Direktoratet for e-helse

Helsedataprogrammet

Programstyremøte 15. desember 2021

Agenda

	Tema	
1	**Velkommen**	**Jon Helge**
2	Godkjenning av referat fra forrige møte	Jon Helge
3	Beslutning om Helseanalyseplattformen	Håvard
4	Juridiske spørsmål og vurderinger	Randi
5	Forslag til prioriterte oppgaver i ny plan for det videre arbeidet med Helsedataservice og Helseanalyseplattformen	Marianne
6	Kommunikasjon	Håvard
7	Takk for i år	Jon Helge og Håvard

Agenda

	Tema	
1	Velkommen	Jon Helge
2	**Godkjenning av referat fra forrige møte**	**Jon Helge**
3	Beslutning om Helseanalyseplattformen	Håvard
4	Juridiske spørsmål og vurderinger	Randi
5	Forslag til prioriterte oppgaver i ny plan for det videre arbeidet med Helsedataservice og Helseanalyseplattformen	Marianne
6	Kommunikasjon	Håvard
7	Takk for i år	Jon Helge og Håvard

Agenda

	Tema	
1	Velkommen	Jon Helge
2	Godkjenning av referat fra forrige møte	Jon Helge
3	**Beslutning om Helseanalyseplattformen**	**Håvard**
4	Juridiske spørsmål og vurderinger	Randi
5	Forslag til prioriterte oppgaver i ny plan for det videre arbeidet med Helsedataservice og Helseanalyseplattformen	Marianne
6	Kommunikasjon	Håvard
7	Takk for i år	Jon Helge og Håvard

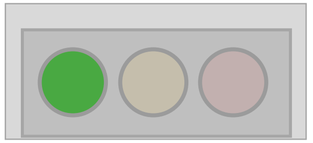
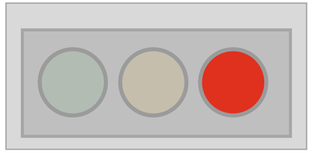
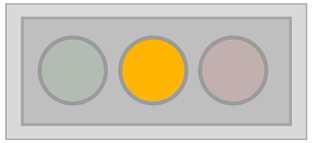
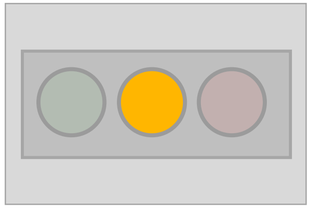
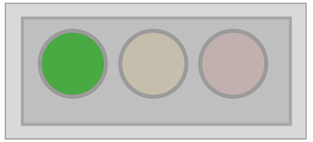
Arbeidet med å realisere HAP i MS Azure må settes på vent

På grunnlag av en samlet risikovurdering av etablering av Helseanalyseplattformen i MS Azure har Direktoratet for e-helse vurdert at det i nåværende situasjon er for stor risiko til å gå videre med en plan om å ha personsensitive data på Helseanalyseplattformen i allmenn sky fra en amerikansk leverandør fra 1. april 2022. Av hensyn til juridisk risiko, omdømmerisiko og behov for kostnadskontroll må den videre utviklingen av data- og analysetjenestene settes på vent til det blir avklart om det kan skje endringer med de forholdene som er utenfor vår kontroll. Samtidig er det usikkert om og eventuelt når det vil la seg løse. Det er derfor behov for å vurdere nærmere om data- og analysetjenestene kan realiseres på andre måter enn i en amerikansk allmenn skyløsning.

Målet med satsningen står fast. Det skal fortsatt bli enklere og raskere å få tilgang til helsedata for analyse og annen sekundærbruk for viktige, samfunnsnyttige formål.

Det at utviklingen av data- og analysetjenester settes på vent, betyr ikke at alt arbeid med løsninger fra Helsedataprogrammet stopper opp. Programmet foreslår budsjett og plan for det videre arbeidet i 2022 der arbeidet med søknads- og saksbehandlingstjenester og den videre etableringen av Helsedataservice fortsetter, og der midler må omdisponeres fra utvikling til utredning av alternative løsninger for data- og analysetjenestene.

Konsekvens av beslutningen

Leveranse	Status og konsekvens	Prioritet
Søknads- og saksbehandlingstjenester	▪ Helsedata.no med variabelutforsker og Felles søknadsskjema er i bruk og påvirkes ikke. ▪ Felles saksbehandlingsløsning er under utprøvning, tas i bruk i januar 2022, og påvirkes ikke. Datakilder fra flere registerforvaltere kan også innlemmes i løsningen.	
Data- og analysetjenester	▪ Datamottak og dataplattform er utviklet og testet, men settes ikke i produksjon. ▪ Datatilrettelegging og utlevering er straks utviklet ferdig, testes minimalt, og tas ikke i bruk. ▪ Kohortutforsker startes det ikke utviklingsarbeid på nå. ▪ For analyserom bør mulig bruksområde for eksisterende infrastruktur kartlegges.	
Informasjonsforvaltning og integrasjonstjenester	▪ Metadataløsning leveres uavhengig av data- og analysetjenester, og arbeidet kan fortsette. ▪ Datamodell for dataprodukt er løsningsuavhengig, kan tas opp igjen ved ny start av utvikling. ▪ Integrasjonsløsning er løsningsspesifikk, har begrenset nytteverdi utenfor Azure-domenet.	
Helsedataservice	▪ Felles søknadsmottak er etablert. HDS kan overta veiledning og saksbehandling. ▪ HDS kan ikke overta vedtaksmyndighet uten data på HAP, uten justering av regelverk. Det bør vurderes å justere regelverk, slik at HDS kan få vedtaksmyndighet og overta saksbehandling og utlevering for registerforvalterne.	
Alternativvurdering (Ny)	▪ Vurdere om og hvordan data- og analysetjenestene kan realiseres i annen teknologi.	

Agenda

	Tema	
1	Velkommen	Jon Helge
2	Godkjenning av referat fra forrige møte	Jon Helge
3	Beslutning om Helseanalyseplattformen	Håvard
4	**Juridiske spørsmål og vurderinger**	**Randi**
5	Forslag til prioriterte oppgaver i ny plan for det videre arbeidet med Helsedataservice og Helseanalyseplattformen	Marianne
6	Kommunikasjon	Håvard
7	Takk for i år	Jon Helge og Håvard

Innledning – Juridiske spørsmål og vurderinger

1) Tema for de juridiske spørsmålene og vurderingene

2) Bakgrunn for vurderingene
- Standardvilkårene til Microsoft
- Schrems II
  - Amerikanske overvåkingslover
- Nye opplysninger om tekniske tiltak og hensiktsmessig bruk av disse

3) Juridisk spørsmål og rettslig grunnlag for vurderingene

4) Overordnet om de juridiske vurderingene

5) Juridiske- og informasjonssikkerhetsvurderinger ved anskaffelsen vs vurderinger per nå

Tema for de juridiske spørsmålene og vurderingene

- Beskyttelse mot leverandør Microsoft inkludert deres rettslige forpliktelser etter amerikansk rett
- Personvernforordningen og helseregisterloven
- Vurderinger av bestemmelser i avtalen (Microsofts standardvilkår for behandling av personopplysninger/DPA) som gjelder
  - 1) Overføringer som gjøres på vegne av direktoratet
  - 2) Overføringer som Microsoft gjør på eget initiativ
  - 3) Microsoft bruk av opplysninger til egne formål inkludert deres rettslige forpliktelser
- Vurderinger av Schrems II dommen
- Tekniske sikkerhetstiltak – vurdering av effekt og mulig bruk av disse

Standardvilkår fra Microsoft – overføring og utlevering

- Direktoratet instruerer Microsoft til å overføre personopplysninger til tredjeland gjennom bruk av tjenester fra Microsoft (lagrer på server i Norge)

- Microsoft vil behandle «customer data» for å ivareta «business operations» - Microsofts egne formål
  - Microsoft er etter avtalen behandlingsansvaret for dette

  - «Customer data» er definert i Avtalen til å også omfatte personopplysninger som kunden legger inn i tjenesten

Forts. standardvilkår fra Microsoft – overføring og utlevering

- «Business operations”:

  “*For purposes of this DPA, “business operations” consist of the following, each as incident to delivery of the Products and Services to Customer: (1) billing and account management; (2) compensation (e.g., calculating employee commissions and partner incentives); (3) internal reporting and business modeling (e.g., forecasting, revenue, capacity planning, product strategy); (4) combatting fraud, cybercrime, or cyber-attacks that may affect Microsoft or Microsoft Products; (5) improving the core functionality of accessibility, privacy or energy-efficiency; and (6) financial reporting and compliance with legal obligations (subject to the limitations on disclosure of Processed Data outlined below)” .*

Schrems II dommen

- 16. juli 2020 (etter anskaffelsen av Helseanalyseplattformen var avsluttet)
- Privacy Shield er ugyldig som overføringsgrunnlag til USA siden den ikke gir et tilstrekkelig beskyttelsesnivå
- Andre overføringsgrunnlag kan benyttes, men da sammen med ytterligere tekniske og organisatoriske tiltak for at opplysningene skal gis et vern som tilsvarer det vernet opplysningene gis etter europeisk lovgivning.
- Tiltakene skal blant annen hindre at amerikanske myndigheter henter inn personopplysninger i samsvar med deres nasjonale etterretningslovgivning
  - FISA 702 (Oppsummert: alle amerikanske selskaper, selv om data er lagret utenfor USA, må levere ut data på forespørsel til amerikansk etterretning. Uklart omfang, og om dataansvarlig får beskjed.)

Juridisk spørsmål og rettslig grunnlag for vurderingene

1) Overføres det personopplysninger til tredjeland uten tilstrekkelige sikkerhetstiltak?
Rettslig grunnlag: personvernforordningen kap. 5 og de vilkårene som følger av Schrems II-dommen.

2) Leverer direktoratet ulovlig ut personopplysninger til Microsoft?

Rettslig grunnlag: personvernforordningen art. 6 og 9, og taushetsplikt etter helseregisterloven § 17 jf. helsepersonelloven §§ 21 flg.

3) Er databehandleravtalen med Microsoft mangelfull?

Rettslig grunnlag: personvernforordningen art. 28 nr. 3 a)

Det er vurdert om tekniske tiltak kan hindre ulovlig utlevering og overføring.

1. Overføres det personopplysninger til tredjeland uten tilstrekkelige sikkerhetstiltak?

Direktoratet mener at kapittel 5 og Schrems-doktrinen bare gjelder når Microsoft overfører opplysninger på vegne av direktoratet. Dette betyr at:

Overføringer som gjøres på vegne av direktoratet

- Direktoratet er ansvarlig for å påse at det finnes overføringsgrunnlag
  - Overføringene er vurdert å være i samsvar med personvernforordningens vilkår jf. også Schrems II

Overføringer som Microsoft gjør på eget initiativ

- Microsoft er ansvarlig for å påse at det finnes overføringsgrunnlag,
  - Direktoratet må likevel etablere sikkerhetstiltak for å hindre slik overføring jf. Artikkel 32

2. Leverer direktoratet ulovlig ut personopplysninger til Microsoft?

- Datatansvarlig må ha rettslig grunnlag for utleveringen etter art. 6, og for særskilte kategorier av personopplysninger må i tillegg et av vilkårene i art. 9 nr. 2 flg. være oppfylt.

- Taushetsplikt for helseopplysninger etter helseregisterloven § 17 jf. helsepersonelloven § 21

- Direktoratet tillater i databehandleravtalen at Microsoft bruker personopplysningene for å ivareta sine «Business operations». Dette kan likestilles med en utlevering mellom to behandlingsansvarlige.

- Tekniske tiltak kan innebære at det ikke kan skje en utlevering til Microsoft.
  - Hva vil i så fall være tilstrekkelige tekniske tiltak? Er det i så fall mulig å benytte disse på en slik måte at direktoratet kan utføre oppgaver med saksbehandling etc.?

3. Er databehandleravtalen med Microsoft mangelfull?

Art. 28 pålegger den behandlingsansvarlige visse plikter ved bruk av databehandlere. Blant annet:

- Plikt for til å påse at databehandler gir

«tilstrekkelige garantier for at de vil gjennomføre egnede tekniske og organisatoriske tiltak som sikrer at behandlingen oppfyller kravene i personvernforordningen og vern av den registrertes rettigheter». (art. 28 nr. 1)

- Skriftlig databehandleravtale

- art. 28 nr. 3 første ledd bokstav a) til h) oppstiller ufravikelige krav til hva en databehandleravtale skal og kan inneholde.
  - bokstav a) som er relevant. Her heter det at databehandleravtalen skal angi at databehandleren

    «***behandler personopplysningene bare på dokumenterte instrukser fra den behandlingsansvarlige,*** *herunder med hensyn til overføring av personopplysninger til en tredjestat eller en internasjonal organisasjon, med mindre det kreves i henhold til unionsretten eller medlemsstatenes nasjonale rett som databehandleren er underlagt; i så fall skal databehandleren underrette den behandlingsansvarlige om nevnte rettslige krav før behandlingen, men mindre denne rett av hensyn til viktige allmenne interesser forbyr en slik underretning»*,

.

Oppsummering av vurderingene

1) Lav juridisk risiko for at det vil være en overføring til Tredjeland som direktoratet vil være dataansvarlig for.

2) Den mest alvorlige juridiske risikoen er at det kan bli utlevert helse- og personopplysninger til Microsoft.

- Avhenger mye av effekten av tekniske sikkerhetstiltak

3) Juridisk risiko for at databehandleravtalen kan bli vurdert som mangelfull

Vurderinger ved anskaffelsen vs vurderinger per nå

Vurderinger ved anskaffelsen

- Risikoen for utlevering av personopplysninger til Microsoft, og for overføring av personopplysninger til tredjeland, ble vurdert som akseptabel i forbindelse med anskaffelsen og avtaleinngåelsen i 2020.
- Tekniske sikkerhetstiltak skulle forhindre at Microsoft faktisk kunne behandle personopplysningene for egne formål og overføre dem til tredjeland.

Vurderinger per nå

- Planlagte tekniske sikkerhetstiltak virker ikke som tiltenkt
- Usikkerhet om effekten av nye tekniske sikkerhetstiltak
- Helseopplysninger kan ikke alltid krypteres med egne nøkler når data er under behandling i analyserommet

Agenda

	Tema	
1	Velkommen	Jon Helge
2	Godkjenning av referat fra forrige møte	Jon Helge
3	Beslutning om Helseanalyseplattformen	Håvard
4	Juridiske spørsmål og vurderinger	Randi
5	**Forslag til prioriterte oppgaver i ny plan for det videre arbeidet med Helsedataservice og Helseanalyseplattformen**	**Marianne**
6	Kommunikasjon	Håvard
7	Takk for i år	Jon Helge og Håvard

Forslag til prioriterte oppgaver i 2022

- Fortsetter videre utvikling av helsedata.no med variabelutforsker og felles søknadsskjema. Flere datakilder innlemmes.
- Metadataarbeidet fortsetter.
- Felles saksbehandlingssystem tas i bruk.
  Flere registerforvaltere kan innlemmes i løsningen.
- Felles søknadsmottak er etablert. Helsedataservice kan overta veiledning og saksbehandling.
- Regelverk bør justeres, slik at Helsedataservice kan få vedtaksmyndighet og overta saksbehandling og utlevering for registerforvalterne, uten data på felles plattform.
- Ferdigstiller løsning for datatilrettelegging og utlevering, men uten å gå i produksjon
- Det må gjøres en alternativvurdering, der det vurderes om og hvordan data- og analysetjenester kan realiseres i en annen teknologi.

Agenda

	Tema	
1	Velkommen	Jon Helge
2	Godkjenning av referat fra forrige møte	Jon Helge
3	Beslutning om Helseanalyseplattformen	Håvard
4	Juridiske spørsmål og vurderinger	Randi
5	Forslag til prioriterte oppgaver i ny plan for det videre arbeidet med Helsedataservice og Helseanalyseplattformen	Marianne
6	**Kommunikasjon**	**Håvard**
7	Takk for i år	Jon Helge og Håvard

Kommunikasjon

Saken blir offentliggjort onsdag 15. desember

Overordnete grep i kommunikasjonen

- Ærlig og tydelig på kompleksitet og vanskelig beslutning/dilemma
- Juridisk risiko er hovedbegrunnelse for pause/re-planlegging
- Fremheving av verdiskaping uavhengig av Sky-spørsmålet
- Det at vi pauser betyr ikke at arbeid som er gjort til nå er forgjeves: fortsatt verdiskaping
- Innhente støtte fra fagmiljøet, samarbeidspartnere og interessenter

Hovedbudskap og tiltak

- Kort redegjørelse beslutning: hovedbudskap/nyhetssak på ehelse.no
- Spørsmål/svar-batteri i beredskap til bruk for ledelse og talspersoner

Etterlatt inntrykk

- Åpenhet om kompleksitet og dilemma
- Verne norske helsedata
- Vi fortsetter å skape verdi og jobbe med nytte av satsingen

Forslag til vedtak

Programstyret gir sin tilslutning til forslag til overordnet plan for det videre arbeidet med ulike tjenester knyttet til Helsedataservice, søknads- og saksbehandlingstjenester og data- og analysetjenester. Innspill fra programstyret blir tatt med i det videre arbeidet med plan og oppfølging.

Agenda

	Tema	
1	Velkommen	Jon Helge
2	Godkjenning av referat fra forrige møte	Jon Helge
3	Beslutning om Helseanalyseplattformen	Håvard
4	Juridiske spørsmål og vurderinger	Randi
5	Forslag til prioriterte oppgaver i ny plan for det videre arbeidet med Helsedataservice og Helseanalyseplattformen	Marianne
6	Kommunikasjon	Håvard
7	**Takk for i år**	**Jon Helge og Håvard**

Status operasjonalisering av forenklet styringsmodell i en overgangsperiode

Programstyret

Referanse-gruppen

Felles styringsråd

Programstyret og referansegruppen slås sammen og komprimeres

Representasjon: Én representant per virksomhet

- Alle virksomheter som har deltatt i RF og PGS blir med videre. Deltagere avklart
- Møteinnkalling til møter i 2022 sendes ut ila 2021

Arbeidsgruppe forskning

Arbeidsgruppe innovasjon og næringsutvikling

Felles arbeidsgruppe

Arbeidsgruppe (AG) forskning og AG innovasjon og næringsliv videreføres i en forenklet modell

Representasjon: Deltakerne i AG forskning og AG innovasjon og næringsutvikling fortsetter i en felles arbeidsgruppe

- Kristian Hveem (leder AGF) og Monica Larsen (leder AGI&N) leder i fellesskap
- Alle deltagere i dagens arbeidsgrupper blir med videre

Direktoratet for e-helse

Direktoratet for e-helse

ekstra

Artikkel 5 Prinsipper for behandling av personopplysninger

1. Personopplysninger skal

a) behandles på en lovlig, rettferdig og åpen måte med hensyn til den registrerte («lovlighet, rettferdighet og åpenhet»),

b) samles inn for spesifikke, uttrykkelig angitte og berettigede formål og ikke viderebehandles på en måte som er uforenlig med disse formålene; viderebehandling for arkivformål i allmennhetens interesse, for formål knyttet til vitenskapelig eller historisk forskning eller for statistiske formål skal, i samsvar med artikkel 89 nr. 1, ikke anses som uforenlig med de opprinnelige formålene («formålsbegrensning»),

c) være adekvate, relevante og begrenset til det som er nødvendig for formålene de behandles for («dataminimering»),

d) Være korrekte og om nødvendig oppdaterte; det må treffes ethvert rimelig tiltak for å sikre at personopplysninger som er uriktige med hensyn til formålene de behandles for, uten opphold slettes eller rettes («riktighet»),

e) lagres slik at det ikke er mulig å identifisere de registrerte i lengre perioder enn det som er nødvendig for formålene som personopplysningene behandles for; personopplysninger kan lagres i lengre perioder dersom de utelukkende vil bli behandlet for arkivformål i allmennhetens interesse, for formål knyttet til vitenskapelig eller historisk forskning eller for statistiske formål i samsvar med artikkel 89 nr. 1, forutsatt at det gjennomføres egnede tekniske og organisatoriske tiltak som kreves i henhold til denne forordning for å sikre de registrertes rettigheter og friheter («lagringsbegrensning»),

f) behandles på en måte som sikrer tilstrekkelig sikkerhet for personopplysningene, herunder vern mot uautorisert eller ulovlig behandling og mot utilsiktet tap, ødeleggelse eller skade, ved bruk av egnede tekniske eller organisatoriske tiltak («integritet og konfidensialitet»).

2. Den behandlingsansvarlige er ansvarlig for og skal kunne påvise at nr. 1 overholdes («ansvar).

Artikkel 6 Behandlingens lovlighet

1. Behandlingen er bare lovlig dersom og i den grad minst ett av følgende vilkår er oppfylt:

a) den registrerte har samtykket til behandling av sine personopplysninger for ett eller flere spesifikke formål,

b) behandlingen er nødvendig for å oppfylle en avtale som den registrerte er part i, eller for å gjennomføre tiltak på den registrertes anmodning før en avtaleinngåelse,

c) behandlingen er nødvendig for å oppfylle en rettslig forpliktelse som påhviler den behandlingsansvarlige,

d) behandlingen er nødvendig for å verne den registrertes eller en annen fysisk persons vitale interesser,

e) behandlingen er nødvendig for å utføre en oppgave i allmennhetens interesse eller utøve offentlig myndighet som den behandlingsansvarlige er pålagt,

f) behandlingen er nødvendig for formål knyttet til de berettigede interessene som forfølges av den behandlingsansvarlige eller en tredjepart, med mindre den registrertes interesser eller grunnleggende rettigheter og friheter går foran og krever vern av personopplysninger, særlig dersom den registrerte er et barn.

Nr. 1 bokstav f) får ikke anvendelse på behandling som utføres av offentlige myndigheter som ledd i utførelsen av deres oppgaver.

2. Medlemsstatene kan opprettholde eller innføre mer spesifikke bestemmelser for å tilpasse anvendelsen av reglene for behandling i denne forordning med henblikk på å sikre samsvar med nr. 1 bokstav c) og e) ved nærmere å fastsette mer spesifikke krav til behandlingen samt andre tiltak som har som mål å sikre en lovlig og rettferdig behandling, herunder i forbindelse med andre særlige behandlingssituasjoner som nevnt i kapittel IX.

3. Grunnlaget for behandlingen nevnt i nr. 1 bokstav c) og e) skal fastsettes i

a) unionsretten eller

b) medlemsstatens nasjonale rett som den behandlingsansvarlige er underlagt.

Formålet med behandlingen skal være fastsatt i nevnte rettslige grunnlag eller, når det gjelder behandlingen nevnt i nr. 1 bokstav e), være nødvendig for å utføre en oppgave i allmennhetens interesse eller utøve offentlig myndighet som den behandlingsansvarlige er pålagt. Nevnte rettslige grunnlag kan inneholde særlige bestemmelser for å tilpasse anvendelsen av reglene i denne forordning, blant annet de generelle vilkårene som skal gjelde for lovligheten av den behandlingsansvarliges behandling, hvilken type opplysninger som skal behandles, berørte registrerte, enhetene som personopplysningene kan utleveres til, og formålene med dette, formålsbegrensning, lagringsperioder samt behandlingsaktiviteter og framgangsmåter for behandling, herunder tiltak for å sikre lovlig og rettferdig behandling, slik som dem fastsatt med henblikk på andre særlige behandlingssituasjoner som nevnt i kapittel IX. Unionsretten eller medlemsstatenes nasjonale rett skal oppfylle et mål i allmennhetens interesse og stå i et rimelig forhold til det berettigede målet som søkes oppnådd.

4. Dersom behandlingen for et annet formål enn det som personopplysningene er blitt samlet inn for, ikke bygger på den registrertes samtykke eller på unionsretten eller medlemsstatenes nasjonale rett som utgjør et nødvendig og forholdsmessig tiltak i et demokratisk samfunn for å sikre oppnåelse av målene nevnt i artikkel 23 nr. 1, skal den behandlingsansvarlige for å avgjøre om behandlingen for et annet formål er forenlig med formålet som personopplysningene opprinnelig ble samlet inn for, blant annet ta hensyn til følgende:

a) enhver forbindelse mellom formålene som personopplysningene er blitt samlet inn for, og formålene med den tiltenkte viderebehandlingen,

b) i hvilken sammenheng personopplysningene er blitt samlet inn, særlig med hensyn til forholdet mellom de registrerte og den behandlingsansvarlige,

c) personopplysningenes art, især om særlige kategorier av personopplysninger behandles, i henhold til artikkel 9, eller om personopplysninger om straffedommer og lovovertredelser behandles, i henhold til artikkel 10,

d) de mulige konsekvensene av den tiltenkte viderebehandlingen for de registrerte,

e) om det foreligger nødvendige garantier, som kan omfatte kryptering eller pseudonymisering.

Artikkel 9 Behandling av særlige kategorier av personopplysninger

1. Behandling av personopplysninger om rasemessig eller etnisk opprinnelse, politisk oppfatning, religion, filosofisk overbevisning eller fagforeningsmedlemskap, samt behandling av genetiske opplysninger og biometriske opplysninger med det formål å entydig identifisere en fysisk person, helseopplysninger eller opplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering, er forbudt.

2. Nr. 1 får ikke anvendelse dersom et av følgende vilkår er oppfylt:

a) Den registrerte har gitt uttrykkelig samtykke til behandling av slike personopplysninger for ett eller flere spesifikke formål, unntatt dersom det i unionsretten eller medlemsstatenes nasjonale rett er fastsatt at den registrerte ikke kan oppheve forbudet nevnt i nr. 1.

b) Behandlingen er nødvendig for at den behandlingsansvarlige eller den registrerte skal kunne oppfylle sine forpliktelser og utøve sine særlige rettigheter på området arbeidsrett, trygderett og sosialrett i den grad dette er tillatt i henhold til unionsretten eller medlemsstatenes nasjonale rett, eller en tariffavtale i henhold til medlemsstatenes nasjonale rett som gir nødvendige garantier for den registrertes grunnleggende rettigheter og interesser.

c) Behandlingen er nødvendig for å verne den registrertes eller en annen fysisk persons vitale interesser dersom den registrerte fysisk eller juridisk ikke er i stand til å gi samtykke.

d) Behandlingen utføres av en stiftelse, sammenslutning eller et annet ideelt organ hvis mål er av politisk, religiøs eller fagforeningsmessig art, som ledd i organets berettigede aktiviteter og med nødvendige garantier, forutsatt at behandlingen bare gjelder organets medlemmer eller tidligere medlemmer eller personer som på grunn av organets mål har regelmessig kontakt med det, og at personopplysningene ikke utleveres til andre enn nevnte organ uten de registrertes samtykke.

e) Behandlingen gjelder personopplysninger som det er åpenbart at den registrerte har offentliggjort.

f) Behandlingen er nødvendig for å fastsette, gjøre gjeldende eller forsvare rettskrav eller når domstolene handler innenfor rammen av sin domsmyndighet

g) Behandlingen er nødvendig av hensyn til viktige allmenne interesser, på grunnlag av unionsretten eller medlemsstatenes nasjonale rett som skal stå i et rimelig forhold til det mål som søkes oppnådd, være forenlig med det grunnleggende innholdet i retten til vern av personopplysninger og sikre egnede og særlige tiltak for å verne den registrertes grunnleggende rettigheter og interesser.

h) Behandlingen er nødvendig i forbindelse med forebyggende medisin eller arbeidsmedisin for å vurdere en arbeidstakers arbeidskapasitet, i forbindelse med medisinsk diagnostikk, yting av helse- eller sosialtjenester, behandling eller forvaltning av helse- eller sosialtjenester og -systemer på grunnlag av unionsretten eller medlemsstatenes nasjonale rett eller i henhold til en avtale med helsepersonell og med forbehold for vilkårene og garantiene nevnt i nr. 3.

i) Behandlingen er nødvendig av allmenne folkehelsehensyn, f.eks. vern mot alvorlige grenseoverskridende helsetrusler eller for å sikre høye kvalitets- og sikkerhetsstandarder for helsetjenester og legemidler eller medisinsk utstyr, på grunnlag av unionsretten eller medlemsstatenes nasjonale rett der det fastsettes egnede og særlige tiltak for å verne den registrertes rettigheter og friheter, særlig taushetsplikt.

j) Behandlingen er nødvendig for arkivformål i allmennhetens interesse, for formål knyttet til vitenskapelig eller historisk forskning eller for statistiske formål i samsvar med artikkel 89 nr. 1 på grunnlag av unionsretten eller medlemsstatenes nasjonale rett som skal stå i et rimelig forhold til det mål som søkes oppnådd, være forenlig med det grunnleggende innholdet i retten til vern av personopplysninger og sikre egnede og særlige tiltak for å verne den registrertes grunnleggende rettigheter og interesser.

3. Personopplysningene nevnt i nr. 1 kan behandles for formålene nevnt i nr. 2 bokstav h) dersom opplysningene behandles av en fagperson som har taushetsplikt i henhold til unionsretten eller medlemsstatenes nasjonale rett eller regler fastsatt av nasjonale vedkommende organer, eller under en slik persons ansvar, eller av en annen person som også har taushetsplikt i henhold til unionsretten eller medlemsstatenes nasjonale rett eller regler fastsatt av nasjonale vedkommende organer.

4. Medlemsstatene kan opprettholde eller innføre ytterligere vilkår, herunder begrensninger, med hensyn til behandling av genetiske opplysninger, biometriske opplysninger eller helseopplysninger

Artikkel 28 Databehandler nr. 1-3

1. Dersom en behandling skal utføres på vegne av en behandlingsansvarlig, skal den behandlingsansvarlige bare bruke databehandlere som gir tilstrekkelige garantier for at de vil gjennomføre egnede tekniske og organisatoriske tiltak som sikrer at behandlingen oppfyller kravene i denne forordning og vern av den registrertes rettigheter.

2. Databehandleren skal ikke engasjere en annen databehandler uten at det på forhånd er innhentet særlig eller generell skriftlig tillatelse til dette fra den behandlingsansvarlige. Dersom det er innhentet en generell skriftlig tillatelse, skal databehandleren underrette den behandlingsansvarlige om eventuelle planer om å benytte andre databehandlere eller skifte ut databehandlere, og dermed gi den behandlingsansvarlige muligheten til å motsette seg slike endringer.

3. Behandling utført av en databehandler skal være underlagt en avtale eller et annet rettslig dokument i henhold til unionsretten eller medlemsstatenes nasjonale rett som er bindende for databehandleren med hensyn til den behandlingsansvarlige, og der gjenstanden for og varigheten av behandlingen, behandlingens art og formål, typen personopplysninger og kategorier av registrerte samt den behandlingsansvarliges rettigheter og plikter er fastsatt. I nevnte avtale eller nevnte andre rettslige dokument skal det særlig angis at databehandleren

a) behandler personopplysningene bare på dokumenterte instrukser fra den behandlingsansvarlige, herunder med hensyn til overføring av personopplysninger til en tredjestat eller en internasjonal organisasjon, med mindre det kreves i henhold til unionsretten eller medlemsstatenes nasjonale rett som databehandleren er underlagt; i så fall skal databehandleren underrette den behandlingsansvarlige om nevnte rettslige krav før behandlingen, men mindre denne rett av hensyn til viktige allmenne interesser forbyr en slik underretning

b) sikrer at personer som er autorisert til å behandle personopplysningene, har forpliktet seg til å behandle opplysningene konfidensielt eller er underlagt en egnet lovfestet taushetsplikt,

c) treffer alle tiltak som er nødvendig i henhold til artikkel 32,

d) overholder vilkårene nevnt i nr. 2 og 4 når det gjelder å engasjere en annen databehandler,

e) idet det tas hensyn til behandlingens art og i den grad det er mulig, bistår, ved hjelp av egnede tekniske og organisatoriske tiltak, den behandlingsansvarlige med å oppfylle vedkommendes plikt til å svare på anmodninger som den registrerte inngir med henblikk på å utøve sine rettigheter fastsatt i kapittel III,

f) bistår den behandlingsansvarlige med å sikre overholdelse av forpliktelsene i henhold til artikkel 32-36, idet det tas hensyn til behandlingens art og den informasjonen som er tilgjengelig for databehandleren,

g) etter den behandlingsansvarliges valg, sletter eller tilbakeleverer alle personopplysninger til den behandlingsansvarlige etter at tjenestene knyttet til behandlingen er levert, og sletter eksisterende kopier, med mindre unionsretten eller medlemsstatenes nasjonale rett krever at personopplysningene lagres

h) gjør tilgjengelig for den behandlingsansvarlige all informasjon som er nødvendig for å påvise at forpliktelsene fastsatt i denne artikkel er oppfylt, samt muliggjør og bidrar til revisjoner, herunder inspeksjoner, som gjennomføres av den behandlingsansvarlige eller en annen revisor på fullmakt fra den behandlingsansvarlige.

Når det gjelder første ledd bokstav h) skal databehandleren omgående underrette den behandlingsansvarlige dersom vedkommende mener at en instruks er i strid med denne forordning eller andre bestemmelser om vern av personopplysninger i unionsretten eller medlemsstatenes nasjonale rett

Artikkel 32 Sikkerhet ved behandlingen

1. Idet det tas hensyn til den tekniske utviklingen, gjennomføringskostnadene og behandlingens art, omfang, formål og sammenhengen den utføres i, samt risikoene av varierende sannsynlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter, skal den behandlingsansvarlige og databehandleren gjennomføre egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen, herunder blant annet, alt etter hva som er egnet,

a) pseudonymisering og kryptering av personopplysninger,

b) evne til å sikre vedvarende konfidensialitet, integritet, tilgjengelighet og robusthet i behandlingssystemene og -tjenestene,

c) evne til å gjenopprette tilgjengeligheten og tilgangen til personopplysninger i rett tid dersom det oppstår en fysisk eller teknisk hendelse,

d) en prosess for regelmessig testing, analysering og vurdering av hvor effektive behandlingens tekniske og organisatoriske sikkerhetstiltak er.

2. Ved vurderingen av egnet sikkerhetsnivå skal det særlig tas hensyn til risikoene forbundet med behandlingen, særlig som følge av utilsiktet eller ulovlig tilintetgjøring, tap, endring eller ikke-autorisert utlevering av eller tilgang til personopplysninger som er overført, lagret eller på annen måte behandlet.

3. Overholdelse av godkjente atferdsnormer som nevnt i artikkel 40 eller en godkjent sertifiseringsmekanisme som nevnt i artikkel 42 kan brukes som en faktor for å påvise at kravene i nr. 1 i denne artikkel er oppfylt.

4. Den behandlingsansvarlige og databehandleren skal treffe tiltak for å sikre at enhver fysisk person som handler for den behandlingsansvarlige eller databehandleren, og som har tilgang til personopplysninger, behandler nevnte opplysninger bare etter instruks fra den behandlingsansvarlige, med mindre unionsretten eller medlemsstatenes nasjonale rett krever at vedkommende gjør dette

Taushetsplikt etter helselovgivningen

Helseregisterloven § 17 Taushetsplikt

Enhver som behandler helseopplysninger etter denne loven, har taushetsplikt etter helsepersonelloven §§ 21 flg. Andre som får adgang eller kjennskap til helseopplysninger fra helseregistre, har samme taushetsplikt. For søknader om dispensasjon fra taushetsplikten for tilgjengeliggjøring av opplysninger i helseregistre gjelder § 19 e.

Helsepersonelloven § 21 Hovedregel om taushetsplikt

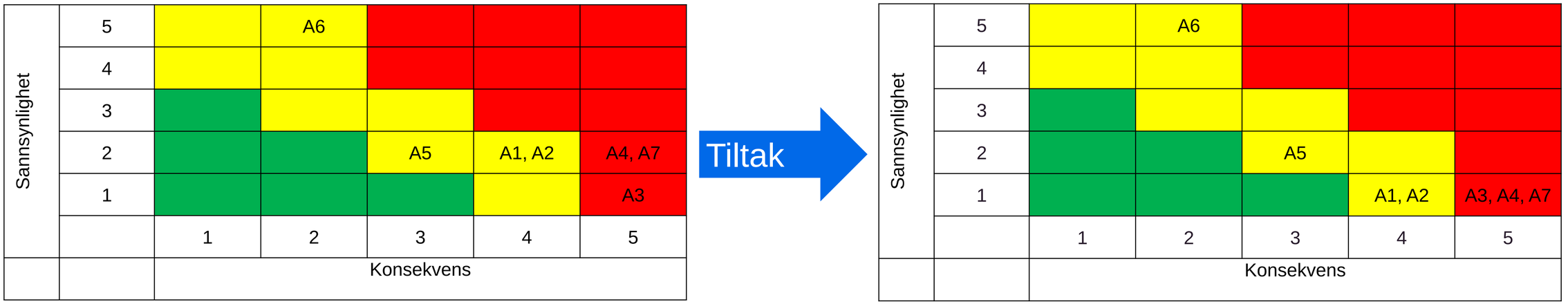
Helsepersonell skal hindre at andre får adgang eller kjennskap til opplysninger om folks legems- eller sykdomsforhold eller andre personlige forhold som de får vite om i egenskap av å være helsepersonell

Helsepersonelloven § 23 Begrensninger i taushetsplikt

Taushetsplikt etter § 21 er ikke til hinder for:

1. at opplysninger gis den som fra før er kjent med opplysningene,
2. at opplysninger gis når ingen berettiget interesse tilsier hemmelighold,
3. at opplysninger gis videre når behovet for beskyttelse må anses ivaretatt ved at individualiserende kjennetegn er utelatt,
4. at opplysninger gis videre når tungtveiende private eller offentlige interesser gjør det rettmessig å gi opplysningene videre,
5. at opplysninger gis videre når helsepersonell gjennom sin yrkesutøvelse har grunn til å tro at dyr blir utsatt for slik mishandling eller alvorlig svikt vedrørende miljø, tilsyn og stell at det anses rettmessig å gi opplysningene videre til Mattilsynet eller politiet eller
6. at opplysningene gis videre etter regler fastsatt i lov eller i medhold av lov når det er uttrykkelig fastsatt eller klart forutsatt at taushetsplikt ikke skal gjelde

ROS – Helsedataprogrammet (ehelse)



ID	Risikoscenario
A1	Etterretningsenheter/politi/påtalemyndigheter i USA får tilgang til våre data ihht. FISA 702 eller Cloud Act hvor myndigheten får tilgang til data via Microsoft. Microsoft vil ha kjennskap og vil varsle dataansvarlig dersom det er lov.
A2	Etterretningsenheter i USA får tilgang til våre data ihht. EO 12333 og PPD-28 hvor myndigheten får tilgang til data uten Microsoft sin hjelp. Dette kan være med eller uten Microsoft sin kjennskap.
A3	Andre tredjeland (ikke USA) får tilgang til våre data ihht. relevant lovgivning i tredjelandet, med Microsoft sin kjennskap, men uten at dataansvarlig nødvendigvis varsles.
A4	Andre tredjeland (ikke USA) får tilgang til våre data ved hemmelig innhenting uten at Microsoft eller dataansvarlig/databehandlere har kjennskap til det.
A5	Personopplysninger tilgjengeliggjøres for MS i et tredjeland i forbindelse med support ved en feil (support tickets vil i praksis sendes av Accenture-ansatte)
A6	Microsoft bruker kundedata (ikke data i HAP) til egne formål som ikke har opprinnelse i lovpålagt utlevering fra myndigheter. I slike tilfeller er Microsoft behandlingsansvarlig/ dataansvarlig for behandlingen.
A7	Microsoft bruker kundedata (som data i HAP, inklusive helseopplysninger) til egne formål som ikke har opprinnelse i lovpålagt utlevering fra myndigheter. I slike tilfeller er Microsoft behandlingsansvarlig/dataansvarlig for behandlingen.

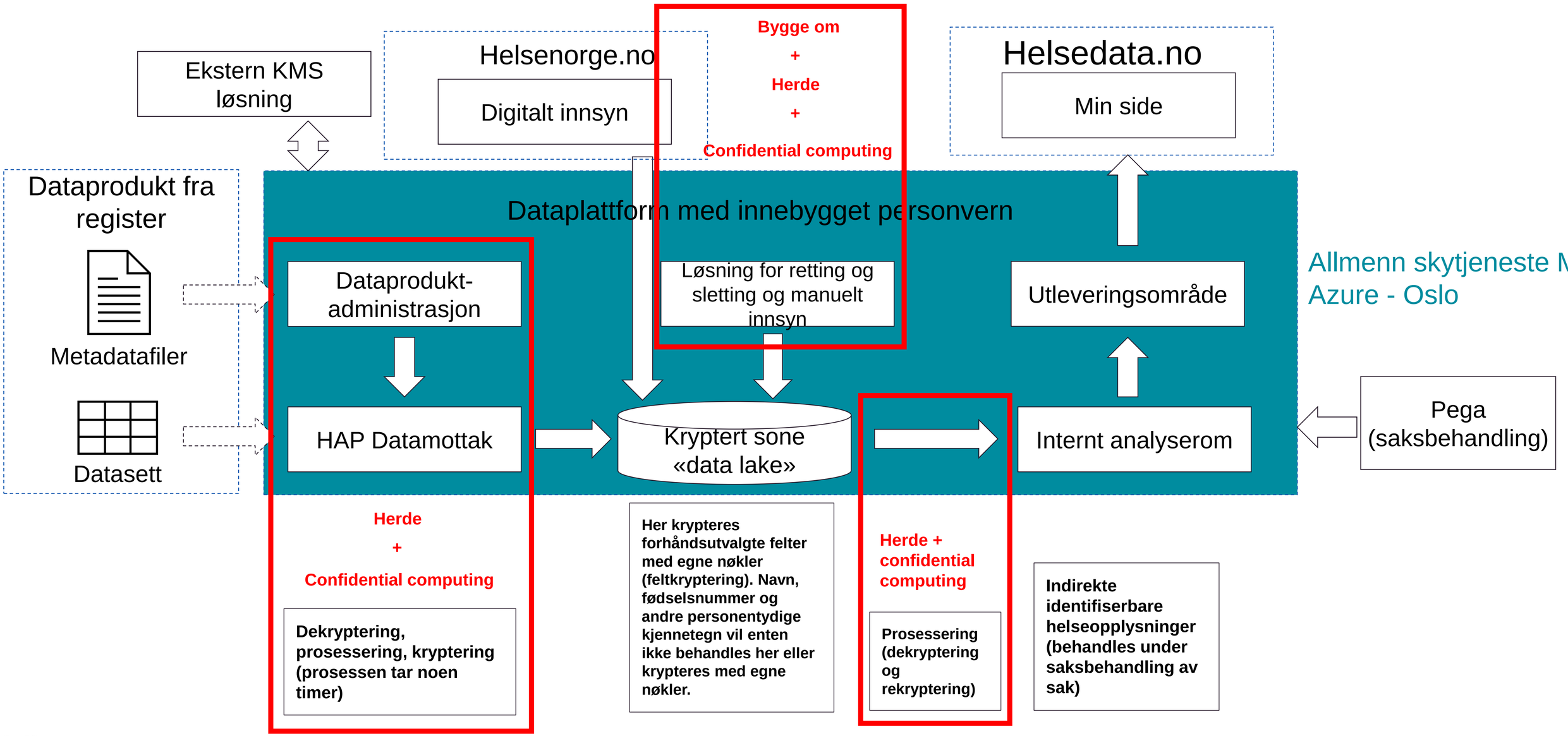
Ytterligere tiltak

1. Rutiner for herding og «confidential computing». Bygge om tjeneste for håndtering av innsynsforespørsler fra innbyggere (*PaaS-tjeneste*) til Azure Batch basert tjeneste.

2. Økt grad av kryptering samtidig som brukskvalitet for saksbehandlere ivaretas.

3. Avklare avtaletekst og forståelse med Microsoft

0: Forenklet (forventet) løsningsskisse av dataplattformen etter «Berlin» leveransen



Storbritannia vurderer at det er sikkert å lagre helsedata i skytjenester i EU og USA

Storbritannia vurderer at det er sikkert å lagre helsedata i allmenne skytjenester i EU og USA

NHS Digital | Department of Health & Social Care | NHS England | NHS Improvement

NHS and social care data: off-shoring and the use of public cloud services

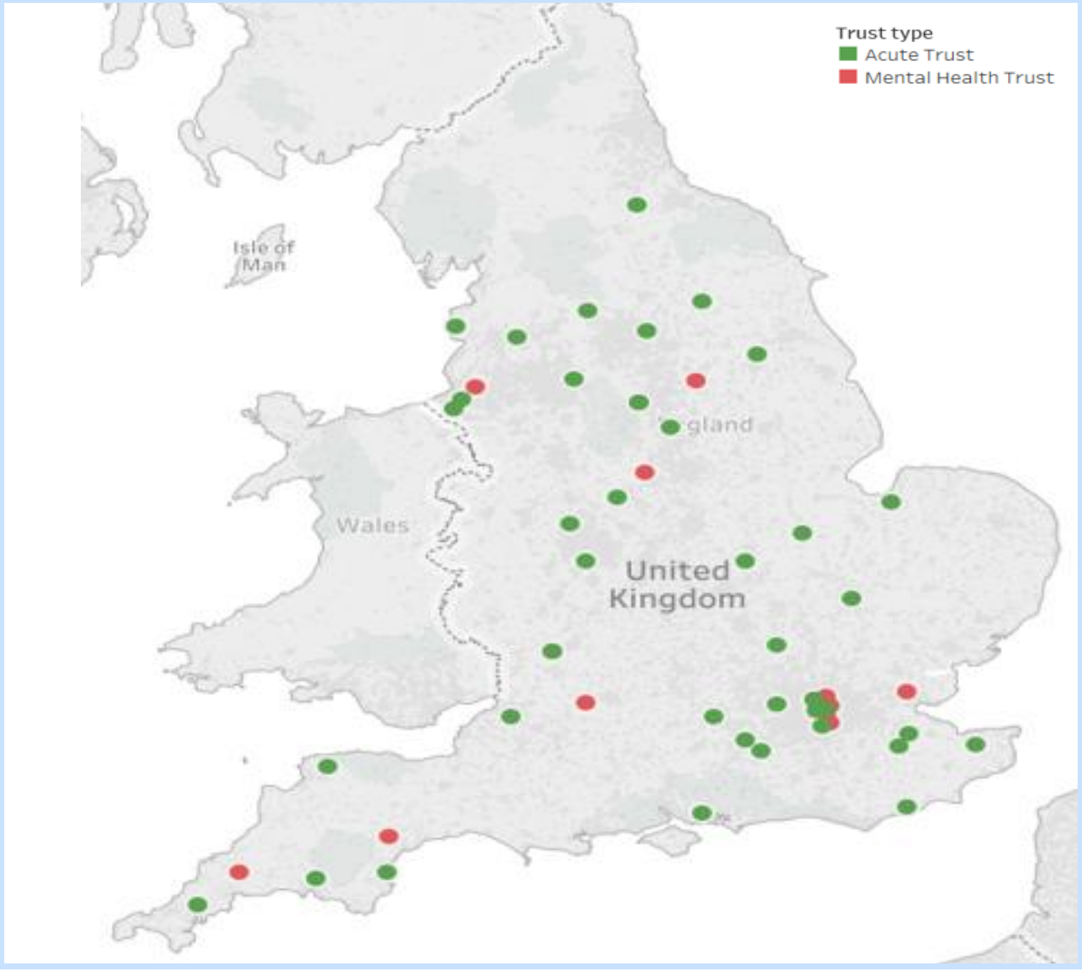
NHS and social care organisations can safely locate health and care data, including confidential patient information, in the public cloud including solutions that make use of data off-shoring.

This guide explains the safeguards that must be put in place to do so, including considerations about where the data can be located.

In brief:

- NHS and Social care providers may use cloud computing services for NHS data. Data must only be hosted within the European Economic Area (EEA), a country deemed adequate by the European Commission, or in the US where covered by Privacy Shield.
- Senior Information Risk Owners (SIROs) locally should be satisfied about appropriate security arrangements (using National Cyber Security Essentials as a guide) in conjunction with Data Protection Officers and Caldicott Guardians.
- Help and advice from the Information Commissioner's Office is available and regularly updated.
- Changes to data protection legislation, including the General Data Protection Regulation (GDPR) from 25 May 2018, puts strict restrictions on the transfer of personal data, particularly when this transfer is outside the European Union. The ICO also regularly updates its GDPR Guidance.

NHS Trust som benytter skytjenester i dag



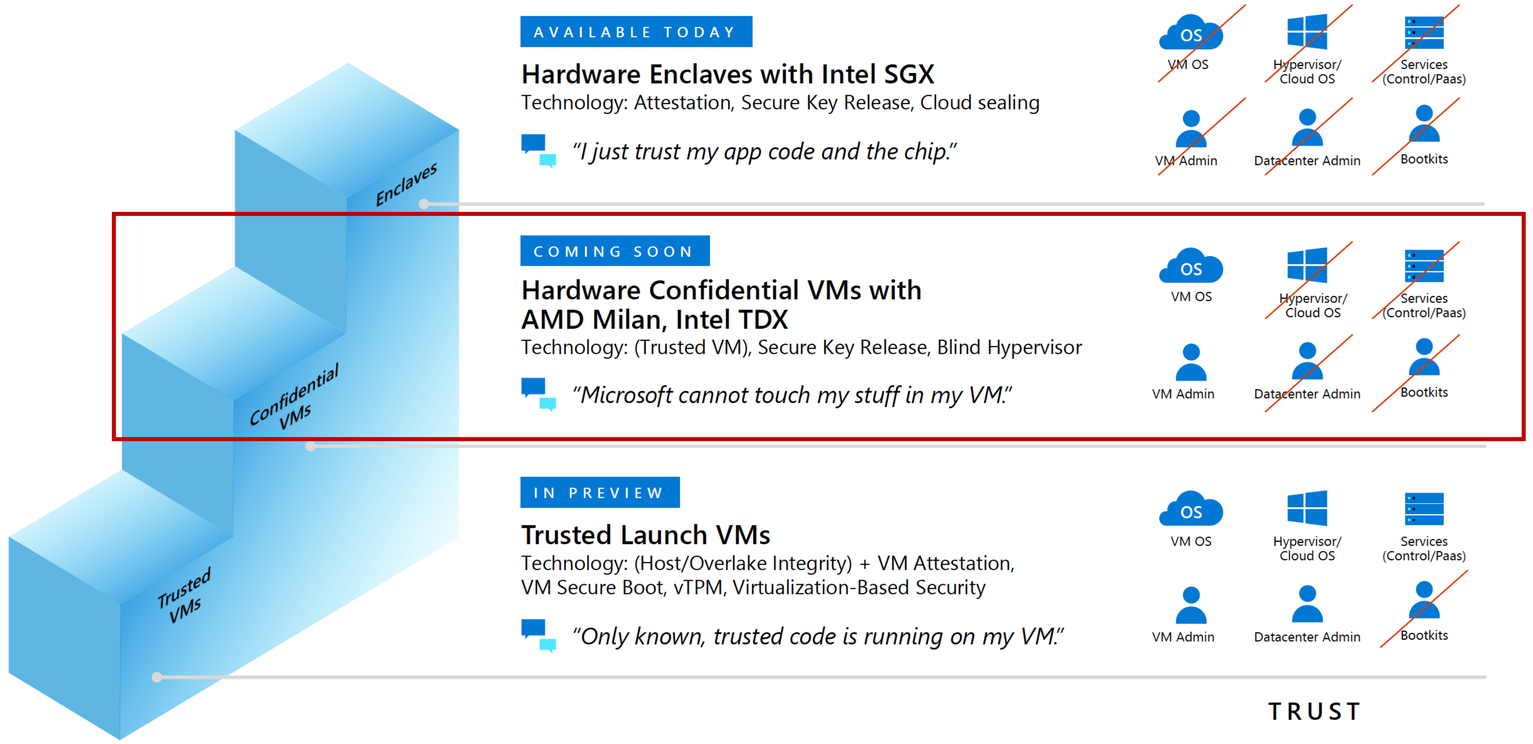
Hva er Confidential Computing?

Det finnes modne teknologier for å beskytte data ved lagring og under transport. Under *behandling* er imidlertid informasjon eksponert for angrep ettersom data er ukryptert i minnet.

Confidential Computing benyttes for å beskytte data under behandling slik at data ikke er tilgjengelig utenfor barrierer definert av Confidential Computing-mekanismer.

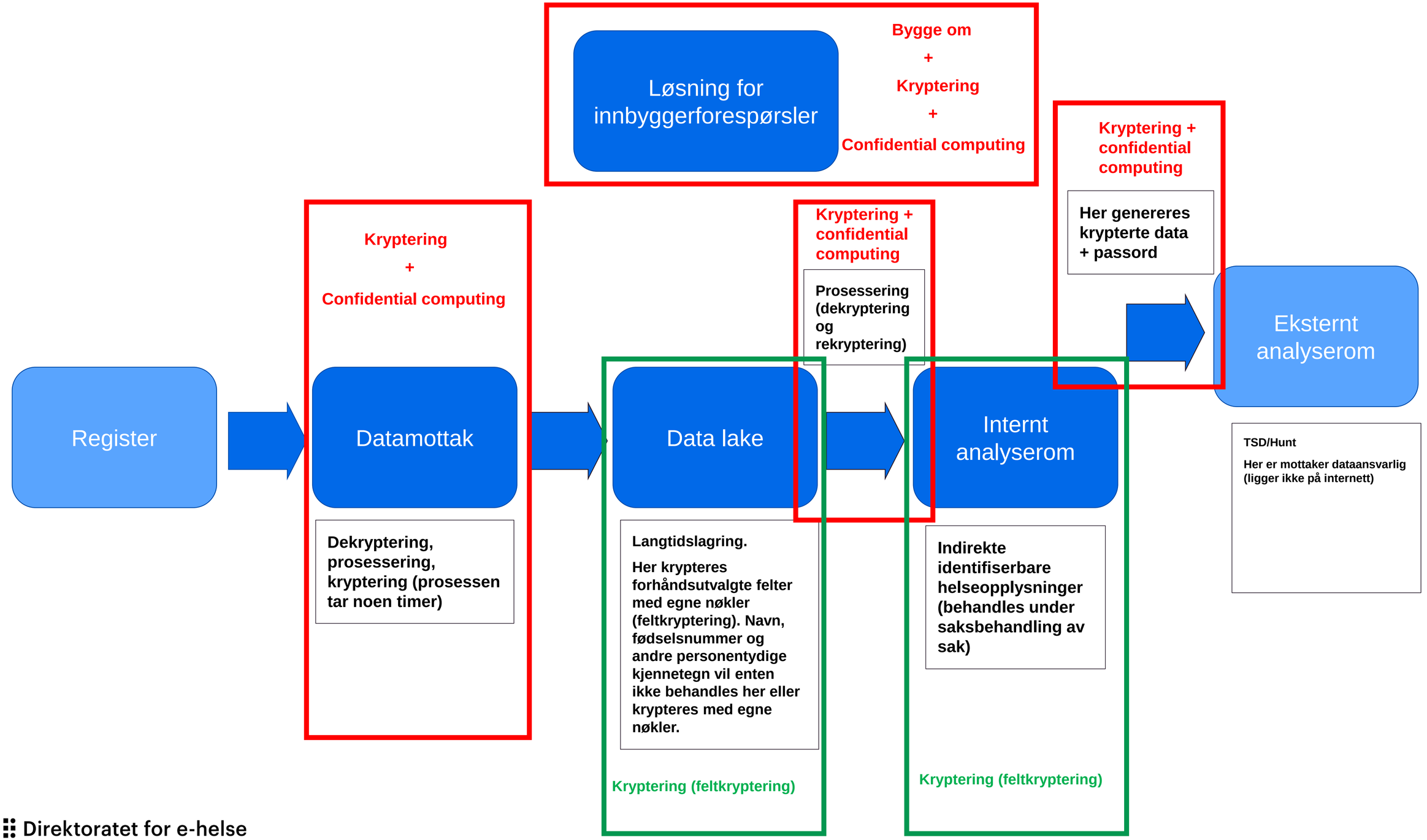
Avhengig av hva man kan stole på finnes ulike Confidential Computing-tjenester:

- **Hardware Enclaves –** barriere etablert på applikasjonsnivå. Krever skreddersydd confidential computing applikasjon som behandler sensitiv data i sikret enklave.
- **Hardware Confidential VM –** barriere etablert på VM-nivå. Forhindrer skyleverandør tilgang til innhold i VM. Ettersom beskyttelse er på VM-nivå kreves ikke tilpasning av applikasjoner.
- **Trusted Launch VM –** sikrer at bare sertifisert kode får kjøre på en VM.



Anbefaling av aktuell teknologi

Hardware Confidential VM vil kunne brukes på spesifikke deler for å sikre HAP mot innsyn fra skyleverandør og forhindre tilgang til ukryptert informasjon utenfor Europa.


Løsning for innbyggerforespørsler
Bygge om
+
Kryptering
+
Confidential computing
Kryptering + confidential computing
Her genereres krypterte data + passord
Kryptering
+
Confidential computing
Kryptering + confidential computing
Prosessering (dekryptering og rekryptering)
Register
Datamottak
Data lake
Internt analyserom
Eksternt analyserom
Dekryptering, prosessering, kryptering (prosessen tar noen timer)
Langtidslagring.
Her krypteres forhåndsutvalgte felter med egne nøkler (feltkryptering). Navn, fødselsnummer og andre personentydige kjennetegn vil enten ikke behandles her eller krypteres med egne nøkler.
Indirekte identifiserbare helseopplysninger (behandles under saksbehandling av sak)
TSD/Hunt
Her er mottaker dataansvarlig (ligger ikke på internett)
Kryptering (feltkryptering)
Kryptering (feltkryptering)

Helseanalyseplattformen

- Etableres med hjemmel i helseregisterloven + egen forskrift
- Samler inn data fra flere helseregistre m.m.
- Dataene skal brukes til sekundærformål
  - Forskning
  - Statistikk
  - Kvalitetsforbedring og styring av helse- og omsorgsforvaltningen
  - m.m.
- Sentraliserer forvaltningen av helsedata
- Formålet er å sørge for enklere, raskere og sikrere tilgjengeliggjøring av helsedata

Fordeler ved å bruke allmenn skytjeneste til HAP

Beslutning om skytjenester:

- ✓ Konseptvalgutredning (2018)
- ✓ Statssekretærutvalg (2018)
- ✓ LM-beslutning (2019)
- ✓ Anskaffelse ROS (2020)

1. Innovasjon og utviklingstempo
2. Ekstrem skalerbarhet, ytelse, kapasitet og stabilitet
3. Redusert investeringsbehov
4. Enklere forvaltning og administrasjon
5. Sikkerhet
6. Funksjonalitet