Dataansvar

I all behandling av person- og helseopplysninger skal det være en dataansvarlig[1]. Den dataansvarlige har hovedansvaret for at behandling av person- og helseopplysninger er i samsvar med gjeldende regelverk. EUs personvernforordning (GDPR) gir rammer for dataansvaret ved å detaljere en mengde plikter og oppgaver, og legger opp til sanksjoner når pliktene ikke overholdes.

Plassering av dataansvar vil påvirke hvilke oppgaver som blir igjen i Direktoratet 2.0 og hvilke oppgaver som overføres til ny tjenesteleverandør. Riktig plassering av dataansvar vil således bidra til å sikre at oppgaver og plikter blir liggende i og utføres i den virksomheten som GDPR legger opp til. Dette vil legge til rette for at Direktoratet 2.0 og ny tjenesteleverandør etterlever GDPR.

Tilleggsoppdraget fra HOD ber om forslag for plassering av dataansvar for løsninger som ikke er regulert i forskrift (Helsenorge og Grunndata). For å sikre en helhetlig tilnærming vil løsningene som er regulert i forskrift som Nasjonal kjernejournal og Reseptformidleren (e-resept) også vurderes. Derfor vil vurdering av plassering av dataansvar i dette kapittelet omfatte Kjernejournal, Reseptformidleren (e-resept), Helsenorge og Grunndata.

Nærmere om dataansvar

Ansvaret for behandling av person- og helseopplysninger (dataansvar) reguleres i GDPR, personopplysningsloven og helselovgivningen.

GDPR er åpen for at flere virksomheter i fellesskap har ansvar for den samme behandling av person- og helseopplysninger (*felles dataansvar*). Dersom to eller flere dataansvarlige i felleskap fastsetter formålene og midlene for behandlingen, skal de være felles dataansvarlige.[2] Denne ordningen kalles ofte "solidarisk dataansvar", der en og hver virksomhet i dette fellesskapet *sammen og på lik linje* som de andre er ansvarlige for den samme behandlingen. Dette innebærer blant annet at innbygger kan henvende seg til hvem som helst av de dataansvarlige,[3] fordi alle de dataansvarlige *de facto* er ansvarlig for hele behandlingen av person- og helseopplysninger. Dette er for å sikre at den registrerte mottar en effektiv erstatning.[4] Enhver dataansvarlig som har betalt full erstatning til den registrerte, kan deretter gjøre regress gjeldende mot andre dataansvarlige som har vært involvert i den samme behandlingen.[5]

Det er et prinsipp i personvernlovgivningen at dataansvaret ikke kan overføres til andre virksomheter dersom dette betyr *deling* av dataansvaret for den samme behandling av personopplysninger. Felles dataansvar innebærer derfor at det blir flere dataansvarlige for

---

[1] For behandling av helseopplysninger brukes begrepet "dataansvarlig", for behandling av andre personopplysninger brukes begrepet "behandlingsansvarlig". Innholdet er det samme og begrepet dataansvarlig benyttes kun i helselovgivningen.
2 Jf. GDPR art. 26 (1).
3 Se GDPR art. 82 (4), fortalepunkt 146.
4 Jf. GDPR art. 82 (4).
5 Jf. GDPR art. 82 (5), fortalepunkt 146.

den samme behandlingen der hver og en har en selvstendig plikt til å oppfylle kravene i personvernregelverket. Dette understreker den grunnleggende forutsetningen om at ansvaret ikke kan delegeres. Utførelsen av behandling av person- og helseopplysningene og tilknyttede oppgaver kan i motsetning til ansvaret delegeres til andre virksomheter, dersom denne virksomheten anses å behandle person- og helseopplysninger *på vegne av* dataansvarlig som databehandler.

GDPR legger opp til såkalt "separat dataansvar" der enkelte virksomheter er ansvarlig kun for behandling av person- og helseopplysninger de selv har kontroll over. En virksomhet som alene bestemmer formålet og virkemidlene har et selvstendig dataansvar for behandlingen av personopplysningene. Innbygger kan i et slikt tilfelle kun henvende seg til den enkelte virksomheten som har ansvar for den konkrete behandlingen. Et eksempel på dette er DDFL (Digital dialog fastlege) på helsenorge.no der fastlegen er dataansvarlig for helseopplysninger som lagres i eget system (med hjemmel i journalføringsplikten i helsepersonelloven), mens direktoratet er dataansvarlig for lagringen på helsenorge.no (med hjemmel i samtykke fra innbyggeren). Innbygger kan henvende seg til fastlegen dersom det er snakk om lagring i pasientjournalen, og til direktoratet for den videre behandlingen som skjer på helsenorge.no.

Kriterier for plassering av dataansvar

Kriterier for plassering av dataansvar – enten det gjelder felles dataansvar eller separat dataansvar – er i prinsippet de samme. Dataansvaret bør plasseres slik at de som har reell kontroll på utøvelsen av oppgaver og ansvar i behandling av person- og helseopplysninger, enten som følge av loven eller av faktiske forhold for den relevante løsningen, er den som blir dataansvarlig.

Hvor dataansvar plasseres er derfor bestemmende for oppgaver og plikter som følger med en slik plassering.

Utgangspunktet for vurderingen av plassering av dataansvar vil alltid være definisjonen av begrepet "dataansvarlig" i regelverket.

Definisjon av "dataansvarlig" i helselovgivningen viser til GDPR:

> *"dataansvarlig: ansvarlig for behandling av helseopplysninger etter personvernforordningen artikkel 4 nr. 7."*[6]

GDPR artikkel 4. nr. 7 definerer "behandlingsansvarlig" som:

> *"en fysisk eller juridisk person, en offentlig myndighet, en institusjon eller ethvert annet organ som alene eller sammen med andre bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes; når formålet med og midlene for behandlingen er fastsatt i unionsretten eller i medlemsstatenes nasjonale rett, kan den behandlingsansvarlige, eller de særlige kriteriene for utpeking av vedkommende, fastsettes i unionsretten eller i medlemsstatenes nasjonale rett,"*

[6] Pasientjournalloven § 2 bokstav e.

I følge artikkel 29-arbeidsgruppen for beskyttelse av personopplysninger (Artikkel 29-gruppen) inneholder definisjonen av behandlingsansvarlig tre hovedelementer:

- det personlige aspektet ("den fysiske eller juridiske person, en offentlig myndighet, en institusjon eller ethvert annet organ");
- muligheten for kontroll ("som alene eller sammen med andre"); og
- de essensielle elementene for å skille behandlingsansvarlig fra andre aktører ("bestemmer *formålet* med behandling av personopplysninger og *hvilke midler* som skal benyttes").

Særlig de to siste punktene gir føringer for hvordan man skiller dataansvarlig fra andre virksomheter som er direkte eller indirekte involvert i behandlingen av person- og helseopplysninger. Dette vil si at den dataansvarliges faktiske innflytelse og kontroll henger sammen med myndighet til å bestemme formålet med behandlingen av person- og helseopplysningene og hvilke midler som skal benyttes.

Dataansvarliges myndighet til å bestemme *formålet* innebærer ansvar for å sikre at løsningen utvikles i tråd med det bestemte formålet og at all behandling av person- og helseopplysninger i løsningen er innenfor dette formålet. Formålets innhold og omfang vil være bestemmende for hva som bør utvikles (på løsningsnivå/tjenestenivå) for å oppnå formålet. Dette er bakgrunnen for at personvernregelverket legger opp til at dataansvarlig også har myndighet til å bestemme *hvilke midler* som skal benyttes for å oppnå formålet.

Omfanget av dataansvar

Både å bestemme formålet og hvilke midler som skal benyttes er strategiske veivalg for dataansvarlig, fordi det vil påvirke hvor stort omfanget av behandling av person- og helseopplysninger vil bli, hva som skal utvikles, endres eller videreutvikles, og hvordan videreutviklingen, forvaltningen og drift av løsningen skal være. Dette gjelder også *prioritering* av endringer og videreutvikling. Å bestemme hva som skal prioriteres har betydning for behandling av person- og helseopplysninger, og er således en strategisk avgjørelse som naturlig ligger til dataansvaret.

På bakgrunn av ovenstående fremgår det dermed at dataansvarliges rolle til å bestemme formålet og midler for behandlingen innebærer et ytterligere og mer omfattende ansvar som kan oppsummeres som følgende:

- Ansvar for etterlevelse av gjeldende regelverk, standarder, osv.
- Ansvar for informasjonssikkerhet og personvern.
- Ansvar for den faktiske databehandlingen i løsningen.
- Ansvar for anskaffelse, *utvikling*, forvaltning og drift av løsninger.
    - Dette innebærer for eksempel ansvar for taktiske og operasjonelle valg og oppgaver knyttet til løsningen.
- Ansvar for *strategiske valg* som direkte eller indirekte påvirker behandling av person- og helseopplysninger i løsningen.
    - Dette innebærer for eksempel ansvar for *prioritering* av endringer og videreutvikling av løsningen som har betydning for behandling av person- og helseopplysninger.

Med GDPR har dataansvarlig fått flere plikter. I realiteten er disse pliktene oppgaver som må utføres. De sentrale pliktene for den dataansvarlige er knyttet til blant annet:

- Behandlingsgrunnlag
    - sikre rettslig grunnlag (GDPR art. 6 og 9)
    - inngå databehandleravtaler når databehandling tjenesteutsettes (GDPR art. 28)
- Tekniske og organisatoriske tiltak
    - etablere internkontroll (GDPR art. 24)
    - ha løsninger med innebygd personvern og personvern som standardinnstilling (GDPR art. 25)
    - sikre personopplysningssikkerhet (GDPR art. 32)
- Protokoll og vurderinger
    - ha oversikt over behandlingen av person- og helseopplysningene (GDPR art. 30)
    - gjennomføre personvernkonsekvensvurderinger (GDPR art. 35)
    - ha forhåndsdrøftinger med Datatilsynet for løsninger som innebærer høy risiko når de planlagte tiltak fra personvernkonsekvensvurderingen ikke reduserer risikoen (GDPR art. 36)
- Håndtering av brudd på personopplysningssikkerheten
    - underrette Datatilsynet ved brudd på personopplysningssikkerheten (avviksmelding) (GDPR art. 33)
    - melde til den registrerte om brudd på personopplysningssikkerheten der dette er pålagt (GDPR art. 34)
- Ivaretakelse av den registrertes rettigheter, blant annet:
    - gi informasjon til den registrerte (GDPR art. 13 og 14)
    - gi den registrerte innsyn (GDPR art. 15)
    - legge til rette for retting og sletting (GDPR art. 16 og 17)
    - legge til rette for begrensning av behandlingen (GDPR art. 18)
    - legge til rette for dataportabilitet (GDPR art. 21)

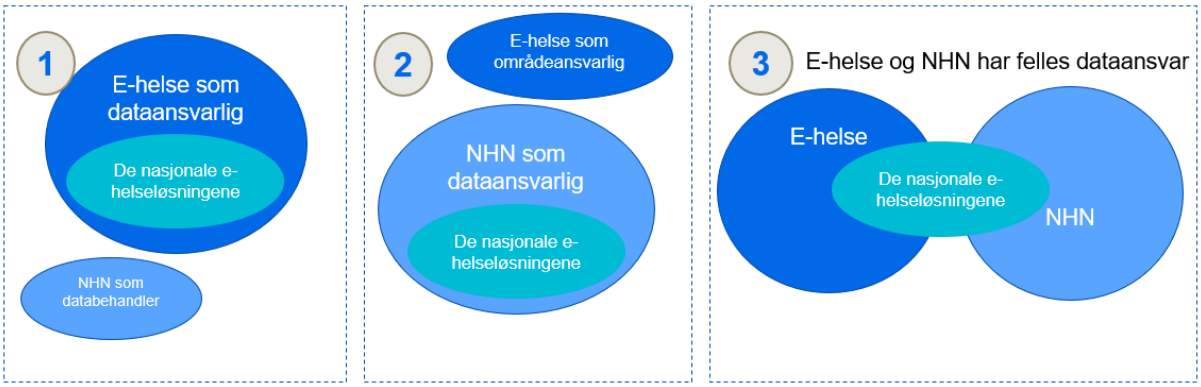
Alt ansvar og plikter beskrevet ovenfor vil i *sin helhet* følge den som har rolle som dataansvarlig.

Modeller for plassering av dataansvar

I denne delen vil det vurderes fordeler og ulemper ved de ulike modellene for plassering av dataansvar som beskrevet nedenfor.

Modeller for plassering av dataansvar som er vurdert:

1. Direktoratet for e-helse som dataansvarlig
2. Ny tjenesteleverandør/NHN som dataansvarlig
3. Direktoratet for e-helse og ny tjenesteleverandør er dataansvarlige sammen (felles dataansvar



Figur: Ulike modeller for plassering av dataansvar

I vurderingen legges det til grunn i alle modellene at dataansvaret ikke kan separeres fra ansvaret for teknisk løsning, fordi ansvar for å bestemme formålet og virkemidler (som f.eks. produktstyring) er tett knyttet til ansvar for å bestemme hvordan behandling av personopplysninger skjer i løsningene i dag. Det vil si hvordan de nasjonale e-helseløsningene er satt opp i dag, er bakgrunnen for hvorfor dataansvaret ikke kan separeres fra ansvaret for teknisk løsning.

Fordeler og ulemper vurderes kun *mellom* modellene. Fordeler og ulemper er ikke uttømmende, men er likevel et forsøk på å gi et helhetsbilde av konsekvensene ved plassering av dataansvar.

Tabell: Fordeler og ulemper angitt i +/-

	Modell 1	Modell 2	Modell 3
Myndighetsrolle			
Premissgiver	- Risiko for blanding av roller	+ Tydeligere rolle for E-helse + E-helse vil ha større avstand til de nasjonale e-helseløsningene, dette kan bidra til mer uavhengighet og nøytralitet i premissgiverrollen	- Risiko for blanding av roller + E-helse vil ha avstand til produksjonsmiljøene for de nasjonale e-helseløsningene, dette kan bidra til mer uavhengighet og nøytralitet i premissgiverrollen

	Modell 1	Modell 2	Modell 3
Fagorgan	- Utredninger, analyser eller anbefalinger kan farges av at E-helse sitter tett på de nasjonale e-helseløsningene - E-helses faglige uavhengighet i andre spørsmål kan bli påvirket av dataansvaret	+ E-helse kan være uavhengig fagorgan	- Utredninger, analyser eller anbefalinger kan farges av at E-helse har felles dataansvar - E-helses faglige uavhengighet i andre spørsmål kan bli påvirket av dataansvaret
Pådriver	+ E-helse kan i større grad bruke erfaring fra utøvelsen av dataansvaret i arbeidet med å være pådriver for personvern og informasjonssikkerhet i sektoren - E-helses prioriteringer vil kunne påvirkes av hvilke spørsmål E-helse selv har mest behov for å adressere som dataansvarlig	+ E-helse kan lettere prioritere arbeidet med å være pådriver for personvern og informasjonssikkerhet i henhold til sektorens totale behov	+ E-helse kan bruke erfaring fra utøvelsen av dataansvaret i arbeidet med å være pådriver for personvern og informasjonssikkerhet i sektoren - E-helses prioriteringer vil kunne påvirkes av hvilke spørsmål E-helse selv har mest behov for å adressere som dataansvarlig
Operasjonelle oppgaver			
Anskaffelse, utvikling, forvaltning og drift	+ Tydelig hvem som skal bestemme: E-helse	+ Tydelig hvem som skal bestemme: NHN	- Må avklares hvem som har ansvar for hva inkl. hvem som har endelig beslutningsmyndighet
(Strategisk) prioritering av utvikling og endringer	+ Tydelig hvem som skal prioritere: E-helse	+ Tydelig hvem som skal prioritere: NHN	- Må avklares hvem som har ansvar for hva inkl. hvem som har endelig beslutningsmyndighet
Løsninger i etableringsfase (mellom utvikling og forvaltning)	+ Tydelig hvem som har beslutningsmyndighet: E-helse	+ Tydelig hvem som har beslutningsmyndighet: NHN	- Må avklares hvem som har ansvar for hva inkl. hvem som har endelig beslutningsmyndighet - Begge virksomheter «eier» risikoen og er ansvarlige (sett fra juridisk ståsted)

	Modell 1	Modell 2	Modell 3
Informasjonsflyt og konsekvenser for ansvar	+ E-helse har tilgang til førstehånds informasjon om alle operasjonelle aktiviteter i de nasjonale e-helseløsningene, dette vil bidra til å ivareta ansvarlighetsprinsippet etter GDPR	+ NHN har tilgang til førstehånds informasjon om alle operasjonelle aktiviteter i de nasjonale e-helseløsningene, dette vil bidra til å ivareta ansvarlighetsprinsippet etter GDPR	- Risiko for at E-helse ikke får tilstrekkelig informasjon om operasjonelle aktiviteter i de nasjonale e-helseløsningene, men er likevel solidarisk ansvarlige - Manglende informasjon kan gjøre det utfordrende å ivareta ansvarlighetsprinsippet etter GDPR
Kompetanse			
Kompetanse	+ E-helse har nødvendig kompetanse til å ivareta dataansvaret	+ Forutsatt at nødvendig kompetanse følger med ved flytting av dataansvaret til NHN, sikres det tilstrekkelig kompetanse i NHN til å ivareta dataansvaret - Dersom nødvendig kompetanse ikke følger med ved flytting av dataansvaret til NHN, må det bygges kompetanse i NHN for ivareta dataansvaret	- Vil være behov for å sikre tilstrekkelig kompetanse i begge virksomheter, dette kan gi behov for duplisering av kompetanse - Vil kreve samarbeid og koordinering mellom ressurser i begge virksomheter
Personvern			
Ivaretakelse av personvern og informasjonssikkerhet i rollen som dataansvarlig	+ Kun én virksomhet er ansvarlig	+ Kun én virksomhet er ansvarlig	- Begge virksomheter blir ansvarlige for personvern og informasjonssikkerhet i den samme behandlingen, dette kan innebære mer prosess, dokumentasjon begge steder, mulig duplisering av oppgaver mv.
Fastsettelse av formål og virkemidler	+ Kun én virksomhet er ansvarlig	+ Kun én virksomhet er ansvarlig	- Begge virksomheter blir ansvarlige, det må avklares hvem som har

	Modell 1	Modell 2	Modell 3
			endelig beslutningsmyndighet
Erstatningsansvar etter GDPR	+ Kun én virksomhet blir erstatningsansvarlig	+ Kun én virksomhet blir erstatningsansvarlig	- Begge virksomheter blir erstatningsansvarlige
Risiko for sanksjoner for dataansvarlig etter GDPR	+ Bøter ilegges kun én virksomhet	+ Bøter ilegges kun én virksomhet	- Bøter kan ilegges begge virksomheter
Innbyggers rettigheter	+ Mer oversiktlig for innbygger + Ett sted for innbyggerhenvendelser	+ Mer oversiktlig for innbygger + Ett sted for innbyggerhenvendelser	- Kan være uoversiktlig for innbygger - Innbygger må kunne henvende seg til begge virksomheter, dette vil føre til behov for mottak av innbyggerhenvendelser to steder
Databehandleravtaler	+ Kun én virksomhet er part i databehandleravtalene som dataansvarlig	+ Kun én virksomhet er part i databehandleravtalene som dataansvarlig	- Kan føre til at begge virksomheter sammen blir part i databehandleravtaler som dataansvarlig - Avtaleforholdene vil kreve mer koordinering og jevnlig oppfølging fra begge virksomheter
Avvikshåndtering	+ Har egen rutine for avvikshåndtering	+ Har egen rutine for avvikshåndtering	- Vil kreve koordinering og samkjøring av rutiner for avvik - Ved avvik som må meldes til Datatilsynet innen 72 timer, vil det kreves tett samarbeid mellom virksomhetene
Innebygd personvern	+ Én virksomhet bestemmer hvordan kravet skal omsettes i praksis	+ Én virksomhet bestemmer hvordan kravet skal omsettes i praksis	- Begge virksomheter blir ansvarlige for å oppfylle kravet, det må avklares hvem som har endelig beslutningsmyndighet når kravet skal omsettes i praksis
Internkontroll, policy, retningslinjer, standarder mv.	+ Kun én virksomhet er ansvarlig	+ Kun én virksomhet er ansvarlig	- Begge virksomheter blir ansvarlige, det må avklares hvem som har

	Modell 1	Modell 2	Modell 3
			endelig beslutningsmyndighet - Vil kreve mer koordinering mellom virksomhetene
Protokoller for behandling av person- og helseopplysninger	+ Har egen protokoll for egne behandlinger	+ Har egen protokoll for egne behandlinger	- De samme behandlingene må protokollføres i begge virksomheter - Vedlikehold av protokoll må skje fortløpende i begge virksomheter
Personvernkonsekvensutredninger (DPIA) og forhåndsdrøftinger med Datatilsynet	+ Kun én virksomhet er ansvarlig + Ledelsesforankring i kun én virksomhet	+ Kun én virksomhet er ansvarlig + Ledelsesforankring i kun én virksomhet	- Begge virksomheter blir ansvarlige for gjennomføring, dette betyr mer prosess - Ledelsesforankring i begge virksomheter
Personvernombudet			
Personvernombudet (PVO)	+ Rollen er etablert som 100% stilling i E-helse i dag	+ Rollen er etablert i NHN, men uten fastsatt prosentandel i dag (PVO har andre oppgaver i tillegg)	- Videreføring av to PVOer vil kreve koordinering - Det kan være behov for å vurdere om det bør utpekes kun ett PVO for de nasjonale e-helseløsningene. Dersom NHNs PVO utpekes, vil det ha konsekvenser for E-helses PVOs rolle, stillingsbeskrivelse mv. og omvendt
Regelverk og etterlevelse			
Ansvar for etterlevelse av personvernlovgivningen for behandling i de nasjonale e-helseløsningene	+ Kun én virksomhet er ansvarlig	+ Kun én virksomhet er ansvarlig	- Begge virksomheter er sammen ansvarlige og begge virksomheter må følge opp etterlevelse i anskaffelser, utvikling, forvaltning og drift, dette vil kreve ressurser og

	Modell 1	Modell 2	Modell 3
			kompetanse begge steder
Statsforetakslovens begrensninger i statens styring av foretaket jf. statsforetaksloven §38	+ Ingen problem iht. statsforetaksloven §38	+ Ingen problem iht. statsforetaksloven §38	- Dersom det besluttes at NHN overtar det totale operasjonelle ansvaret for de nasjonale e-helseløsningene, kan valg av felles dataansvar medføre en risiko for at E-helse detaljstyrer NHN på en måte som kan være i strid med statsforetaksloven §38 og beste praksis for statlig styring av statseide virksomheter, ref. prinsipp om mål og resultatstyring
Behov for endringer i kjernejournalforskriften og reseptformidlerforskriften	+ Ingen behov for endring	- Behov for endring: dataansvar legges til en ny virksomhet (NHN)	- Behov for endring: NHN utpekes som felles dataansvarlig (i tillegg til E-helse) – det må avklares med HOD om dette er mulig i det hele tatt da dette endrer grunnleggende forutsetninger i forskriftene
Videreføring av dagens ordning der E-helse har fortolkningsansvar for kjernejournalforskriften og reseptformidlerforskriften (ansvaret kan ikke flyttes til NHN)	- Fortolkning kan farges av at E-helse sitter tett på Kjernejournal og e-resept	+ E-helses fortolkning vil kunne bli mer uavhengig og nøytral	- Fortolkning kan farges av at E-helse sitter tett på Kjernejournal og e-resept

På bakgrunn av tabellen ovenfor fremgår det at:

- Modell 1 og Modell 3 kan blant annet føre til at direktoratet myndighetsrolle (premissgiver, fagorgan og pådriver) ikke blir tilstrekkelig uavhengig og nøytral
- Modell 1 (dagens ordning) vil videreføre de samme utfordringene med risiko for blant annet blanding av roller
- Modell 3 kan føre til at det kreves mer prosess, dokumentasjon i begge virksomheter, mulig duplisering av oppgaver mv.

Tabellen viser også at plassering av dataansvar i én virksomhet vil blant annet bidra til at utførelsen av oppgaver og plikter blir mindre utfordrende, gi en mer helhetlig tilnærming til de nasjonale e-helseløsningene (utvikling, endringer, forvaltning, drift osv.), samt bidra til bedre ivaretakelse av innbyggers rettigheter.

Felles dataansvar vil blant annet kunne føre til uklarhet rundt roller og ansvarsfordeling, medføre stor grad av *kontinuerlig* koordinering og samarbeid, samt eventuelt behov for duplisering av kompetanse.

Forslag til plassering av dataansvar

Som nevnt tidligere bør *ikke* en plassering av dataansvar medføre en deling av dataansvaret for den samme behandling av person- og helseopplysninger. En ordning der fordeling av oppgaver og ansvar mellom to virksomheter som i prinsippet innebærer en deling av dataansvaret for den samme behandlingen, vil lett tolkes som et felles dataansvar etter GDPR. Dette særlig fordi det ikke kreves en avtale om felles dataansvar (i motsetning til krav til avtale mellom dataansvarlig og databehandler). Det vil si at terskelen for å tolke en ordning til å være felles dataansvar vil være lav.

Den europeiske unions domstol (Court of Justice of the European Union – CJEU) er kjent for å praktisere en vid tolkning når det gjelder felles dataansvar, både før og etter GDPR trådte i kraft. I de to sakene som ble besluttet i 2018[7], fastslo CJEU at en fysisk eller juridisk person som utøver *innflytelse* på behandling av personopplysninger, til eget formål, og som på bakgrunn av dette (innflytelse), deltar i fastsettelsen av formålene og midlene til behandlingen, betraktes som en dataansvarlig.[8]

En formalisert modell der Direktoratet 2.0 har *innflytelse* eller skal bestemme *i detalj* over hvilke tjenester som skal utvikles eller endres av ny tjenesteleverandør i de nasjonale e-helseløsningene, kan være nok til å fastslå at Direktoratet 2.0 og ny tjenesteleverandør bestemmer formålet og midler i fellesskap. En ordning med felles dataansvar mellom Direktoratet 2.0 og ny tjenesteleverandør vil stille krav til at det er tilgjengelige ressurser i begge virksomhetene med fagkompetanse på flere områder for hver av løsningene. En slik ordning kan også skape usikkerhet overfor innbyggere om hvem som er ansvarlig for hva. Selv om innbygger kan henvende seg til begge dataansvarlige, vil dette kunne påvirke tilliten til løsningene.

For å unngå felles dataansvar mellom Direktoratet 2.0 og ny tjenesteleverandør, bør dataansvaret for de nasjonale e-helseløsningene (Kjernejournal, e-resept, Helsenorge og Grunndata) derfor plasseres *samlet og i sin helhet* i den nye tjenesteleverandøren.

Plassering av dataansvar for løsninger regulert i forskrift

Direktoratet for e-helse er tildelt rollen som dataansvarlig for Nasjonal kjernejournal og Reseptformidleren (e-resept) etter henholdsvis kjernejournalforskriften og reseptformidlerforskriften.

---

[7] Se CJEU C-210/16 *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH* (5.6.2018) og CJEU *C-25/17. Tietosuojavaltuutettu v Jehovan todistajat — uskonnollinen yhdyskunta* (10.7.2018).

[8] Se også CJEU C-131/12. Google Spain SL, Google. Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González (13.5.2014).

En plassering av dataansvar for disse to løsningene i den nye tjenesteleverandøren vil kreve endringer i de to nevnte forskriftene.

Plassering av dataansvar for løsninger som ikke er regulert i forskrift

I motsetning til kjernejournal og e-resept, er dataansvaret på Helsenorge og Grunndata ikke regulert i lov eller forskrift.

Helsenorge

Dataansvaret på Helsenorge er i dag plassert i flere virksomheter. Helsenorge består av 5 felleskomponenter og cirka 30 tjenester i drift per januar 2019 som sammen muliggjør digitaliserte helsetjenester overfor helse- og omsorgssektoren. Direktoratet for e-helse er dataansvarlig for helsenorgeplattformen, felleskomponentene og flere av tjenestene. For de øvrige tjenestene er det virksomheter i sektoren som er dataansvarlige.

Når dataansvar for Helsenorge plasseres i ny tjenesteleverandør vil dette si at ny tjenesteleverandør trer inn som dataansvarlig etter direktoratet, og vil overta oppgaver og plikter som medfølger dataansvaret. Gjeldende databehandleravtaler som regulerer forholdet mellom direktoratet og virksomheter som benytter seg av helsenorgeplattformen vil måtte endres tilsvarende. I tillegg vil alle tjenesteavtaler måtte endres i henhold til den nye plasseringen av dataansvar.

Grunndata

Grunndata består i dag av grunndataplattformen, 6 registre med personopplysninger og 3 registre uten personopplysninger. Direktoratet er per nå dataansvarlig for grunndataplattformen og 2 registre med personopplysninger (Adresseregisteret og Oppføringsregisteret).

Ved ny plassering av dataansvaret kan ny tjenesteleverandør, på samme måte som i Helsenorge, tre inn som dataansvarlig etter direktoratet. De aktuelle databehandleravtaler og tjenesteavtaler må i så fall endres.

Behov for regelverksutvikling

Plassering av dataansvar er ofte svært utfordrende både for Helsenorge og Grunndata. For Helsenorge kreves det ofte en omfattende prosess før dataansvar kan plasseres. Dette skyldes blant annet at virksomhetene i sektoren ikke har kontroll over den faktiske behandlingen i deres tjenester som skjer på helsenorgeplattformen, og det har derfor ikke vært naturlig for virksomhetene å påta seg dataansvaret for denne delen behandlingen. Ny plassering av dataansvar til tjenesteleverandør vil ikke løse denne utfordringen.

Direktoratet mener derfor at det er viktig å sikre at ny tjenesteleverandør har nødvendige virkemidler til å utføre rollen som dataansvarlig.

Direktoratet har i dag en rolle både som dataansvarlig og databehandler på Helsenorge avhengig av hvilken tjeneste det er snakk om. På sikt er det grunn til å tro at det er hensiktsmessig å regulere dataansvar på Helsenorge i lov eller forskrift.

En modell for å regulere dataansvaret på Helsenorge, er at det kun fastsettes *kriterier* for utpeking av dataansvarlig, men ikke nødvendigvis *hvem* som skal ha dataansvar. Denne modellen for plassering av dataansvar er sjelden brukt, men GDPR gir rom for en slik regulering av dataansvaret.[9]

Modellen vil fortsatt kreve en konkret vurdering av oppfyllelsen av kriteriene og de reelle forholdene for å fastsette hvem som faktisk vil bli dataansvarlig. Likevel vil modellen gi mer sikkerhet i plasseringen av dataansvar enn dagens situasjon, og vil bidra til å tydeliggjøre ansvarsforholdene på Helsenorge.

Denne modellen for å plassere dataansvar vil i fremtiden også kunne være hensiktsmessig for Grunndata når produktet har kommet lenger i sin utvikling av plattformen og tilknyttede tjenester.

Uavhengig av om det vil bli regulering eller ikke for Helsenorge og Grunndata, vil det være nødvendig å sørge for at ny tjenesteleverandør *som ikke er et forvaltningsorgan (med myndighet)* kan møte dagens utfordringer og i tillegg er rustet til å håndtere kompleksiteten i en fremtidig plattform med voksende antall tjenester.

[9] Se definisjon av behandlingsansvarlig i GDPR art. 4 (7): *"en fysisk eller juridisk person, en offentlig myndighet, en institusjon eller ethvert annet organ som alene eller sammen med andre bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes; når formålet med og midlene for behandlingen er fastsatt i unionsretten eller i medlemsstatenes nasjonale rett, kan den behandlingsansvarlige, eller de særlige kriteriene for utpeking av vedkommende, fastsettes i unionsretten eller i medlemsstatenes nasjonale rett"*