilken teknologi som benyttes eller hva formålet med behandlingen av personopplysninger er. Det gjelder ikke andre regler for dette når personopplysninger behandles ved bruk av kunstig intelligens.

Nye analyseteknikker, som kunstig intelligens (KI) og maskinlæring (ML), trenger tilgang til store mengder data. Data må lagres og deles mellom virksomheter og land, og samtidig må dataansvarlig sikre at personvernet og sikkerheten ivaretas. Her vil bruk av skytjenester være viktig moment.

Distribuert analyse er en metode som sikrer at data forblir lokalt der de er lagret, og muliggjør trygge analyser med flere datakilder som er underlagt ulike regler. Les mer om dette Utviklingstrekk 2021 - ehelse

Koordineringsprosjektet "Bedre bruk av kunstig intelligens" igangsetter høsten 2021 et eget delprosjekt kalt "KI – data og algoritmer" i regi av Direktoratet for e-helse. Delprosjektet vil tydeliggjøre behov og anbefale eventuelle tiltak for å støtte oppunder helsetjenestens behov for tilgang til tilstrekkelig mengder data.

Det er naturlig at dette delprosjektet tar med seg problemstillingene om helseopplysninger i sky med seg i sitt arbeid. Delprosjektet bør oppsummere eventuelle funn dersom de gjennom sitt arbeid avdekker at det er behov for mer veiledning om helseopplysninger i skytjenester, særskilt om det er behov for konkret veiledning om hva som være ytterligere tiltak ved overføring av helseopplysninger til andre land enn et EU/EØS/godkjent land.