*Helse- og omsorgsdepartementet*

# Høringsnotat

# Krav om bakgrunnssjekk av personell i kritiske stillinger og funksjoner, og begrenset deling av store datasett – endringer i helselovgivningen

Høringsfrist 1. oktober 2024

# Innhold

# 1 Innledning

Departementet foreslår i dette høringsnotatet endringer i pasientjournalloven, helseregisterloven og helsepersonelloven, for å kunne sjekke bakgrunnen til personell i kritiske stillinger og funksjoner i helse- og omsorgssektoren, utover det som følger av sikkerhetsloven. Forslaget berører primært stillinger eller roller hvor potensialet for skade som følge av tilgang til IKT-systemer er stort. Dette er typisk driftspersonell som har høyt tilgangsnivå eller kontroll over virksomhetens IKT-systemer, sikkerhetspersonell og annet personell som har tilgang til store datasett med person- og helseopplysninger. Departementet foreslår at også forskere med tilgang til store datasett kan omfattes. Videre vil utviklere av kritiske løsninger kunne omfattes.

Departementet foreslår også endringer i helseregisterloven og helsepersonelloven for å kunne begrense deling av enkelte store sett med helsedata, av hensyn til nasjonale sikkerhetsinteresser.

Flere av aktørene i helse- og omsorgsektoren drifter og forvalter informasjonssystemer, hvor det behandles store datasett med person- og helseopplysninger, som ikke er sikkerhetsgradert informasjon. De aktuelle systemene er heller ikke definert som skjermingsverdig objekt eller infrastruktur. Sikkerhetslovens krav til autorisasjon og sikkerhetsklarering for tilgang til informasjonen, samt krav til adgangsklarering for tilgang til skjermingsverdig objekt og infrastruktur, er derfor ikke direkte anvendbare. Informasjonen vil likevel kunne ha betydning for nasjonale sikkerhetsinteresser, dersom den blir kompromittert.

Personell i kritiske funksjoner er gitt tilganger til innhold i systemer eller kontroll over systemer. Tilgangen gis ut fra stillingens tjenstlige behov, men kan misbrukes dersom feil person ansettes i disse stillingene. Potensiale for skade er stort, og misbruk vil kunne true helse- og omsorgstjenestens evne til å ivareta sine oppgaver og befolkningens helse og sikkerhet, og derigjennom vil kunne skade de nasjonale sikkerhetsinteressene.

Det er derfor nødvendig å sikre et forsvarlig sikkerhetsnivå, bl.a. ved å stille krav om at personell i kritiske stillinger og funksjoner er vurdert sikkerhetsmessig skikket, og at vi kan ha begrunnet tillit til at personellet har den nødvendige pålitelighet, lojalitet og dømmekraft som stillingene forutsetter. Slik tillit fordrer bakgrunnssjekk av personellet basert på relevante kilder. Et slikt krav bør også gjelde ved bruk av eksterne tjenestetilbydere.

Ivaretagelse av integritet, tilgjengelighet, konfidensialitet og nasjonal sikkerhet knyttet til digitale helsesystemer er stadig mer krevende, fordi trussel- og risikobildet er komplekst, i stadig endring og berører alle samfunnsområder. Trusselaktørenes intensjon er vanskelig å forutsi, fordi grunnlaget kan endre seg raskt. Statlige trusselaktører og andre trusselaktører med betydelige ressurser og evne har over tid vist en økende vilje til å utnytte våre sårbarheter gjennom en helhetlig og langsiktig tilnærming, og har i økende grad hatt fokus også på helse- og omsorgssektoren.

Sammensatte trusler er egnet til å ramme samfunnet bredt. Trusselaktører bruker bevisst ulike virkemidler for å få innpass i verdikjeder. Departementet forventer at dette vil

vedvare og tilspisse seg. Tilgang til informasjon kan være en aktørs forsøk på å oppnå kontroll eller betydelig innflytelse, herunder hindre funksjoner. Dette vil kunne påvirke helsetjenestens evne til å levere trygge og gode tjenester, utgjøre en trussel mot befolkningen og være i strid med nasjonale sikkerhetsinteresser. Det er viktig at vi har mulighet til å identifisere aktuelle trusler, vurdere konsekvensene og begrense trusselaktørenes spillerom.

I stortingsmeldingen (Meld. St. 9 (2022–2023)) om nasjonal kontroll og digital motstandskraft for å ivareta nasjonal sikkerhet, redegjør Regjeringen for behovet for en helhetlig og langsiktig tilnærming til nasjonal sikkerhet i hele samfunnet. I meldingen påpekes det at det er behov for å vurdere hvordan vi kan få bedre oversikt over verdier som ikke dekkes av sikkerhetsloven, men som likevel kan ha betydning for våre nasjonale sikkerhetsinteresser. Det fremgår også at det er behov for å gjennomgå annet relevant regelverk for å forsikre seg om at hensyn til nasjonal sikkerhet inngår som vurderingskriterium, der det er relevant.

Som en del av arbeidet med oppfølging av sikkerhet i helse- og omsorgssektoren og av Meld. St. 9 (2022–2023), har Helse- og omsorgsdepartementet vurdert at det er behov for å kunne stille krav til bakgrunnssjekk av personell i kritiske stillinger og funksjoner, utover det som følger av sikkerhetsloven og gjeldende rett for øvrig.

Videre er det blitt synliggjort et behov for å kunne begrense deling av enkelte store sett med helsedata av hensyn til de nasjonale sikkerhetsinteressene. Utviklingen og bruk av kunstig intelligens har også aktualisert problemstillingen. Dette gjelder store aggregerte datasett med anonyme eller indirekte identifiserbare helsedata. Med store datasett mener departementet datasett som alene eller sammen med andre datasett, sier noe om en befolkningsgruppe.

De to tiltakene omtalt ovenfor er adskilte, men har betydelige likhetspunkter og berøringsflater. Formålet med departementets forslag er bedre å kunne ivareta helse- og omsorgstjenestens oppgaver, befolkningens helse og den enkeltes personvern, ved å redusere risiko for at «utro tjenere» ansettes i kritiske stillinger og ved at store sett med helsedata ikke blir tilgjengelig for aktører som kan utgjøre en trussel.

Departementet mener forslagene vil bidra til å ivareta befolkningens grunnleggende helse og sikkerhet, og øke den nasjonale motstandskraften mot dagens sammensatte trusselbilde.

# 2 Gjeldende rett

## 2.1 Pasientjournalloven

Lovens formål er at behandling av helseopplysninger skal skje på en måte som gir pasienter og brukere helsehjelp av god kvalitet ved at relevante og nødvendige opplysninger på en rask og effektiv måte blir tilgjengelige for helsepersonell. Samtidig skal loven sikre at opplysninger ikke gis til uvedkommende, og sikre pasienters og brukeres personvern, pasientsikkerhet og rett til informasjon og medvirkning.

Pasientjournalloven gjelder behandling av helseopplysninger som er nødvendige for å yte, administrere eller kvalitetssikre helsehjelp til enkeltpersoner, jf. § 3.

Krav til informasjonssikkerhet følger av § 22. I bestemmelsen er det bestemt at den dataansvarlige og databehandleren, skal gjennomføre tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen. Den dataansvarlige og databehandleren skal blant annet sørge for tilgangsstyring, logging og etterfølgende kontroll. Bestemmelsen er direkte knyttet til personvernforordningen artikkel 32 ved henvisning.

Av § 22 andre ledd følger at departementet i forskrift kan fastsette nærmere krav til informasjonssikkerhet ved behandling av helseopplysninger.

## 2.2 Helseregisterloven

Lovens formål er å legge til rette for innsamling og annen behandling av helseopplysninger, for å fremme helse, forebygge sykdom og skade og gi bedre helse- og omsorgstjenester. Loven skal sikre at behandlingen foretas på en etisk forsvarlig måte, ivaretar den enkeltes personvern og brukes til individets og samfunnets beste. Dette følger av § 1.

Lovens saklige virkeområde er regulert i § 3. Loven gjelder for behandling av helseopplysninger til statistikk, helseanalyser, forskning, kvalitetsforbedring, planlegging, styring og beredskap i helse- og omsorgsforvaltningen og helse- og omsorgstjenesten.

Helseregisterloven § 19 til § 19 h regulerer adgangen til å tilgjengeliggjøre og sammenstille helseopplysninger fra helseregistre. Utarbeidelse og tilgjengeliggjøring av anonym statistikk og andre anonyme opplysninger er regulert i § 19. Det er fri adgang til å tilgjengeliggjøre anonym statistikk og andre anonyme opplysninger, fordi slike data ikke kan knyttes til enkeltpersoner og derfor ikke omfattes av reglene om personvern og taushetsplikt.

Bestemmelsen er et utslag av prinsippet om dataminimering i personvernforordningen artikkel 5 nr. 1 bokstav c. Det følger av dette prinsippet at graden av personidentifikasjon skal være så liten som mulig (jf. helseregisterloven § 6 andre ledd første punktum). Utgangspunktet er derfor at opplysninger fra helseregistre som tilgjengeliggjøres skal være anonyme. Direkte eller indirekte personidentifiserende opplysninger kan bare tilgjengeliggjøres dersom det er nødvendig ut fra formålet med behandlingen.

Tilgjengeliggjøring av helseopplysninger er regulert i § 19 a. Bestemmelsen fastsetter vilkårene for tilgjengeliggjøring av direkte og indirekte personidentifiserbare helseopplysninger fra helseregistre, inkludert sammenstilte datasett. Dersom vilkårene i helseregisterloven § 19 a er oppfylt, er det ikke bare tillatt, men også en plikt, for den dataansvarlige å tilgjengeliggjøre opplysningene.

Reglene for dispensasjon fra taushetsplikten følger av § 19 e. Helseopplysninger i helseregistre er taushetsbelagte, jf. helseregisterloven § 17 som viser til helsepersonelloven §§ 21 flg. Dersom søkeren skal kunne få opplysningene, må enten de registrerte ha samtykket til tilgjengeliggjøringen eller så må tilgjengeliggjøringen være i samsvar med unntak eller dispensasjon fra taushetsplikten. Helseregisterloven § 19 e fastsetter hvilke vilkår som må være oppfylt for å kunne gi dispensasjon fra taushetsplikten ved tilgjengeliggjøring fra helseregistre. Bestemmelsen regulerer vedtak om dispensasjon fra taushetsplikten ved tilgjengeliggjøring av opplysninger som er omfattet av helseregisterloven. Ved helsepersonells tilgjengeliggjøring av opplysninger fra pasientjournaler og andre behandlingsrettede helseregistre, gjelder helsepersonelloven § 29.

I helseregisterloven § 19b er det gitt et særskilt unntak fra taushetsplikten ved tilgjengeliggjøring av indirekte identifiserbare helseopplysninger fra nasjonale helseregistre omfattet av lovens § 11. Vilkåret er at «hensynet til den registrertes integritet og konfidensialitet er ivaretatt og behandlingen av opplysningene er av vesentlig interesse for samfunnet.»

Bestemmelsene om tilgjengeliggjøring er nærmere beskrevet i *Prop.63 L (2019–2020) Endringer i helseregisterloven m.m. (tilgjengeliggjøring av helsedata)*.

Kravene til informasjonssikkerhet følger av helseregisterloven § 21. Den dataansvarlige og databehandleren skal gjennomføre tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen. Den dataansvarlige og databehandleren skal blant annet sørge for tilgangsstyring, logging og etterfølgende kontroll. Bestemmelsen er direkte knyttet til personvernforordningen artikkel 32 ved henvisning. Av § 21 andre ledd følger at departementet i forskrift kan fastsette nærmere krav til informasjonssikkerhet ved behandling av helseopplysninger.

## 2.3 Sikkerhetsloven

Loven skal bidra til a) å trygge Norges suverenitet, territorielle integritet og demokratiske styreform og andre nasjonale sikkerhetsinteresser, b) å forebygge, avdekke og motvirke sikkerhetstruende virksomhet og c) at sikkerhetstiltak gjennomføres i samsvar med grunnleggende rettsprinsipper og verdier i et demokratisk samfunn. Se loven § 1-1.

Objekter og infrastruktur er skjermingsverdige dersom det enten kan skade grunnleggende nasjonale funksjoner om de får redusert funksjonalitet eller blir utsatt for skadeverk, ødeleggelse eller rettsstridig overtakelse, eller kan skade nasjonale sikkerhetsinteresser på annen måte, jf. § 7-1.

Av loven § 8-1 følger at personer som skal få tilgang til sikkerhetsgradert informasjon, skal autoriseres i samsvar med § 8-9. Det samme gjelder personer som skal ha adgang til skjermingsverdige objekter og infrastruktur som det er fattet vedtak om etter § 8-3.

Videre følger at personer som skal autoriseres for tilgang til informasjon gradert konfidensielt eller høyere, må ha gyldig sikkerhetsklarering. Personer som skal autoriseres for tilgang til skjermingsverdige objekter og infrastruktur som det er fattet vedtak om etter § 8-3, må ha gyldig adgangsklarering. Adgangsklarering kan benyttes som sikkerhetstiltak dersom fysisk eller logisk tilgang til hele eller deler av et objekt eller en infrastruktur gjør det mulig å skade grunnleggende nasjonale funksjoner. Det følger av klareringsforskriften (forskrift om sikkerhetsklarering og annen klarering) § 15 at hvert departement, innenfor sitt ansvarsområde kan fatte vedtak om krav til adgangsklarering der et objekt eller en infrastruktur kan være et mål for ikke-statlig terror, attentat eller annen alvorlig kriminalitet. Kan objektet eller infrastrukturen være mål for statlig sabotasje eller andre tilsiktede anslag fra en annen stat, kan departementet fatte vedtak om krav til utvidet adgangsklarering.

En person kan bare klareres dersom det ikke finnes rimelig grunn til å tvile på at personen er sikkerhetsmessig skikket, jf. § 8-4. Klareringsmyndigheten fatter avgjørelse om klarering. I vurderingen skal det legges vekt på forhold som er relevante for personens pålitelighet, lojalitet og dømmekraft i forbindelse med behandling av gradert informasjon og tilgang til skjermingsverdige objekter og infrastruktur. Vurderingen skal gjøres basert på en bakgrunnssjekk. Klareringsmyndigheten skal se til at klareringssaken er så godt opplyst som mulig. Dersom det er tvil om en person er sikkerhetsmessig skikket, skal klareringsmyndigheten ha en sikkerhetssamtale med personen.

Sivil klareringsmyndighet (SKM) er et direktorat og forvaltningsorgan under Justis- og beredskapsdepartementet. Som den sentrale sivile klareringsmyndigheten, er samfunnsoppdraget å beskytte nasjonale verdier ved å redusere risikoen for innsidere. Arbeidet skal gi merkbare effekter for samfunnet og brukerne, knyttet til justis- og beredskapssektoren sine hovedmål rettsikkerhet og trygghet i samfunnet.

## 2.4 Offentleglova

Formålet med loven er å legge til rette for at offentlig virksomhet er åpen og gjennomsiktig, for slik å styrke informasjons- og ytringsfriheten, den demokratiske deltakelsen, den enkeltes rettssikkerhet, tillit til det offentlige og kontrollen fra allmenheten. Loven skal også legge til rette for viderebruk av offentlig informasjon.

Hovedregelen om innsyn følger av § 3:

«Saksdokument, journalar og liknande register for organet er opne for innsyn dersom ikkje anna følgjer av lov eller forskrift med heimel i lov. Alle kan krevje innsyn i saksdokument, journalar og liknande register til organet hos vedkommande organ».

Etter offentlighetsloven § 21 kan det «gjerast unntak frå innsyn for opplysningar når det er påkravd av nasjonale tryggingsomsyn eller forsvaret av landet». Bestemmelsen gir

forvaltningen en adgang, men ikke en plikt til å nekte innsyn i slike dokumenter. Dette innebærer at det også skal vurderes om det likevel skal gis innsyn (merinnsyn).

Unntaket etter bestemmelsen favner videre enn opplysninger som er gradert iht. sikkerhetsloven, men er likevel begrenset.

## 2.5 Personopplysningsloven og personvernforordningen

EUs personvernforordning er gjennomført i norsk rett ved lov 15. juni 2018 nr. 38 om behandling av personopplysninger § 1. Personvernforordningen fastsetter regler om vern av fysiske personer i forbindelse med behandling av personopplysninger, samt regler om fri utveksling av personopplysninger. Det er presisert i artikkel 1 at forordningen sikrer vern av fysiske personers grunnleggende rettigheter og friheter, særlig deres rett til vern av personopplysninger. Personvernforordningen skal leses i lys av andre menneskerettigheter.

Behandling av personopplysninger som er nødvendig av hensynet til rikets eller alliertes sikkerhet, forholdet til fremmede makter og andre vitale nasjonale sikkerhetsinteresser, er unntatt fra tilsynsmyndighetens tilgang til opplysninger etter personvernforordningen artikkel 58 nr. 1, se personopplysningsloven § 23 tredje ledd. Dette betyr at Datatilsynet ikke er undersøkelsesmyndighet, og kan bl.a. ikke pålegge den behandlingsansvarlige eller databehandleren å framlegge all informasjon den trenger for å kunne utføre sine oppgaver, eller utføre undersøkelser i form av personvernrevisjoner. Personopplysningsloven og forordningen for øvrig, kommer imidlertid til anvendelse.

Personvernforordningen bygger på noen grunnleggende prinsipper som må ivaretas ved behandling av person- og helseopplysninger, og som likevel skal følges ved behandlingen av personopplysninger. Personvernprinsippene følger av artikkel 5 og består av:

– Prinsippene om lovlighet, rettferdighet og åpenhet

– Prinsippet om formålsbegrensning

– Prinsippet om dataminimering

– Prinsippet om riktighet

– Prinsippet om lagringsbegrensninger

– Prinsippet om integritet og konfidensialitet

– Prinsippet om ansvar

Prinsippene gir uttrykk for både grunnleggende hensyn som personvernforordningen skal ivareta, og konkrete krav til hvordan personopplysninger skal behandles. Prinsippene er selvstendige regler som stiller krav til all behandling av personopplysninger. I tillegg skal de brukes i tolkningen av andre bestemmelser i forordningen og personvernbestemmelser i andre lover, herunder lover som regulerer behandling av personopplysninger i helse- og omsorgssektoren.

Enhver behandling av person- og helseopplysninger krever en eller flere behandlingsansvarlige/dataansvarlige. Behandlingsansvaret påhviler i utgangspunktet den virksomheten «som alene eller sammen med andre bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes». Dette følger av personvernforordningen artikkel 4 nr. 7.

Videre krever behandling av «vanlige» og såkalt særlig kategorier av personopplysninger - blant annet helseopplysninger - et behandlingsgrunnlag etter personvernforordningen artikkel 6 nr. 1. Behandlingen av særlig kategorier av personopplysninger må også oppfylle vilkårene i et av unntakene i artikkel 9.

Det er et vilkår i artikkel 6 nr. 3 og artikkel 9 nr. 2 bokstav h at behandlingen også skal fastsettes i nasjonal rett eller unionsretten. Dette kalles et supplerende rettslig grunnlag. Forslaget til lovendringer vil være supplerende rettslig grunnlag.

## 2.6 Diskrimineringsvernet

Diskrimineringsvernet er regulert i Grunnloven § 98. Første ledd angir en plikt til å likebehandle, ved at det slås fast at «[a]lle er like for loven». Andre ledd har et negativt formulert diskrimineringsforbud: «Intet menneske må utsettes for usaklig eller uforholdsmessig forskjellsbehandling». Dette forbudet krever først en vurdering av om det foreligger en forskjellsbehandling, og deretter en avveining av begrunnelsen for å forskjellsbehandle mot hensynet til de individene som rammes av den ulike behandlingen.

Diskrimineringsvernet er også nedfelt i en rekke menneskerettighetskonvensjoner, blant annet Den europeiske menneskerettskonvensjon (EMK) artikkel 14, FNs konvensjon om sivile og politiske rettigheter (SP) artikkel 26 og FNs konvensjon om økonomiske, sosiale og kulturelle rettigheter (ØSK) artikkel 2.

Likestillings- og diskrimineringsloven § 6 forbyr direkte og indirekte diskriminering på grunn av kjønn, graviditet, permisjon ved fødsel eller adopsjon, omsorgsoppgaver, etnisitet, religion, livssyn, funksjonsnedsettelse, seksuell orientering, kjønnsidentitet, kjønnsuttrykk, alder eller kombinasjoner av disse grunnlagene.

Etnisitet er et av flere diskrimineringsgrunnlag. Med etnisitet menes blant annet nasjonal opprinnelse, avstamning, hudfarge og språk.

Med direkte forskjellsbehandling menes at en person behandles dårligere enn andre blir, har blitt eller ville blitt behandlet i en tilsvarende situasjon, på grunn av etnisitet eller en av de andre diskrimineringsgrunnene, jf. § 7. Med indirekte forskjellsbehandling menes enhver tilsynelatende nøytral bestemmelse, betingelse, praksis, handling eller unnlatelse som vil stille personer dårligere enn andre, på grunn av et av de samme forholdene.

Loven gjelder på alle samfunnsområder, både i privat og offentlig sektor, jf. § 2. Diskrimineringsforbudene gjelder alle sider av et arbeidsforhold, jf. § 29. Dette omfatter blant annet stillingsutlysning, ansettelse og omplassering. Forbudene gjelder også «arbeidsgiveres valg og behandling av selvstendig næringsdrivende og innleide arbeidstakere.».

Diskrimineringsforbudet gjelder ikke dersom forskjellsbehandlingen har en tilstrekkelig saklig begrunnelse, jf. § 9 første ledd. Forskjellsbehandling er ikke i strid med diskrimineringsforbudet når den har et saklig formål, er nødvendig for å oppnå formålet og ikke er uforholdsmessig inngripende overfor den eller de som forskjellsbehandles.

I arbeidsforhold er vernet skjerpet, jf. § 9 andre ledd:

> I arbeidsforhold og ved valg og behandling av selvstendig næringsdrivende og innleide arbeidstakere er direkte forskjellsbehandling på grunn av kjønn, etnisitet, religion, livssyn, funksjonsnedsettelse, seksuell orientering, kjønnsidentitet og kjønnsuttrykk bare tillatt hvis denne egenskapen har avgjørende betydning for utøvelsen av arbeidet eller yrket, og vilkårene i første ledd er oppfylt.

Diskrimineringsvernet betyr blant annet at all lovgivning som innebærer forskjells-behandling av etniske grupper, nasjonaliteter osv., må begrunnes særlig etter vilkårene for lovlig forskjellsbehandling i § 9.

I diskrimineringsloven § 30 er det gitt særlige regler om innhenting av opplysninger ved ansettelser:

«Arbeidsgivere må ikke i ansettelsesprosessen, herunder under intervju eller på annen måte, innhente opplysninger om en søkers

a. graviditet, adopsjon eller planer om å få barn
b. religion eller livssyn
c. etnisitet
d. funksjonsnedsettelse
e. seksuelle orientering, kjønnsidentitet eller kjønnsuttrykk.

Innhenting av opplysninger om etnisitet, religion, livssyn, funksjonsnedsettelse og samlivsform er likevel tillatt hvis opplysningene har avgjørende betydning for utøvelsen av arbeidet eller yrket.

Innhenting av opplysninger om søkerens samlivsform, religion eller livssyn er tillatt hvis virksomheten har som formål å fremme bestemte livssyn eller religiøse syn, og arbeidstakers stilling vil ha betydning for å gjennomføre formålet. Dersom slike opplysninger vil bli krevet, må dette oppgis i utlysningen av stillingen.»

## 2.7 Arbeidsmiljøloven

Arbeidsmiljøloven gjelder for enhver virksomhet som sysselsetter arbeidstakere. Loven har som formål å sikre et arbeidsmiljø som gir grunnlag for en helsefremmende og meningsfylt arbeidssituasjon, som gir full trygghet mot fysiske og psykiske skadevirkninger.

Arbeidsmiljøloven kapittel 9 regulerer kontrolltiltak i arbeidslivet, og gir både materielle og prosessuelle regler. Bestemmelsene i kapittel 9 suppleres av lovfestede og ulovfestede arbeidsrettslige og personvernrettslige regler og prinsipper, se f.eks. punkt 2.5.

Kontrolltiltak dekker et bredt spekter av tiltak, basert på ulike hensyn. Disse tiltakene varierer fra enkle kontroller, som å registrere når ansatte kommer på jobb eller å sjekke at de bruker påkrevd verneutstyr, til mer inngripende metoder som kameraovervåking eller rusmiddeltesting. Paragraf 9-1 stiller materielle krav til kontrolltiltakene som virksomheten iverksetter. Tiltaket skal ha et saklig formål som er forankret i virksomhetens behov og det må ikke medføre en uforholdsmessig belastning for arbeidstakeren, jf. bestemmelsens første ledd. Det vil si at hvert kontrolltiltak må være egnet og nødvendig, saklig begrunnet overfor den det gjelder, og ikke føre til usaklig forskjellsbehandling. Det vises for øvrig til gjennomgangen av saklighets- og forholdsmessighetskravet i punkt 4.2.

Innhenting av helseopplysninger ved ansettelse er regulert i § 9-3. Arbeidsgiver kan bare innhente opplysninger som er nødvendige for å vurdere om arbeidssøkeren kan utføre arbeidsoppgaver tillagt stillingen.

Arbeidsmiljøloven kapittel 13 har flere bestemmelser om vern mot diskriminering. Av § 13-1 følger bl.a. at direkte og indirekte diskriminering på grunn av politisk syn, medlemskap i arbeidstakerorganisasjon eller alder er forbudt. Ved diskriminering på grunn av bl.a. etnisitet, gjelder likestillings- og diskrimineringsloven, se punkt 2.6. Krav knyttet til statsborgerskap o.l. vil omfattes av «etnisitet».

Etter § 13-3 er det flere unntak fra forbudet mot diskriminering. Av første ledd følger at forskjellsbehandling som har et saklig formål, ikke er uforholdsmessig inngripende overfor den eller de som forskjellsbehandles og som er nødvendig for utøvelse av arbeid eller yrke, ikke anses som diskriminering. Videre følger av andre ledd at forskjellsbehandling som er nødvendig for å oppnå et saklig formål og som ikke er uforholdsmessig inngripende overfor den eller de som forskjellsbehandles, ikke er i strid med forbudet mot indirekte diskriminering mv.

Spørsmål om innhenting av opplysninger mens ansettelsesforholdet består, må vurderes opp mot de alminnelige regler i kapittel 13 om diskrimineringsforbud og kapittel 9 om iverksettelse av kontrolltiltak og reglene i personopplysningsloven.

## 2.8 Statsansatteloven

For arbeidstakere i statsforvaltningen suppleres arbeidsmiljølovens regler av statsansatteloven, jf. § 1. Loven gjelder imidlertid ikke for ansatte i helseforetakene, jf. helseforetaksloven § 5 andre ledd. I tillegg er forvaltningsloven sentral for arbeidsforhold som omfattes av statsansatteloven. Dette gjelder særlig saksbehandlingsreglene som på enkelte områder supplerer statsansatteloven.

Det følger av statsansatteloven § 3 (kvalifikasjonsprinsippet) at den best kvalifiserte søkeren skal ansettes eller utnevnes i ledig stilling eller embete, med mindre det er gjort unntak i lov eller forskrift. Videre følger at det ved vurderingen av hvem som er best

kvalifisert, skal det legges vekt på utdanning, erfaring og personlig egnethet, sammenholdt med kvalifikasjonskravene som er fastsatt i utlysningen. Muligheten for at den ansatte kan bli adgangsklarert må kunne innfortolkes som et kvalifikasjonskrav slik at kvalifikasjonsprinsippet i § 3 ikke er til hinder for en utvelgelse av arbeidstakere basert på mulighet for klarering.

# 3 Lov om digital sikkerhet og to nye EU-direktiver

NIS2-direktivet (EU) 2022/2555 ble vedtatt i EU 14. desember 2022 og skal erstatte NIS1-direktivet (EU) 2016/1148. NIS2-direktivet er en del av en større pakke med tiltak fra EU, hvor også direktiv (EU) 2022/2557 om kritiske enheters motstandsdyktighet (CER-direktivet) inngår.

Medlemsstatene skal sikre en koordinert gjennomføring av NIS2-direktivet og CER-direktivet. Etter direktivene skal nødvendige nasjonale regelverksendringer være på plass innen 17. oktober 2024, og tre i kraft dagen etter.

I Norge er NIS1 implementert gjennom lov om digital sikkerhet, se Prop. 109 LS (2022–2023)/Innst. 78 L (2023-2024) Lov om digital sikkerhet (digitalsikkerhetsloven) og samtykke til godkjenning av EØS-komiteens beslutninger nr. 21/2023 og 22/2023 om innlemmelse i EØS-avtalen av direktiv (EU) 2016/1148 og forordningene (EU) 2018/151 og (EU) 2019/881. Digitalsikkerhetsloven er behandlet i Stortinget, ble sanksjonert i statsråd i desember 2023 og trer i kraft fra den tiden Kongen bestemmer.

Prop. 109 LS ba også Stortinget om samtykke til godkjenning av to beslutninger i EØS-komiteen om innlemmelse i EØS-avtalen av NIS1-direktivet, tilhørende gjennomføringsforordning og cybersikkerhetsforordningen.

Lov om digital sikkerhet forplikter virksomheter som har en særlig viktig rolle for å opprettholde kritisk samfunnsmessig og økonomisk aktivitet, til å overholde digitale sikkerhetskrav og varsle om alvorlige digitale hendelser. Loven stiller overordnede krav til sikkerhet og varsling, og virkeområdet er kun angitt i form av hvilke sektorer den gjelder i. Dette forutsetter et underliggende regelverk med tydeligere avgrensinger og konkretiseringer. Loven inneholder derfor en vid adgang til å fastsette nærmere bestemmelser i forskrift. Loven etablerer rammeverk for tilsyn med virksomhetene og åpner for ileggelse av pålegg og eventuelt overtredelsesgebyr ved manglende oppfyllelse av pliktene. Myndighetene skal også ta imot varsler om alvorlige digitale hendelser.

## 3.1 NIS2-direktivet (EU) 2022/2555 om tiltak for å sikre et høyt felles nivå for sikkerhet i nettverks- og informasjonssystemer

NIS2-direktivet (EU) 2022/2555 om tiltak for å sikre et høyt felles nivå for sikkerhet i nettverks- og informasjonssystemer, er markert som EØS-relevant.

Formålet med NIS2-direktivet er å øke motstandsdyktigheten i nettverks- og informasjonssystemer til både private og offentlige aktører i EU, redusere fragmenteringen i sektorer som allerede er omfattet av NIS-direktivet og øke felles bevissthet og kapasitet knyttet til motstandsdyktighet.

NIS2-direktivet er omfattende og berører mange ulike samfunnssektorer. Direktivet utvider virkeområdet i forhold til NIS1-direktivet, ved å innlemme flere sektorer som anses som kritiske for både økonomien og samfunnet, herunder forskning. Videre skjerpes kravene til virksomhetenes risikovurdering av nettverks- og informasjonssystemer og det innføres mer presise rapporteringskrav. Dessuten harmoniseres sanksjonsbestemmelsene.

*Virkeområde*

Alle virksomheter av en viss størrelse og en viss type (fastsatt i direktivet) er omfattet. Også mindre virksomheter som anses å ha en nøkkelrolle for samfunnet, økonomien eller en viss sektor, er omfattet. Tilbydere av samfunnsviktige tjenester innen 18 definerte sektorer omfattes. Direktivet skiller mellom mer og mindre samfunnsviktige tjenester («vesentlige» og «viktige»), og alle fremgår av direktivets vedlegg.

De «vesentlige tjenestene» fremgår av direktivets vedlegg 1. Denne gruppen omfatter utvalgte offentlige eller private tilbydere av samfunnsviktige tjenester, herunder helse, drikkevann, digital infrastruktur, IKT-tjenester og offentlig forvaltning (sentral og regional).

Den «viktige» gruppen omfatter tilbydere oppført i vedlegg 2, som bl.a. omfatter produksjon av bl.a. medisinsk utstyr, IKT-utstyr, kjøretøy, elektronikk, maskiner, transportutstyr, og tilbydere av digitale tjenester og forskning.

Klassifisering og inndeling i to ulike kategorier, medfører to ulike tilsynsregimer.

Det enkelte land kan velge å gjøre direktivet gjeldende også for lokalforvaltningen og utdanningsinstitusjoner, jf. artikkel 2 nr. 5.

I likhet med NIS1 oppstiller NIS2 et generelt unntak fra sikkerhets- og varslingskravene, samt tilsynsbestemmelsene, for virksomheter som er omfattet av sektorspesifikke EU-regler som minst tilsvarer kravene i NIS2, jf. artikkel 4.

*Sikkerhetskrav*

Tilbydere skal iverksette hensiktsmessige og proporsjonale tekniske og organisatoriske tiltak for å håndtere risiko i nettverk og informasjonssystemer, jf. artikkel 21 nr. 2. Dette følger også av gjeldende direktiv (NIS1). I samme artikkel oppstilles det i tillegg en risikostyringsmetode, med en minimumsliste med grunnleggende sikkerhetselementer som må legges til grunn for sikkerhetsarbeidet. Dette gjelder blant annet krav om at tilbydere må håndtere cybersikkerhetsrisiko i forsyningskjeder og hos leverandører, planer for vedlikehold, overvåkning og testing samt bruk av krypto.

*Tilsyn med tilbydere*

Bestemmelsene om tilsyn skiller mellom tilbydere av «vesentlige» og «viktige» samfunnsviktige tjenester. Tilbydere av «viktige» samfunnsviktige tjenester skal underlegges et mindre strengt tilsynsregime enn tilbydere av «vesentlige» samfunnsviktige tjenester (se artiklene 32 og 33). For eksempel skal tilsyn overfor tilbydere av «viktige» samfunnsviktige tjenester kun skje dersom det foreligger informasjon om at tilbyderen ikke overholder kravene i direktivet. Noe forenklet innebærer dette at tilbydere av «vesentlige» tjenester kan bli gjenstand for uanmeldt tilsyn, mens dette ikke er tilfellet for de «viktige» tjenestene. Dette tilsvarer forskjellen mellom tilbydere av samfunnsviktige tjenester og digitale tjenester etter dagens direktiv (NIS1). Ellers innfører direktivet mer detaljerte og strengere tiltak for nasjonale tilsynsmyndigheter og tar sikte på å harmonisere sanksjonsregimer i medlemsstatene.

## 3.2 CER-direktivet (EU) 2022/2557 om kritiske enheters motstandsdyktighet

Direktiv (EU) 2022/2557 av 14. desember 2022 om kritiske enheters motstandsdyktighet (CER-direktivet) er markert som EØS-relevant.

Direktivets formål og virkeområde er regulert i artikkel 1. Det følger av bestemmelsen at medlemsstatene skal treffe konkrete foranstaltninger for å sikre at tjenester, som er vesentlige for å opprettholde vitale samfunnsmessige funksjoner eller økonomiske aktiviteter, leveres uhindret i det indre markedet. Dette omfatter bl.a. å identifisere kritiske enheter og støtte disse i å oppfylle forpliktelsene de er pålagt, se bokstav a. Videre følger det i bokstav b forpliktelser for kritiske enheter til å styrke deres motstandsdyktighet og evne til at levere tjenestene. Direktivet fastsetter også regler for bl.a. tilsyn med kritiske enheter, håndhevelse og identifisering av kritiske enheter av særlig europeisk betydning, se bokstav c. Spørsmål knyttet til cybersikkerhet er omhandlet i NIS2 direktivet.

Artikkel 13 regulerer kritiske enheters tiltak for motstandsdyktighet. Av nr. 1 følger at medlemsstatene skal sikre at kritiske enheter treffer passende og forholdsmessige tekniske, sikkerhetsmessige og organisatoriske tiltak for å sikre deres motstandsdyktighet. Dette skal gjøres på grunnlag av de relevante opplysningene som medlemsstatene har gitt om risikovurderingen, og av resultatene av de kritiske enhetenes risikovurderinger. Dette omfatter bl.a. tiltak som er nødvendige for å sikre tilstrekkelig fysisk beskyttelse av lokaler og kritisk infrastruktur, herunder barrierer, verktøy og rutiner for overvåkning, deteksjonsutstyr og adgangskontroll (bokstav b). Videre skal det sikres passende styring av medarbeidersikkerheten, som fastsettelse av kategorier av personale som innehar kritiske funksjoner, fastleggelse av adgangsrettigheter til lokaler, kritisk infrastruktur og sensitive opplysninger, prosedyrer for bakgrunnskontroll etter artikkel 14 og utpeking av kategorier av personer, som er forpliktet til å gjennomgå slik bakgrunnskontroll (bokstav e). Dette gjelder også bruk av eksterne tjenestetilbydere i kritiske enheter.

Medlemsstatene skal også sikre at kritiske enheter har innført og anvender en plan for motstandsdyktighet eller et eller flere tilsvarende dokumenter, som beskriver tiltakene, jf. nr. 2.

Artikkel 14 gjelder bakgrunnskontroll. Medlemsstatene skal angi på hvilke betingelser en kritisk enhet i særlige tilfeller og med hensyn til risikovurderingen, har tillatelse til å inngi anmodninger om bakgrunnskontroll av personer, som bl.a. ivaretar sensitive oppgaver i eller til fordel for en kritisk enhet, er bemyndiget til å få direkte adgang eller fjernadgang til en kritisk enhets lokaler, opplysninger eller kontrollsystemer, herunder i forbindelse med den kritiske enhets sikkerhet eller overveies ansatt i stillinger som omfattes av disse kriteriene.

Bakgrunnskontroll skal være forholdsmessig og strengt begrenset til det som er nødvendig. Den foretas utelukkende for å vurdere en potensiell sikkerhetsrisiko for den berørte kritiske enhet. En bakgrunnskontroll skal minst bekrefte identiteten til den personen som er gjenstand for bakgrunnskontrollen og kontrollere strafferegistrene for

den angjeldende person for så vidt angår lovovertredelser, som ville være relevante for en bestemt stilling.

Ved bakgrunnskontroll skal det europeiske informasjonssystemet for strafferegistre benyttes.

# 4 Risikobildet og behovet for tiltak

## 4.1 Den sikkerhetspolitiske situasjonen

Den sikkerhetspolitiske situasjonen i Norge er mer uforutsigbar enn på mange år. Dette vil kunne true helse- og omsorgstjenestens evne til å ivareta sine oppgaver. De siste årene har hendelser som Russlands invasjon av Ukraina, sabotasje og innsidevirksomhet preget trusselbildet. Det er viktigere enn noen gang at vi samarbeider om å verne verdier og kritiske samfunnsfunksjoner. Evnen til å levere helsetjenester av god kvalitet med tilstrekkelig pasientsikkerhet, er en slik samfunnskritisk funksjon. For å beskytte oss mot forskjellige trusler kreves det godt sikkerhets- og beredskapsarbeid på tvers av sektorer, og i den enkelte virksomhet og hos den enkelte medarbeider.

Når trussel- og risikobilde er i stadig og rask endring, er det krevende å gjennomføre risiko- og sårbarhetsanalyser som grunnlag for langsiktige beslutninger. Dette understreker behovet for at helse- og omsorgssektoren har et klart regelverk og enhetlig krav å forholde seg til. Det synliggjør også viktigheten av tett samarbeid med tjenestene som tegner dagens trusselbilde og miljøer som studerer mer langsiktige trender.

I nasjonal trusselvurdering (NTV) for 2024 gir PST en ugradert redegjørelse av trusselbildet som det norske samfunnet står overfor dette året. Vurderingen setter søkelys på etterretningstrusselen, med særskilt vekt på russisk og kinesisk etterretning, samt på terrortrusselen og trusler mot myndighetspersoner. Den delen som gjelder statlig etterretningsvirksomhet, er oppsummert slik:

> «Russlands angrepskrig i Ukraina har skapt en ny sikkerhetspolitisk situasjon som påvirker trusselbildet i Norge. Krigen bidrar til å skjerpe etterretningstrusselen fra Russland sammenlignet med før invasjonen. Samtidig gjør Norges NATO-medlemskap og vår felles grense at Russland vil bruke etterretningstjenestene sine mot norske mål i overskuelig fremtid.
>
> I dagens sikkerhetspolitiske klima er også etterretningstrusselen fra Kina betydelig. Etter vår vurdering vil trusselen tilta de nærmeste årene. Dette skyldes blant annet Kinas posisjonering i nordområdene, et forverret forhold mellom Kina og Vesten samt et kinesisk ønske om kontroll over kritiske forsyningskjeder.
>
> I tillegg forventer vi fortsatt aktivitet fra Iran og Nord-Korea mot norske mål i 2024.»

Nasjonal sikkerhetsmyndighet (NSM) oppsummerer i rapporten «Risiko 2024» situasjonen slik:

> «Situasjonsforståelsen må styrkes i hele samfunnet. For virksomheter innebærer det å kartlegge virksomhetens verdier, avhengigheter og relevante trusler. Det sammensatte og dynamiske trusselbildet som Etterretningstjenesten og PST beskriver, gjør helhetlig, forebyggende sikkerhetsarbeid enda viktigere. Det nytter ikke med eksempelvis gode fysiske sikringstiltak dersom virksomhetens verdier enkelt kan rammes digitalt eller gjennom leverandørkjeden. Bortfall av en underleverandør kan få alvorlige konsekvenser, ikke bare for selskaper med avhengighetsforhold, men også for nasjonal sikkerhet.
>
> Kritisk infrastruktur må skjermes mot innsyn og påvirkning. Både utenlandske oppkjøp og investeringer i norske selskaper og anskaffelser må i større grad ses i sammenheng med

> nasjonal sikkerhet. Importert teknologi kan være utstyrt med skjulte bakdører eller sårbarheter som kan utnyttes. […]
>
> Cybersikkerheten i virksomheter og hos myndigheter utfordres av stadig mer avanserte cyberoperasjoner. Kunstig intelligens må tas i bruk for å styrke analyse og avdekking av cyberoperasjoner. Samtidig må brukere av kunstig intelligens-modeller være bevisst på sårbarheter i teknologien som kan utnyttes av trusselaktører. Kunstig intelligens gjør fabrikkerte nyheter stadig mer troverdige. Kombinert med at desinformasjon kan spres på en helt annen skala enn tidligere, utfordres grunnmuren i demokratiske styresett.»

I Fokus 2024 uttaler Etterretningstjenesten:

> «Det er en vedvarende risiko for at vestlig teknologi får militær anvendelse i Russland, Kina, Iran og Nord-Korea. Innviklede eierstrukturer og uoversiktlige forsyningskjeder benyttes for å omgå vestlig eksportregelverk. Internasjonalt forskningssamarbeid blir utnyttet for kunnskapsoverføring til militære formål ved siden av det uttrykte formålet.
>
> Statlig kontroll over kommersielle interesser er økende både i Russland og Kina. Moskva har knyttet tettere bånd til næringsaktører. Beijing har lenge utøvd et svært aktivt statlig eierskap, eier stadig større andeler i kinesisk næringsliv og innfører stadig strengere lovverk, med krav om at selskap og enkeltpersoner understøtter partistatens målsettinger. Myndighetene i begge land øver press på næringslivsledere.
>
> Russland, Iran og Nord-Korea har alle sterke miljøer på enkelte teknologiområder med militær anvendelse. Kina er likevel på et eget nivå når det gjelder bredden i ekspertise.»

Norsk helsenett SF (Helse- og kommuneCERT), har i situasjonsbilde oppdatert januar 2024 uttalt:

- Det er meget sannsynlig at fremmede stater ser på helsesektoren som et mål for spionasje.
- Det er sannsynlig at norsk helse- og kommunesektor vil treffes av angrep fra aktører som et ledd i det generelle arbeidet til statlige eller stats-sponsede etterretningstjenester.

Departementet mener den teknologiske utviklingen gjør det nødvendig med endringer i bestemmelsene om informasjonssikkerhet i pasientjournalloven og helseregisterloven. Truslene mot viktige samfunnsfunksjoner som understøtter nasjonale sikkerhetsinteresser representeres i stor grad av sofistikerte angripere med høy evne og kapasitet. Aktørene kan være statlige eller statsfinansierte grupper som bryter seg inn i IKT-systemer for å påføre skade eller hente informasjon som kan benyttes for å nå økonomiske, politiske eller militære mål. Statlige aktører kan være andre staters etterretnings- og sikkerhetstjenester, inkludert aktører engasjert av disse. Motivene kan i ytterste konsekvens være forberedelser til fremtidige sabotasjeoperasjoner, terrorisme eller krig. Utsatte grupper er leverandører, utviklere og operatører knyttet til kritisk infrastruktur, for eksempel i forbindelse med plassering av digitale bakdører og utro tjenere.

Den digitale trusselen er skjerpet. Tidligere var digitale sårbarheter først og fremst et tema for tradisjonell informasjons- og kommunikasjonsteknologi. De seneste år har man imidlertid blitt oppmerksom på mulighetene for bevisste anslag, også mot helse- og omsorgssektoren. Fremmede makter kan gjennom nettverksbaserte etterretningsoperasjoner i fredstid erverve inngående kjennskap til kritisk infrastruktur.

Kunnskapen kan senere benyttes til å gjennomføre intenderte uønskede hendelser. Flere land utvikler skadevare som vil kunne brukes til å sabotere infrastruktur eller forstyrre kritiske samfunnsfunksjoner. På den annen side arbeides det aktivt for å utbedre feil, tette smutthull og øke forsvarsevnen. Utviklingen minner mer og mer om et våpenkappløp. Skadevare kan ramme alle systemer som er koblet til et nettverk. Brannmurer og antivirusprogramvare er ingen garanti mot kompromittering, selv om slike tiltak reduserer risikoen.

Endringene i risikobildet synliggjør et behov for regelendringer for bedre å kunne ivareta helse- og omsorgstjenestens oppgaver og den enkeltes personvern, ved å redusere risiko for at utro tjenere ansettes i kritiske stillinger og at store sett med helsedata ikke blir tilgjengelig for aktører som kan utgjøre en trussel.

## 4.2 Bakgrunnssjekk av personell

### 4.2.1 Bakgrunn

Den sikkerhetspolitiske situasjonen og risikobildet har endret seg de siste årene. Lav eller manglende sikkerhetsmessig bevissthet kan øke risikoen for at personell kompromitterer sensitiv informasjon og blir bevisste eller ubevisste innsidere. For å sikre helse- og omsorgstjenestens evne til å ivareta sine oppgaver, personvern og grunnleggende sikkerhet, og øke den nasjonale motstandskraften mot dagens sammensatte trusselbilde, er det nødvendig med god sikkerhetsstyring og daglig sikkerhetsmessig ledelse i virksomhetene. For å sikre et forsvarlig sikkerhetsnivå og beskyttelse av nasjonale verdier, er det også nødvendig med høy sikkerhetsmessig bevissthet hos personellet.

En innsidetrussel er en sikkerhetsrisiko knyttet til en person innen virksomheten. Det oppstår vanligvis ved at en nåværende eller tidligere ansatt, entreprenør, leverandør eller partner med legitim tilgang, misbruker sin tilgang til skade for virksomhetens nettverk, systemer og data. En innsidehandling kan utføres med vilje (tilsiktet) eller utilsiktet. Fordi innsideren har legitim tilgang, er det vanskelig for sikkerhetsfagfolk og applikasjoner å skille mellom normal og skadelig aktivitet:

> «Metodene flere etterretningstjenester bruker, er sofistikerte og utspekulerte. De kan være krevende å avdekke. Imidlertid vil gode personellmessige, fysiske, organisatoriske og digitale sikringstiltak redusere risikoen for at innsidere gjør skade på virksomheten og nasjonal sikkerhet» (NSM Risiko 2024).

Etter hvert som informasjonssystemer i større grad regionaliseres og eventuelt nasjonaliseres, vil også mer informasjon sentraliseres i felles systemer, hvilket igjen øker konsekvensen ved etterretnings- og informasjonsuthentingsoperasjoner. Dette vil kunne ha betydning for vår evne til å levere helse- og omsorgstjenester av høy kvalitet.

Bakgrunnssjekk er en form for egnethetsvurdering av personell. Bakgrunnssjekk er et inngripende tiltak, og skal ikke gjennomføres i større grad enn nødvendig for å redusere risiko. Den avgjørende vurderingen opp mot diskrimineringsvernet, er om en forskjellsbehandling er usaklig eller uforholdsmessig. Forskjellsbehandlingen må ha en

viss sammenheng med kjønn, alder, religion, livssyn, funksjonsnedsettelse eller andre vesentlige forhold ved en person for å være i strid med diskrimineringsvernet. Krav knyttet til statsborgerskap kan være et slikt element.

Luftfartstilsynet gjennomfører bakgrunnssjekk av personer som arbeider i eller har tilknytning til luftfart. Hvordan bakgrunnssjekken utføres er regulert i lov 11. juni 1993 nr. 101 om luftfart (luftfartsloven) § 7-25 og forskrift 1. mars 2011 nr. 214 om forebyggelse av anslag mot sikkerheten i luftfarten mv (securityforskriften). Videre kan det, etter luftfartsloven § 7-24 i forskrift stilles krav til vandel for personer som har adgang til og ferdes på landingsplasser og andre luftfartsanlegg, og bestemmes hvilke vandelskrav som skal gjelde.

Kravet om bakgrunnssjekk i luftfarten følger av EØS-regelverk (Kommisjonens gjennomføringsforordning (EU) 2015/1998 av 5. november 2015 om fastsettelse av detaljerte tiltak for gjennomføring av de felles grunnleggende standardene for luftfartssikkerhet artikkel 1.2.3.1 i vedlegget til forordningen (gjennomføringsforordningen)). Gjennomføringsforordningen er gjennomført i securityforskriften § 3, som blant annet er hjemlet i luftfartsloven § 7-24. I henhold til gjennomføringsforordningens vedlegg punkt 11.1.3 skal en bakgrunnssjekk minst bestå av følgende elementer:

- fastslå personens identitet på grunnlag av dokumentasjon
- vurdering av søkers politiattest
- oversikt over arbeid, utdanning og oppholdssted de fem siste år.

Etter sikkerhetsloven stilles det krav til klarering og hva som skal vektlegges i vurderingen, jf. lovens kapittel 8 og klareringsforskriften. Videre er det i sikkerhetsloven etablert en egen metodikk for hvordan mulige skjermingsverdige verdier, infrastruktur og informasjon og informasjonssystem skal kartlegges. Denne metodikken kan også benyttes for å identifisere stillinger og funksjoner der det kan være aktuelt å stille krav om bakgrunnssjekk etter helselovgivningen.

Metodikken kan gjenbrukes til å gi god oversikt over verdier som ikke dekkes av sikkerhetsloven, men som likevel kan ha betydning for helse- og omsorgstjenestens evne til å ivareta sine oppgaver, befolkningens helse og personvern, og nasjonale sikkerhetsinteresser. Dette kan være fysiske, digitale og andre verdier. Samtidig må en oversikt over verdier ses i sammenheng med trussel- og risikobildet, for å forstå egne sårbarheter og for å kunne ivareta egen sikkerhet.

Innen helse- og omsorgssektoren vil det primært være de fire regionale IKT-leverandørene, de regionale helseforetakene, enkelte helseforetak, Norsk helsenett SF, Helseplattformen AS, Folkehelseinstituttet, Direktoratet for strålevern og atomberedskap og Helsedirektoratet som vil ha behov for å kunne få utført bakgrunnssjekk av personell.

### 4.2.2 Departementets vurderinger og forslag

Enkelte IKT-systemer og helseregistre er av en slik art, at karakteren av og det store volumet av informasjon tilsier at det ikke skal være rimelig grunn til å tvile på at personell

med driftstilgang er sikkerhetsmessig skikket. Dette er personell i roller med stor og utvidet tilgang til helse- og personopplysninger som kan være av interesse for en trusselutøver, og hvor personellet alene eller sammen med andre kan gjøre stor skade og kunne true helse- og omsorgstjenestens evne til å ivareta sine oppgaver. Departementet har blitt orientert om at dette også kan gjelde selv om informasjonen i seg selv ikke faller inn under sikkerhetslovens bestemmelser om skjermingsverdig informasjon, og systemet i seg selv ikke faller inn under bestemmelsene om skjermingsverdig informasjonssystem. Uten egen lovhjemmel, er det begrenset anledning til bakgrunnssjekk av den enkelte som innehar eller søker en kritisk stilling. Lovhjemmel vil også bidra til etterlevelse av personvernforordningens prinsipper om lovlighet, rettferdighet og åpenhet, jf. artikkel 5.

Departementet mener behovet for å vurdere om personellet er sikkerhetsmessig skikket gjennom en bakgrunnssjekk er reelt, og at det derfor er nødvendig å regulere dette i lov. Det angjeldende personellet vil være bemyndiget til å få direkte adgang eller fjernadgang, til en kritisk enhets lokaler, opplysninger eller kontrollsystemer. Personellet vil på denne måten kunne innhente eller ha direkte tilgang til en rekke ulike kliniske, kvalitetsmessige, økonomiske og administrative datakilder med store mengder person- og helseopplysninger. Gjennom misbruk av sin stilling kan personell i disse rollene skade dataenes integritet, tilgjengelighet og konfidensialitet. Dette vil kunne true helse- og omsorgstjenestens evne til å ivareta sine oppgaver. Potensiale for skade er stort.

I dag benytter virksomhetene ulike tiltak for å vurdere om personellet er skikket, bl.a. såkalte «sårbarhetssamtaler». Dette er verdifullt som en normativ forventningsavklaring og tydeliggjøring av personellets plikter, men vil ikke kunne brukes til å oppdage eller gjenkjenne en ondsinnet aktør.

Departementet har sammen med sektoren identifisert og vurdert aktuelle informasjonssystemer, objekter og infrastruktur og foretatt utpeking og klassifisering av skjermingsverdige verdier i samsvar med krav i sikkerhetsloven og forskrifter gitt i medhold av loven. Som en konsekvens av dette arbeidet og som en oppfølging av Meld. St. 9 (2022–2023), har Helse- og omsorgsdepartementet vurdert at det er nødvendig å redusere risiko for at utro tjenere (innsidetrussel) ansettes i kritiske stillinger med adgang til enkelte typer objekter og infrastruktur, hvor det behandles kritisk informasjon eller store datamengder.

Departementet mener det er behov for å kunne stille krav til bakgrunnssjekk av personell i kritiske stillinger og funksjoner, ut over det som følger av sikkerhetsloven. Dette gjelder personell knyttet til objekter og informasjonssystemer som ikke inneholder sikkerhetsgradert informasjon og ikke er utpekt som skjermingsverdig objekt, infrastruktur eller verdier. Informasjonen personellet vil ha tilgang til, vil likevel kunne ha betydning for nasjonale sikkerhetsinteresser dersom den blir kompromittert. Informasjonen vil også ha betydning for ivaretakelse av helse- og omsorgstjenestens oppgaver, befolkningens helse og den enkeltes personvern. Sikkerhetslovens krav til autorisasjon og sikkerhetsklarering for tilgang til informasjonen, samt krav til adgangsklarering for tilgang til skjermingsverdig objekt og infrastruktur, er derfor ikke anvendbar.

Det er nødvendig å sikre et forsvarlig sikkerhetsnivå, bl.a. ved å stille krav om at personell i kritiske stillinger og funksjoner er vurdert sikkerhetsmessig skikket, og at vi kan ha begrunnet tillit til at personellet har den nødvendige pålitelighet, lojalitet og dømmekraft som stillingen forutsetter.

Departementet er av den oppfatning at slik tillit fordrer bakgrunnssjekk av personellet basert på relevante kilder. Ved å kunne benytte bakgrunnssjekk ved ansettelser til disse stillingene, vil sannsynligheten for ondsinnede angrep i form av vitende eller uvitende innsidere reduseres. Dette vil styrke pasientsikkerheten. Med bakgrunnssjekk menes her altså noe annet enn den type sjekk som i dag benyttes i rekrutteringssammenheng, som et begrep for sjekk av arbeidssøkers CV, utdanning mv. i ansettelsesprosesser. Departementet foreslår videre at det presiseres i pasientjournalloven § 22 og helseregisterloven § 21 at det ved vurderingen av hva som er et forsvarlig sikkerhetsnivå, også skal tas hensyn til den teknologiske utviklingen og nasjonale sikkerhetsinteresser.

De aktuelle virksomhetene har etablert rutiner og praksis iht. sikkerhetsloven for sikkerhetsklarering og autorisering av eget personell. Det er imidlertid en vesentlig begrensning at klareringshjemmelen er forankret i sikkerhetsloven. Dette betyr at denne typen bakgrunnssjekk kun kommer til anvendelse om objektet, informasjon eller informasjonssystemet er underlagt sikkerhetsloven eller utpekt som skjermingsverdig verdi.

Det vil alltid være informasjon og informasjonssystemer i skjæringspunktet mellom det som utpekes og klassifiseres etter sikkerhetsloven og annen informasjon og systemer som også kan ha betydning for helse- og omsorgstjenestens evne til å ivareta sine oppgaver og nasjonale sikkerhetsinteresser. Bakgrunnssjekk etter forslaget her vil redusere muligheten for at personer som representerer en sikkerhetsrisiko gis adgang til informasjonssystemer hvor det behandles store datamengder og det aggregerte tilgangsnivået vil være svært høyt.

*Saklig og forholdsmessig - diskrimineringsvern*

Bakgrunnssjekk av personell kan være problematisk i forhold til arbeidslivslovgivningen og diskrimineringsloven, særlig fordi det kan komme i konflikt med personvernhensyn og diskrimineringsforbud. Departementet er opptatt av at bakgrunnssjekk skal være forholdsmessig og begrenset til det som er nødvendig. Slik kontroll skal foretas utelukkende for å vurdere en mulig sikkerhetsrisiko for den berørte kritiske enhet.

Bakgrunnssjekk vil være ekskluderende fordi det innebærer en grundig vurdering av en persons bakgrunn, inkludert politiattest, oversikt over arbeid, utdanning, oppholdssted, økonomisk situasjon og andre personlige forhold. Søkerens nasjonalitet, landbakgrunn o.l. vil også kunne inngå i denne vurderingen. Vurderingen kan føre til at personer som tidligere har hatt problemer, selv de som ikke nødvendigvis er relevante for jobben de søker, kan bli utelukket fra ansettelse.

Vektlegging av nasjonalitet, landbakgrunn o.l. kan støte an mot forbudet mot diskriminering på grunn av etnisitet. Retten til å ikke bli diskriminert er en grunnleggende

menneskerettighet, som er gjennomført i norsk rett blant annet i Grunnloven § 98 og likestillings- og diskrimineringsloven, se omtale i 2.6 om diskrimineringsvern.

Den avgjørende vurderingen opp mot diskrimineringsvernet, er om forskjellsbehandlingen er saklig, nødvendig og forholdsmessig. Det følger av likestillings- og diskrimineringsloven § 9 at forskjellsbehandlingen ikke er i strid med diskrimineringsforbudet når den 1) har et saklig formål, 2) er nødvendig for å oppnå formålet og 3) den ikke er uforholdsmessig inngripende overfor den eller de som forskjellsbehandles.

Det er derfor viktig at prosessen med bakgrunnssjekk er transparent, rettferdig og proporsjonal, og at den ikke diskriminerer urimelig mot enkelte grupper eller individer. Det er også viktig at det finnes klare og rettferdige klageprosesser. Det er viktig at bakgrunnssjekken gjennomføres på en måte som er proporsjonal med jobbens natur og krav, og at den respekterer arbeidstakeres og arbeidssøkeres rettigheter og verdighet.

Departementet mener at et krav om bakgrunnssjekk med vektlegging av nasjonalitet, landbakgrunn o.l. kan være saklig, nødvendig og forholdsmessig, og således ikke diskriminerende. Departementet vil også påpeke at tiltakene skal baseres på en konkret vurdering av den enkelte tilsetting mv. og sikkerhetsrisiko knyttet til de oppgavene og rollene den enkelte skal ha.

Videre må tiltakene vurderes konkret for den enkelte søkeren, ut fra om det er rimelig grunn til å tvile på at personen er sikkerhetsmessig skikket. I tillegg til de ordinære vurderingskriteriene, skal det legges vekt på hjemlandets sikkerhetsmessige betydning, personens tilknytning til hjemlandet og tilknytningen til Norge. Ved bakgrunnssjekk av en person med utenlandsk statsborgerskap skal det vurderes særskilt om bruk av vilkår, kan være et risikoreduserende tiltak. Krav til botid i Norge eller et annet land hvor vi har reell mulighet til å fastslå personens identitet på grunnlag av dokumentasjon, vurdering av politiattest, oversikt over arbeid, utdanning og oppholdssted de siste årene, kan være viktige elementer i en slik vurdering.

*Forslag til lovendringer*

Departementet foreslår krav om bakgrunnssjekk av visse typer personell, utover de som allerede er sikkerhetsklarerte. Kravet skal også gjelde ved utlysning av stillinger og i ansettelsesprosesser. Kravet fastsettes i pasientjournalloven, helsepersonelloven og helseregisterloven. Forslaget omfatter situasjoner der den enkelte datakilde ikke er vurdert å være skjermingsverdig etter sikkerhetsloven, men hvor det aggregerte tilgangsnivået likevel vil være svært høyt.

Behovet for å kunne utføre bakgrunnssjekk er begrenset og gjelder personell som er bemyndiget til å få direkte adgang eller fjernadgang til en kritisk enhets lokaler, opplysninger eller kontrollsystemer. «Normale brukere» vil ikke ha et tilgangsnivå som medfører denne type risiko. Med kritisk enhet menes i denne sammenheng områder hvor det behandles store datamengder. I CER-direktivet (artikkel 2 nr. 1) er kritisk enhet: «en offentlig eller privat enhed, som er blevet identificeret af en medlemsstat i overensstemmelse med artikel 6 som tilhørende en af kategorierne anført i […]».

Forslagets virkeområde er personell i roller med stor og utvidet tilgang til helsedata som kan være av interesse for en trusselutøver, og hvor personell alene eller sammen med andre kan gjøre stor skade og kunne true helse- og omsorgstjenestens evne til å ivareta sine oppgaver. Det gjelder personell med tekniske tilganger til data i et stort omfang, med mulighet til å se hele eller store deler av databaser, ikke bare enkeltoppslag. Det kan gjelde personell som arbeider med tilgangsstyring av prioriterte tilganger, personell som arbeider med kjernenettverk, sentrale virtualiseringsprosesser og sentral databaseinfrastruktur, dataanalytikere med store tilgangsrettigheter, databaseadministratorer for større databaser, sikkerhetsledere, sikkerhetsanalytikere, dokumentasjonsforvaltere mv.

Dette er tilganger som gjør at personellet kan opparbeide seg dyp og omfattende kunnskap om virksomhetskritisk informasjon over tid, herunder informasjon om tekniske og organisatoriske sårbarheter, anbudsdokumenter, store mengder med logginformasjon, tilgang til å se hva ansatte gjør på sine pc'er eller tilgang til andre ansattes e-poster. Det vil også kunne være tekniske tilganger til nasjonalt kritisk infrastruktur som ikke er underlagt sikkerhetsloven. Det vil imidlertid også kunne omfatte utviklere av kritiske løsninger, som gjennom tilsiktede handlinger kan legge inn ondsinnet kode/bakdør, og som om det settes i produksjon og misbrukes, kan volde stor skade. Dette vil også kunne gjelde forskere med tilgang til denne type datasett. I lovforslaget er dette beskrevet som en «bred» tilgang.

Dette vil også kunne omfatte forskere og annen sekundærbruk, med tilgang til store datasett med person- og helseopplysninger eller informasjonssystemer hvor det behandles store aggregerte datamengder med person- og helseopplysninger.

Etter forslaget skal den enkelte virksomhet påse at personell, som etter en bakgrunnssjekk ikke fremstår som egnet, ikke gis tilgang til objekter og infrastruktur med informasjon som antas å ha betydning for større gruppers personvern, helse- og omsorgstjenestens evne til å yte forsvarlige helsetjenester og nasjonale sikkerhetsinteresser. Et slikt krav skal også gjelde ved bruk av eksterne tjenestetilbydere. Forslaget omfatter både rekrutteringssituasjoner og situasjoner hvor personellet vil miste tilgangen etter å ha tiltrådt stillingen. Konsekvensen og den videre prosessen vil være ulike i de to typetilfellene. I det første tilfellet vil vedkommende normalt ikke kunne ansettes, i det andre tilfelle må det vurderes andre oppgaver for vedkommende eller eventuelt oppsigelse hvis det ikke er mulig å finne annet passende arbeid.

Departementet foreslår at det i pasientjournalloven § 22 og helseregisterloven § 21 presiseres at departementet i forskrift kan fastsette nærmere krav til tekniske og organisatoriske sikkerhetstiltak. Hensynet til nasjonale sikkerhetsinteresser vil etter forslaget være et egnet grunnlag for slike forskrifter. Departementet forslår også to nye bestemmelser, hhv. pasientjournalloven § 22a og helseregisterloven § 21a om bakgrunnssjekk.

Pasientjournalloven § 22 og helseregisterloven § 21 regulerer informasjonssikkerhet ved behandling av personopplysninger. Bestemmelsene er begrenset til å gjelde ved

behandling av personopplysninger gjennom henvisning til personvernforordningen artikkel 32. Dette ivaretar ikke andre sikkerhetsutfordringer, herunder behov for å ivareta nasjonale sikkerhetsinteresser. Departementet foreslår derfor at lovbestemmelsens overskrift endres til «Tekniske og organisatoriske sikkerhetstiltak». Dette vil gi et bedre bilde av hva bestemmelsen regulerer.

Departementet foreslår videre at bestemmelsens ordlyd endres slik at det tydelig fremgår at bestemmelsen også dekker andre sikkerhetsutfordringer. Det foreslås derfor at det også inntas en plikt til å gjennomføre en risikovurdering av nettverks- og informasjonssystemer som benyttes for å levere tjenester etter disse to lovene. Ved vurderingen av hva som er et forsvarlig sikkerhetsnivå, skal det blant annet ses hen til den teknologiske utviklingen og nasjonale sikkerhetsinteresser. Dataansvarlige og databehandleren skal iverksette proporsjonale tiltak for å forebygge, avdekke og redusere konsekvensene av skadelige hendelser. Tiltakene skal sikre kontinuitet i tjenesteleveransen. Tiltakene skal samlet sørge for et sikkerhetsnivå som er tilpasset risikoen.

Når det gjelder departementets forslag til de to nye bestemmelsene, hhv. pasientjournalloven § 22a og helseregisterloven § 21a om bakgrunnssjekk, går dette lengre enn det som følger av rammene i gjeldende rett (sikkerhetsloven, arbeidsmiljøloven og statstjenestemannsloven), men som nevnt ovenfor uten at det vil utgjøre usaklig eller uforholdsmessig diskriminering. Departementet mener at mer generelle kriterier, med rett til å innhente og validere om det aktuelle personellet og utføre en grundigere kontroll enn det som følger av gjeldende rett, vil kunne ivareta både diskrimineringsvernet og nasjonale sikkerhetsinteresser på en bedre måte.

Den nærmere avgrensningen av kravet om bakgrunnssjekk vil bli fastsatt i forskrift etter § 22a og § 21a. Utkast til forskrift vil bli utarbeidet blant annet på bakgrunn av høringsinnspillene til lovforslagene og sendt på alminnelig høring. Det forutsettes at lovbestemmelsene om bakgrunnssjekk ikke kan settes i verk før forskriften er fastsatt.

Når det gjelder adgangen til å klage, foreslår departementet at det presiseres i forslaget til pasientjournalloven § 22a og helseregisterloven § 21a at avgjørelsen om å kreve bakgrunnssjekk kan påklages. Det ligger implisitt i dette at utfallet eller konsekvensen av bakgrunnssjekken ikke kan påklages. Dette har grunnlag i at selve bakgrunnssjekken vil være basert på mer objektive kriterier og at aksept av risiko forbundet med om personen er sikkerhetsmessig skikket må avgjøres av arbeidsgiveren/dataansvarlig. Departementet vil komme tilbake til hvilket organ som vil være klageinstans i arbeidet med forskrift.

Utfordringene departementet her omtaler er i stor grad sektorovergripende og berører flere departementers ansvarsområder. Det arbeides derfor i flere sektorer for å redusere risiko for skade mot nasjonal sikkerhet og sørge for tilstrekkelig nasjonal kunnskap og kompetanse innenfor fagområder og teknologier av betydning for nasjonal sikkerhet.

Departementets forslag har store likhetstrekk med mekanismene i sikkerhetsloven og forskriftene gitt i medhold av denne loven. Departementet mener det er fornuftig å gjenbruke etablerte mekanismer, tiltak og vurderinger der det passer.

I vurderingen av personellet, skal det legges vekt på forhold som er relevante for personens pålitelighet, lojalitet og dømmekraft i forbindelse med behandling av informasjon med betydning for nasjonale sikkerhetsinteresser og tilgang til objekter og infrastruktur med slik informasjon. Vurderingen skal gjøres på grunnlag av en bakgrunnssjekk, og tilsvarer kravet i sikkerhetsloven § 8-4 andre ledd.

Terminologien «nasjonale sikkerhetsinteresser» er i forslaget benyttet på en måte som favner noe videre enn legaldefinisjonen i sikkerhetsloven § 1-5. Skadefølgene vil være noe mindre enn ved kompromittering av objekter som er skjermet etter sikkerhetsloven, men kritiske samfunnsfunksjoner vil likevel rammes. Ordlyden er innenfor begreper som er benyttet i annet regelverk, herunder «andre vitale nasjonale sikkerhetsinteresser», jf. personopplysningsloven § 23, «offentlig sikkerhet» («public security») etter EU-retten og «nasjonale tryggingsomsyn eller forsvaret av landet» som benyttes i offentlighetsloven.

Hvilke egenopplysninger som skal etterspørres, registre som kontrolleres og forhold som vurderes, må reguleres nærmere i forskrift. Departementet mener at bakgrunnssjekken minst må kunne bekrefte identiteten til vedkommende og kontrollere strafferegistrene for lovovertredelser, jf. CER-direktivet. Etter forskrift om sikkerhet i luftfarten § 54, følger at vedkommende må fremlegge opplysninger om utdannelse og ansettelsesforhold de siste fem år og uttømmende politiattest, jf. politiregisterloven § 41. Departementet mener bakgrunnssjekken bør åpne for innhenting av noe mindre bakgrunnsinformasjon om vedkommende enn det som følger av klareringsforskriften kapittel 2 (§ 6 flg.). Krav til oversikt over personalia, familieforhold, statsborgerskap, straffbare forhold, arbeid og oppholdssted de siste årene er aktuelt.

Av klareringsforskriften § 6 følger at den som skal sikkerhetsklareres, skal samtykke til personkontrollen. Samtykket gis på et skjema fastsatt av Nasjonal sikkerhetsmyndighet. På skjemaet kan Nasjonal sikkerhetsmyndighet be den som skal klareres, opplyse om informasjon som er relevant for vurderingen. Dette omfatter bl.a. personalia, nåværende og tidligere statsborgerskap, bostedsadresser og opphold utenfor Norge, sivil status og familieforhold, utdanning og arbeidsforhold og om man har vært anmeldt, siktet eller tiltalt for straffbare forhold, eller er blitt ilagt strafferettslige og disiplinære reaksjoner i Norge eller i utlandet.

Videre er det i forskriften §§ 8 og 9 bestemt at opplysninger til personkonkontrollen kan innhentes og videreformidles til klareringsmyndigheten fra en rekke registre, herunder politiets registre, registre hos Politiets sikkerhetstjeneste og Skatteetatens registre. I § 10 er det bestemt at det kan innhentes tilsvarende opplysninger fra andre staters myndigheter som fastsatt i §§ 8 og 9 for de respektive klareringene.

Det er i forslaget til pasientjournalloven § 22a og helseregisterloven § 21a presisert at bakgrunnssjekken også skal omfatte opplysninger fra relevante offentlige registre. Videre er det presisert at behandlingsansvarlige for relevante registre plikter å utlevere registeropplysninger uten hinder av taushetsplikt. Hvilke registre dette er vil bli fastsatt i forskrift.

Det stilles også krav om at personen skal fremlegge uttømmende og utvidet politiattest, jf. politiregisterloven § 41 nr. 2. Krav om politiattest følger imidlertid også av særlovgivning, herunder helsepersonelleovn § 20a. Av bestemmelsen følger bl.a. at den som skal yte spesialisthelsetjenester og tannhelsetjenester til barn, skal fremlegge politiattest som nevnt i politiregisterloven § 39 første ledd (barneomsorgsattest) ved tilbud om stilling mv. Selv om personen har fremlagt politiattest etter en annen bestemmelse ved ansettelse, skal det likevel fremlegges uttømmende og utvidet politiattest. Den dataansvarlige vil på denne måten få opplysninger om ilagte straffereaksjoner, samt om siktelser og tiltaler, noe som vil være en viktig og nødvendig del av bakgrunnssjekk etter forslaget her.

Ut over opplysninger som fremkommer på politiattesten oppstilles det ikke plikt for politiet til å utlevere opplysninger. Dette betyr imidlertid ikke at opplysninger fra politiet ikke kan inngå i bakgrunnssjekken. Politiet vil kunne utlevere opplysninger etter ulike bestemmelser i politiregisterloven. Etter politiregisterloven § 27 kan politiet utlevere opplysninger dersom det er nødvendig for å avverge eller forebygge lovbrudd. Politiregisterloven §§ 30 og 31 åpner for at opplysninger utleveres til andre offentlige organer og til private i deres interesse, dersom dette er nødvendig for å fremme mottakerorganets oppgaver etter lov eller for å hindre at virksomhet blir utøvd på en uforsvarlig måte. Politiregisterforskriften §§ 9-6 og 9-7 inneholder en nærmere eksemplifisering av aktuelle mottakere. Opplistingen er ikke uttømmende.

Når det gjelder opplysninger fra andre kilder, herunder Politiets sikkerhetstjeneste, andre etterretningsregistre, offentlige myndigheter, tjenestesteder, arbeidsplasser og andre referanser følger det av forslaget at dette kan omfattes, men i slike tilfeller oppstilles det ingen utleveringsplikt. Politiets sikkerhetstjeneste kan dermed gi relevant informasjon til en bakgrunnssjekk, men det vil være opp til tjenesten om og i tilfelle hvilke opplysninger som skal kunne utleveres. Eventuell utlevering av gradert informasjon må skje innenfor sikkerhetslovens rammer, og mottaker må i tilfelle kunne håndtere opplysningene i tråd med sikkerhetsloven.

Lovbestemmelsene og den nærmere forskriftsreguleringen vil bidra til å oppfylle personvernforordningens prinsipper om dataminimering og om riktighet.

*Søknad, frivillighet og gyldighetstid*

Ansvaret for å vurdere konkret hvilke objekter og infrastruktur som trenger beskyttelse ligger hos den enkelte virksomhet. Departementet har forståelse for at det er krevende for de enkelte virksomhetene å operasjonalisere dette ansvaret. Den raske teknologiske utviklingen og uklare skillelinjer mellom hva som kan benyttes til sivile og militære formål, gjør det utfordrende å vurdere hva som trenger beskyttelse. Dette innebærer en risiko for ulik praksis blant virksomhetene og en fragmentert tilnærming til beskyttelse av norske kunnskapsverdier.

Departementet ønsker at bakgrunnssjekken skal profesjonaliseres, sikre tilstrekkelig rettsikkerhet og enhetlig praksis. Departementet arbeider med sikte på at bakgrunnssjekken over tid skal utføres av en sentral aktør med særlig kompetanse på

personkontroll. Utfordringene synes i stor grad å være sektorovergripende, som over tid eventuelt kan håndteres i arbeidet med implementering av CER-direktivet artikkel 14 om bakgrunnskontroll. Se punkt 3.2.

Departementet foreslår at alle som faller inn under kravene, må søke om bakgrunnssjekk. Den som skal klareres, må som nevnt ha gitt samtykke til kontrollen. Dette er presisert i forslaget til pasientjournalloven § 22a og helseregisterloven § 21a. At stillingen eller rollen krever bakgrunnssjekk besluttes av virksomheten. Samtykke til bakgrunnssjekk vil ikke oppfylle kravene til samtykke i personvernforordningen, men ingen skal mot sin vilje bli tvunget til å oppgi informasjon eller på annen måte gjennomføre en bakgrunnssjekk. Konsekvensen av å ikke «samtykke» vil imidlertid være at vedkommende ikke kan utføre de aktuelle arbeidsoppgavene og derfor ikke kan inneha en stilling hvor det stilles krav til sikkerhetsmessig skikkethet og bakgrunnssjekk.

En bakgrunnssjekk er en egnethetsvurdering som skal omfatte opplysninger gitt av personen som skal sjekkes. Personen plikter å gi fullstendige opplysninger om forhold som kan ha betydning for vurderingen av om personen er sikkerhetsmessig skikket. Departementet foreslår, som ovenfor nevnt at det utdypes i forskrift hva søker må fremlegge av informasjon, herunder opplysninger om utdannelse og ansettelsesforhold.

Departementet presiserer i forslaget til pasientjournalloven § 22a og helseregisterloven § 21a at personell som innehar sikkerhetsklarering eller adgangsklarering i henhold til sikkerhetsloven anses å oppfylle krav til bakgrunnssjekk.

Etter klareringsforskriften er en sikkerhetsklarering og adgangsklarering gyldig i inntil fem år, dersom ikke annet følger av avtale mellom Norge og en annen stat eller internasjonal organisasjon. For departementet fremstår det som hensiktsmessig med tilsvarende gyldighetstid for bakgrunnssjekk etter de foreslåtte hjemmelsgrunnlagene. Dette bør reguleres i forskrift, herunder plikter knyttet til endringer i situasjonen til den kontrollerte.

Når det er nødvendig å sikre et forsvarlig sikkerhetsnivå, ved å stille krav til bakgrunnssjekk er det også viktig med oppdatert og korrekt oversikt over hvem som er klarert på dette grunnlaget. Departementet er usikker på om virksomhetsinterne oversikter ivaretar behovet, eller om det bør etableres en nasjonal løsning. En nasjonal oversikt kan etableres på samme måte som følger av klareringsforskriften, hvor Nasjonal sikkerhetsmyndighet (NSM) skal ha et register over alle klareringsavgjørelser. Registeret skal bl.a. inneholde informasjon om klareringsstatus, vilkår knyttet til klareringen og den klarertes tilknytning til andre stater. Det er også presisert i forskriften at opplysninger om klareringsstatus kan utleveres til klareringsmyndigheter og autorisasjonsansvarlige. Departementet vil vurdere dette spørsmålet nærmere og eventuelt komme tilbake til dette ved fastsettelse av forskrift.

*Særlig om personvern*

Det å innhente bakgrunnsinformasjon av til dels inngripende karakter, med tilhørende negative konsekvenser dersom vedkommende ikke fyller nærmere bestemte vilkår, er et

inngrep i det enkelte personellets personvern. Formålet med å innføre bakgrunnssjekk er imidlertid å begrense risiko for kompromittering av bl.a. helseopplysninger, som i seg selv er et personverntiltak.

Personvernforordningen fastsetter regler om vern av fysiske personer i forbindelse med behandling av personopplysninger, samt regler om fri utveksling av personopplysninger. Se omtale i 2.6. Behandling av personopplysninger som er nødvendig av hensynet til rikets eller alliertes sikkerhet, forholdet til fremmede makter og andre vitale nasjonale sikkerhetsinteresser, er unntatt fra tilsynsmyndighetens tilgang til opplysninger etter personvernforordningen artikkel 58 nr. 1, se personopplysningsloven § 23 tredje ledd.

Departementet mener den foreslåtte behandlingen av personopplysninger er nødvendig av hensyn til «andre vitale nasjonale sikkerhetsinteresser», jf. personopplysningsloven § 23 tredje ledd. Dette betyr at Datatilsynet ikke er undersøkelsesmyndighet, og derfor ikke kan pålegge den dataansvarlige eller databehandleren å framlegge all informasjon den trenger for å kunne utføre sine oppgaver, eller utføre undersøkelser i form av personvernrevisjoner mv.

Personvernforordningen bygger på noen grunnleggende prinsipper, som likevel må ivaretas ved behandling av person- og helseopplysninger. Personvernprinsippene følger av artikkel 5 og består av:

– Prinsippene om lovlighet, rettferdighet og åpenhet

– Prinsippet om formålsbegrensning

– Prinsippet om dataminimering

– Prinsippet om riktighet

– Prinsippet om lagringsbegrensninger

– Prinsippet om integritet og konfidensialitet

– Prinsippet om ansvar

Prinsippene gir uttrykk for både grunnleggende hensyn som personvernforordningen skal ivareta, og konkrete krav til hvordan personopplysninger skal behandles. Disse prinsippene er ivaretatt ved departementets forslag, og er nærmere omhandlet i den konkrete vurderingen, se bl.a. spørsmålet om dataminimering i omtalen av hva som skal innhentes av informasjon og om formålsbegrensning.

Inngrepet i personvernet som behandlingen av personopplysningene medfører, skal være proporsjonalt med behandlingens formål, jf. artikkel 5 bokstav c. Departementet mener at bakgrunnssjekk av ansatte i enkelte kritiske stillinger og funksjoner, for bedre å kunne ivareta helse- og omsorgstjenestens oppgaver, befolkningens helse og den enkeltes personvern ved å redusere risiko for utro tjenere, er proporsjonalt med formålet. Departementet presiserer at dette forutsetter gode rutiner, konfidensialitet, sikring mv., og mener at dette er ivaretatt i forslaget til pasientjournalloven § 22a og helseregisterloven § 21a og øvrig regelverk eller vil bli ivaretatt i etterfølgende forskrift.

Videre krever behandling av «vanlige» og såkalt særlig kategorier av personopplysninger et behandlingsgrunnlag etter personvernforordningen artikkel 6 nr. 1. Behandling av særlig kategorier av personopplysninger må også oppfylle vilkårene i et av unntakene fra forbudet mot behandling av helseopplysninger i artikkel 9. Departementet mener behandlingen av opplysninger for kontrollformål, er omfattet av artikkel 6 nr. 1 bokstav d, eventuelt bokstav e og unntaket i artikkel 9 nr. 2 bokstav g. Avgivelse av opplysninger til bakgrunnssjekk skal være frivillig, men samtykke er ikke egnet som behandlingsgrunnlag.

Det er et vilkår i artikkel 6 nr. 3 nevnt i nr. 1 bokstav e, at behandlingen også skal fastsettes i nasjonal rett eller unionsretten. Dette kalles et supplerende rettslig grunnlag. Lovendringene i dette forslaget vil utgjøre et slikt supplerende rettslig grunnlag.

## 4.3 Begrenset deling av store datasett

### 4.3.1 Bakgrunn

Departementet har, på bakgrunn av endringene i den sikkerhetspolitiske situasjonen og utviklingen av det tekniske mulighetsrommet, grunn til å anta at også store aggregerte datasett med anonym eller indirekte identifiserbar helsedata er av interesse for trusselaktører og kan true nasjonale sikkerhetsinteresser. Med store datasett mener departementet datasett som alene eller sammen med andre datasett sier noe om en større befolkningsgruppe og som vil kunne ha betydning for nasjonale sikkerhetsinteresser, dersom de blir kompromittert.

Dette kan være datasett som ikke tidligere har vært ansett å utgjøre en sikkerhetsrisiko. Slike datasett er i dag, i relativt stor utstrekning, offentlig tilgjengelig. Utviklingen og bruk av kunstig intelligens har også aktualisert problemstillingen. Se omtale av det generelle trusselbildet i punkt 4.1.

### 4.3.2 Departementets vurderinger og forslag

I Norge har vi i dag stor grad av åpenhet, med offentlig deling og publisering av store datasett med aggregerte anonyme helsedata. Dette er en utviklingsretning som i stor grad også følger av våre EØS-rettslige forpliktelser, bl.a. gjennom datadelingsregelverket. Personvernforordningen kommer ikke til anvendelse på anonyme data.

Forskning på og analyse av helsedata er svært viktig for å vurdere hvordan det står til med helsen i den norske befolkningen, hvordan pasientsikkerheten er, og om kvaliteten på tjenestene er god nok. Det hjelper oss også til å forstå hva som påvirker helsen i befolkningen og til å planlegge framtidens behov for helsetjenester.

Helsedata er et vidt begrep som kan omfatte alle typer opplysninger om helse, enten de frembringes i helse- og omsorgstjenestene, gjennom de store befolkningsundersøkelsene eller på andre måter. Helsedata brukes både til å administrere og yte helsehjelp (primærbruk) og til å holde oversikt over helsetilstanden i befolkningen, over aktivitet og ressursbruk i helse- og omsorgstjenesten, til å forstå hva som påvirker helsen i befolkningen og til å utvikle kunnskap om forebygging, diagnostikk, behandling og

effekter av behandlingen (sekundærbruk). Tilgang til helsedata er nødvendig for legemiddelutvikling og i utvikling av produkter og løsninger for helse- og omsorgstjenesten og bidrar samtidig til innovasjon, kommersialisering og økt verdiskaping.

Endringene i den sikkerhetspolitiske situasjonen og det tekniske mulighetsrommet, har endret risikobildet knyttet til tilgjengeliggjøring av store aggregerte datasett med anonyme eller indirekte identifiserbare helsedata. Det er grunn til å tro at kompromittering av store datasett med helseinformasjon som ikke er (direkte) personidentifiserbar, også kan ha betydning for nasjonale sikkerhetsinteresser. Ifølge NSMs trusselvurdering må vi regne med at skjerpet risikobilde er en vedvarende situasjon.

I Meld. St. 9 (2022–2023) (kapittel 2, innledningen) fremgår følgende:

> Regjeringen er i meldingen opptatt av å forsterke innsatsen for å styrke samfunnets kollektive motstandskraft. Kunnskap, kompetanse og bevissthet på alle nivåer i samfunnet er avgjørende for å oppnå dette. Det dreier seg om forståelse av trussel- og risikobildet, hvorfor nasjonal sikkerhet er viktig, hvordan det treffer den enkelte og hvilke relevante tiltak som bør gjennomføres. I Norge har vi høy grad av tillit – både til hverandre og myndighetene. Høy grad av tillit gjør oss mer motstandsdyktige mot andre staters påvirkningsoperasjoner, som kan ha som formål å skape politisk og sosial uro. Men også i Norge kan denne tilliten være under press, og den kan være skjevt fordelt mellom ulike grupper i befolkningen. Vi må derfor styrke forståelsen, kunnskapen og bevisstheten om både trusler og tiltak i hele befolkningen. Dersom statens virkemidler ikke er forståelige og forutsigbare, og befolkningen har mangelfull kunnskap, kan det over tid undergrave tilliten til myndighetene. I et åpent samfunn som Norge må vi ta høyde for at ulike typer av lovlig aktivitet kan misbrukes, blant annet til etterretningsformål. Det vil være ulike hensyn som står mot hverandre, og en restrisiko vil alltid finnes.

Etter offentlighetsloven § 21 kan det *«gjerast unntak frå innsyn for opplysningar når det er påkravd av nasjonale tryggingsomsyn eller forsvaret av landet»*, se punkt 2.4. Departementet mener unntaket etter offentlighetsloven ikke fremstår som tilstrekkelig for å ivareta nasjonale sikkerhetsinteresser og øke den nasjonale motstandskraften mot dagens sammensatte trussel- og utfordringsbilde.

I helseretten er adgangen til å unnta deling av datasett med helseinformasjon, som ikke er personidentifiserbar og som kan ha betydning for nasjonale sikkerhetsinteresser, begrenset. Det samme gjelder opplysninger som er unntatt fra taushetsplikten på grunnlag av samtykke fra den opplysningene gjelder. Departementet mener at det, i større grad enn i dag er nødvendig å ha mulighet til å kunne begrense tilgang til denne type datasett og at dette bør fremgå av helseregisterloven og helsepersonelloven. Departementet vil presisere at behovet for skjerming ikke gjelder alle store datasett, og at hovedregelen fortsatt bør være at det gis tilgang.

Unntak for deling av sett med anonyme helsedata som kan true nasjonale sikkerhetsinteresser, er i samsvar med EØS-avtalen. EUs forordninger og direktiver om datadeling, har unntak for deling som er berettiget av hensyn til offentlig sikkerhet («public security»). Dette gjelder bl.a. EUs forordning (EU) 2018/1807 om en ramme for

fri flyt av andre opplysninger enn personopplysninger i EU, datastyringsforordningen (Data Governance Act (EU) 2022/868) og forslag til dataforordning (Data Act). De aktuelle EU-rettsaktene er, eller vil bli implementert i annet regelverk.

I det ovenfor nevnte EU-regelverket legges til grunn forståelsen av «offentlig sikkerhet», slik det er definert i EU-retten og særlig traktaten om Den europeiske unions virkemåte (TFEU) artikkel 52. Begrepet «offentlig sikkerhet» dekker både den interne og den eksterne sikkerheten i en medlemsstat, samt spørsmål om samfunnssikkerhet. «Offentlig sikkerhet» forutsetter at det foreligger en reell og tilstrekkelig alvorlig trussel som påvirker en av de grunnleggende samfunnsinteressene, for eksempel en trussel mot institusjoners og grunnleggende offentlige tjenesters virkemåte og befolkningens overlevelse, samt risikoen for en alvorlig forstyrrelse av internasjonale relasjoner eller nasjoners fredelige sameksistens, eller en trussel mot militære interesser. Departementet mener nasjonale sikkerhetsinteresser er omfattet av begrepet «offentlig sikkerhet».

Kompetanse og kunnskap om risiko, trusler, sårbarheter og effektive mottiltak er en forutsetning for å kunne beskytte våre verdier mot uønskede hendelser. Det er derfor viktig at de aktuelle virksomhetene setter seg i stand til å kunne identifisere denne type utfordringer og fatte beslutninger om begrenset deling. I samsvar med forholdsmessighetsprinsippet bør unntak som er begrunnet ut fra hensynet til offentlig sikkerhet, være egnet til å sikre at det fastsatte målet nås, og ikke gå lenger enn det som er nødvendig for å nå dette målet.

Unntak fra deling med begrunnelse av at slik deling antas å ville ha betydning for nasjonale sikkerhetsinteresser, må vurderes konkret. Departementet mener sikkerhetslovens metodikk for hvordan nasjonale verdier skal kartlegges, også vil kunne benyttes for å identifisere datasett det kan være aktuelt å underlegge begrenset deling. Metoden er egnet for å gi god oversikt over verdier som ikke dekkes av sikkerhetsloven, men som likevel kan ha betydning for nasjonal sikkerhet. Samtidig må en oversikt over verdier ses i sammenheng med trussel- og risikobildet, for å forstå egne sårbarheter og for å kunne ivareta egen sikkerhet.

Den faktiske vurderingen av hvilke datasett som vil kunne ha betydning for nasjonale sikkerhetsinteresser, vil kunne være krevende for de enkelte virksomhetene å foreta. Det er i utgangspunktet heller ikke vurderinger som virksomhetene er «rigget» for å foreta. Det er derfor viktig at kriteriene i større grad utdypes og beskrives i forskriftsarbeidet og eventuelt i rundskriv. Det er også en forutsetning at det er tett dialog mellom helsemyndighetene som skal forestå disse vurderingene og de nasjonale instansene med særskilt kompetanse på samfunnssikkerhet. Dette vil kunne bidra til at du ulike virksomhetene i begrenset grad tolker like saker ulikt og at tilgang til disse datasettene ikke blir begrenset i for stor grad. Departementet vil for øvrig påpeke at virksomhetene har personell og ivaretar kravene i og i medhold av sikkerhetsloven på en god måte. Det er derfor mye kompetanse som vil kunne gi synergier for å utføre disse nye vurderingene.

Departementet foreslår på denne bakgrunn endringer i helseregisterloven §§ 19, 19 a, 19 e og helsepersonelloven § 29, som gir hjemmel til å begrense tilgjengeliggjøring av store

sett med helsedata, dersom tilgjengeliggjøringen kan ha betydning for nasjonale sikkerhetsinteresser. Departementet mener at et unntak med begrensninger knyttet nasjonale sikkerhetsinteresser, som ivaretar unntak etter våre EØS-rettslige forpliktelser etter datadelingsregelverket, må ivaretas med klar hjemmel i nasjonal lovgivning.

Ved søknad om tilgjengeliggjøring av personidentifiserbare data, kan krav om bakgrunnssjekk av personell hos mottaker være et alternativ til å nekte tilgjengeliggjøring. Se omtale av bakgrunnssjekk i punkt 4.2.

# 5 Økonomiske og administrative konsekvenser

Forslagene om å begrense delingen av store datasett ved tilgjengeliggjøring fra helseregistre, vil kunne ha noe administrative og økonomiske konsekvenser for dataansvarlig for registrene. Dataansvarlig må i enkelte saker gjøre tilleggsvurderinger av hensynet til nasjonale sikkerhetsinteresser.

Kravet om bakgrunnssjekk vil ha administrative og økonomiske konsekvenser for dataansvarlig, ved innhenting av opplysninger og tilleggsvurderinger knyttet til personellet. Forslaget vil ikke ha direkte økonomiske konsekvenser for privatpersoner.

Konsekvensene antas bare å gjelde statlige aktører, og merutgiftene dekkes innenfor gjeldende budsjettrammer.

# 6 Forslag til lovendringer

I

**I lov 2. juli 1999 nr. 64 om helsepersonell m.v. (helsepersonelloven) gjøres følgende endringer:**

§ 29 nytt tredje og fjerde punktum i fjerde ledd skal lyde:

*Dersom tilgjengeliggjøring av helseopplysninger kan true nasjonale sikkerhetsinteresser, skal opplysningene ikke gjøres tilgjengelig. Departementet kan kreve at det utføres bakgrunnssjekk i samsvar med pasientjournalloven § 22a av mottaker, med mindre mottaker kan fremlegge dokumentasjon på gyldig relevant klarering etter sikkerhetsloven eller relevant bakgrunnssjekk.*

II

**I lov 20. juni 2014 nr. 42 om behandling av helseopplysninger ved ytelse av helsehjelp (pasientjournalloven) gjøres følgende endringer:**

§ 22 skal lyde:

§ 22 *Tekniske og organisatoriske sikkerhetstiltak*

*Den dataansvarlige og databehandleren skal gjennomføre nødvendige tekniske og organisatoriske tiltak for å sikre personopplysninger. Tiltakene skal være egnet med hensyn til risikoen ved behandlingen av personopplysningene, jf. personvernforordningen artikkel 32. Den dataansvarlige og databehandleren skal også gjennomføre risikovurderinger av nettverks- og informasjonssystemene som benyttes for å levere tjenester i henhold til denne loven.*

*Sikkerhetstiltakene skal være proporsjonale og tilpasset risikoen. Ved vurderingen av hva som er et forsvarlig sikkerhetsnivå, skal det tas hensyn til den enkeltes personvern, helse- og omsorgstjenestens evne til å ivareta sine oppgaver, den teknologiske utviklingen og nasjonale sikkerhetsinteresser.*

*Den dataansvarlige og databehandleren skal iverksette tiltak for å forebygge, avdekke og redusere konsekvensene av skadelige hendelser. Dette omfatter tiltak som bl.a. tilgangsstyring, logging, etterfølgende kontroll og bakgrunnssjekk etter § 22 a. Tiltakene skal sikre kontinuitet i tjenesteleveransen.*

*Departementet kan i forskrift fastsette nærmere krav til tekniske og organisatoriske sikkerhetstiltak.*

Ny § 22a skal lyde:

*§ 22a Bakgrunnssjekk*

*Den dataansvarlige skal kreve og gjennomføre bakgrunnssjekk av personer som skal ha eller har bred tilgang til objekter eller infrastruktur hvor det behandles store datasett med person- og helseopplysninger som er kritisk for helse- og omsorgstjenestens evne til å ivareta sine oppgaver. Beslutning om krav til bakgrunnssjekk for den konkrete stillingen skal begrunnes. Det skal ikke kreves bakgrunnssjekk dersom det kan iverksettes andre egnede sikkerhetstiltak.*

*Den som skal underlegges bakgrunnssjekk, må ha gitt samtykke til dette.*

*En bakgrunnssjekk skal omfatte opplysninger gitt av personen selv. Personen plikter å gi fullstendige opplysninger om forhold som kan ha betydning for vurderingen av sikkerhetsmessig skikkethet. Personen skal fremlegge uttømmende og utvidet politiattest, jf. politiregisterloven § 41 nr. 2. Bakgrunnssjekken skal også omfatte opplysninger fra relevante offentlige registre. Bakgrunnssjekken kan omfatte opplysninger fra andre kilder, som Politiets sikkerhetstjeneste, Politiet, andre offentlige myndigheter, tjenestesteder, arbeidsplasser og andre referanser.*

*I vurderingen skal det legges vekt på forhold som er relevante for personens pålitelighet, lojalitet og dømmekraft i forbindelse med tilgang til informasjon eller funksjoner som er kritisk for helse- og omsorgstjenestens evne til å ivareta sine oppgaver. Dette omfatter bl.a. opplysninger om straffbare handlinger, forhold som kan føre til at personen selv, eller personens nærstående, utsettes for trusler slik at personen kan bli presset til å handle i strid med sikkerhetsinteresser, feilaktig eller unnlatt framstilling av faktiske forhold som personen måtte forstå har betydning for bakgrunnssjekken, sykdom som kan gi svekkelse av påliteligheten, lojaliteten eller dømmekraften, tilknytning til andre stater og annet som kan gi grunn til å frykte at en person vil kunne opptre i strid med nasjonale sikkerhetsinteresser.*

*Bakgrunnssjekken skal være så godt opplyst som mulig. Opplysninger om nærstående personer skal bare tillegges vekt dersom opplysningene er sikkerhetsmessig relevante. Politisk engasjement og annet lovlig samfunnsengasjement, som medlemskap i, sympati med eller aktivitet for politiske partier eller organisasjoner, skal ikke tillegges vekt i vurderingen.*

*Dersom det er tvil om en person er sikkerhetsmessig skikket, skal det avholdes en sikkerhetssamtale med personen.*

*Avgjørelsen om å kreve bakgrunnssjekk kan påklages.*

*Personell med sikkerhetsklarering eller adgangsklarering etter sikkerhetsloven anses å oppfylle kravene.*

*Behandlingsansvarlige for relevante offentlige registre plikter å utlevere registeropplysninger uten hinder av taushetsplikt. Registeropplysninger skal meddeles skriftlig. Det kan ikke kreves vederlag for registeropplysningene.*

*Opplysninger som virksomheten har fått i forbindelse med bakgrunnssjekk, skal ikke benyttes til andre formål enn vurdering av om personen er sikkerhetsmessig skikket.*

*Departementet kan gi forskrift om bakgrunnssjekk, herunder hvilke opplysninger som kan innhentes, hvilke registre opplysninger kan innhentes fra og hvilket organ som skal ha ansvar for bakgrunnssjekken.*

III

**I lov 20. juni 2014 nr. 43 om helseregistre og behandling av helseopplysninger (helseregisterloven) gjøres følgende endringer:**

§ 19 fjerde ledd skal lyde:

Utarbeidet statistikk skal være anonym. *Statistikk som kan true nasjonale sikkerhetsinteresser skal ikke gjøres offentlig tilgjengelig.*

§ 19a nytt åttende ledd skal lyde:

*Dersom tilgjengeliggjøring av helseopplysninger kan true nasjonale sikkerhetsinteresser, skal opplysningene ikke gjøres tilgjengelig. Dataansvarlig kan kreve at det utføres bakgrunnssjekk i samsvar med § 21a av mottaker, med mindre mottaker kan fremlegge dokumentasjon på gyldig relevant klarering etter sikkerhetsloven eller relevant bakgrunnssjekk.*

§ 19e fjerde ledd skal lyde:

Det kan bare gis dispensasjon dersom tilgjengeliggjøringen er ubetenkelig ut fra etiske, medisinske og helsefaglige hensyn *og ikke vil true nasjonale sikkerhetsinteresser*. For tilgjengeliggjøring til medisinsk og helsefaglig forskning skal mottakeren ha fått forhåndsgodkjenning fra den regionale komiteen for medisinsk og helsefaglig forskningsetikk, jf. helseforskningsloven § 33. *Departementet kan kreve at det utføres bakgrunnssjekk i samsvar med § 21 a av mottaker, med mindre mottaker kan fremlegge dokumentasjon på gyldig relevant klarering etter sikkerhetsloven eller relevant bakgrunnssjekk.*

§ 21 skal lyde:

§ 21 *Tekniske og organisatoriske sikkerhetstiltak*

*Den dataansvarlige og databehandleren skal gjennomføre nødvendige tekniske og organisatoriske tiltak for å sikre personopplysninger. Dette skal være egnet med hensyn til risikoen ved behandlingen av disse opplysningene, jf. personvernforordningen artikkel 32.* I registre som er etablert med hjemmel i §§ 10 eller 11, skal navn, fødselsnummer og andre personidentifiserende kjennetegn lagres kryptert. *Den dataansvarlige og databehandleren skal også gjennomføre risikovurderinger av nettverks- og informasjonssystemene som benyttes for å levere tjenester i henhold til denne loven.*

*Sikkerhetstiltakene skal være proporsjonale og tilpasset risikoen.*

*Ved vurderingen av hva som er et forsvarlig sikkerhetsnivå, skal det tas hensyn til den enkeltes personvern, helse- og omsorgstjenestens evne til å ivareta sine oppgaver, den teknologiske utviklingen og nasjonale sikkerhetsinteresser.*

*Den dataansvarlige og databehandleren skal iverksette tiltak for å forebygge, avdekke og redusere konsekvensene av skadelige hendelser. Dette omfatter tiltak som bl.a. tilgangsstyring, logging, etterfølgende kontroll og bakgrunnssjekk av personell etter § 21a. Tiltakene skal sikre kontinuitet i tjenesteleveransen.*

*Departementet kan i forskrift fastsette nærmere krav til tekniske og organisatoriske sikkerhetstiltak.*

Ny § 21 a skal lyde:

*§ 21a Bakgrunnssjekk*

*Den dataansvarlige skal kreve og gjennomføre bakgrunnssjekk av personer som skal ha eller har bred tilgang til objekter eller infrastruktur, hvor det behandles store datasett med person- og helseopplysninger som er kritisk for den dataansvarlige og databehandlerens evne til å ivareta sine oppgaver. Beslutning om krav til bakgrunnssjekk for den konkrete stillingen skal begrunnes. Det skal ikke kreves bakgrunnssjekk dersom det kan iverksettes andre egnede sikkerhetstiltak.*

*Den som skal underlegges bakgrunnssjekk, må ha gitt samtykke til dette.*

*En bakgrunnssjekk skal omfatte opplysninger gitt av personen selv. Personen plikter å gi fullstendige opplysninger om forhold som kan ha betydning for vurderingen av sikkerhetsmessig skikkethet. Bakgrunnssjekken skal også omfatte opplysninger fra relevante offentlige registre og uttømmende politiattest jf. politiregisterloven § 40 nr. 2. Bakgrunnssjekken kan omfatte opplysninger fra andre kilder, som Politiets sikkerhetstjeneste, offentlige myndigheter, tjenestesteder, arbeidsplasser og andre referanser.*

*I vurderingen skal det legges vekt på forhold som er relevante for personens pålitelighet, lojalitet og dømmekraft i forbindelse med tilgang til informasjon eller funksjoner som er kritisk for den dataansvarlige og databehandlerens evne til å ivareta sine oppgaver. Dette omfatter bl.a. opplysninger om straffbare handlinger, forhold som kan føre til at personen selv, eller personens nærstående, utsettes for trusler slik at personen kan bli presset til å handle i strid med sikkerhetsinteresser, feilaktig eller unnlatt framstilling av faktiske forhold som personen måtte forstå har betydning for bakgrunnssjekken, sykdom som kan gi svekkelse av påliteligheten, lojaliteten eller dømmekraften, tilknytning til andre stater og annet som kan gi grunn til å frykte at en person vil kunne opptre i strid med nasjonale sikkerhetsinteresser.*

*Bakgrunnssjekken skal være så godt opplyst som mulig. Opplysninger om nærstående personer skal bare tillegges vekt dersom opplysningene er sikkerhetsmessig relevante. Politisk engasjement og annet lovlig samfunnsengasjement, som medlemskap i, sympati med eller aktivitet for politiske partier eller organisasjoner, skal ikke tillegges vekt i vurderingen.*

*Dersom det er tvil om en person er sikkerhetsmessig skikket, skal det avholdes en sikkerhetssamtale med personen.*

*Avgjørelsen om å kreve bakgrunnssjekk kan påklages.*

*Personell med sikkerhetsklarering eller adgangsklarering etter sikkerhetsloven anses å oppfylle kravene.*

*Behandlingsansvarlige for relevante offentlige registre plikter å utlevere registeropplysninger uten hinder av taushetsplikt. Registeropplysninger skal meddeles skriftlig. Det kan ikke kreves vederlag for registeropplysningene.*

*Opplysninger som virksomheten har fått i forbindelse med bakgrunnssjekk, skal ikke benyttes til andre formål enn vurdering av om personen er sikkerhetsmessig skikket.*

*Departementet kan gi forskrift om bakgrunnssjekk, herunder hvilke opplysninger som kan innhentes, hvilke registre opplysninger kan innhentes fra og hvilket organ som skal ha ansvar for bakgrunnssjekken.*