Trusselutsatte personer med adressesperre (faktaark 55)

Versjon 2.0

Dette faktaarket er et støttedokument under Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren (Normen) som forvaltes av Styringsgruppen for Normen etter Normens forvaltningsmodell. Se mer på www.normen.no

Tema for faktaarket	Faktaarket gir anbefalinger om hvordan opplysninger om trusselutsatte personer bør behandles i helsesektoren. Som trusselutsatte regnes her personer som har innvilget adressesperre i folkeregisteret. Adressesperre innvilges for trusselutsatte personer, dvs. personer som står i fare for å bli utsatt for alvorlig kriminalitet rettet mot liv, helse eller frihet. Typiske eksempler er vitner, informanter og personer som har blitt eller er utsatt for vold og trusler. Dette faktaarket gir også en forklaring på hva adressesperre i folkeregisteret innebærer. Faktaarket skal bidra til at helse- og omsorgssektoren opprettholder beskyttelse for trusselutsatte ved at: • Virksomheter, helsepersonell og øvrige ansatte forholder seg til beslutningen om adressesperre på riktig måte. • Det klargjøres hvilke krav som skal stilles til systemer som behandler adresse eller andre geolokaliserende opplysninger. • Virksomheter forstår sitt ansvar for å ha systemer som sikrer riktig oppfølging og bruk av fastsatt adressesperre. Dette faktaarket omtaler ikke bruk av klientadresse, som benyttes i de tilfeller adressen kan røpe et forhold som må regnes som personlig. Dette vil normalt gjelde fengsler, institusjoner under rusomsorgen, psykiatriske institusjoner og hjem for psykisk utviklingshemmede. Personer som melder flytting til slike institusjoner får angitt adressen i folkeregistrert som «klientadresse».
Dette faktaarket er spesielt relevant for	Målgruppen for faktaarket er virksomheter som har pasienter, brukere eller ansatte med sperret adresse. Hver virksomhet i helse- og omsorgssektoren må fastsette og følge egne rutiner og prosedyrer for bruk av folkeregisteropplysninger som har til hensikt å beskytte enkeltpersoner. Kripos har et tett samarbeid med helse- og omsorgssektoren og kan bistå og gi råd i aktuelle spørsmål.
Krav i gjeldende versjon av Normen	Faktaarket gjelder blant annet følgende kapitler i Normen: • Kapittel 5.2 Tilgangsstyring • Kapittel 5.3 Fysisk sikkerhet og håndtering av utstyr

Relevante lov- og forskriftsbestemmelser, standarder og andre rammeverk	Følgende lov- og forskriftsbestemmelser, standarder og andre rammeverk er spesielt relevante for faktaarket: - Instruks for behandling av dokumenter som trenger beskyttelse av andre grunner enn nevnt i sikkerhetsloven med forskrifter (beskyttelsesinstruksen). - Behandling av opplysninger om personer med adressesperre – Veileder fra Kripos Målgruppen for dokumentet er offentlige og private aktører som leverer tjenester til fysiske personer.

Om trusselutsatte

1.1 Innledning

Adressesperre i folkeregisteret er et tiltak for å beskytte trusselutsatte personer, dvs. personer som står i fare for å bli utsatt for alvorlig kriminalitet rettet mot liv, helse eller frihet. Typiske eksempler er vitner, informanter og personer som har blitt eller er utsatt for vold og trusler. Personer med adressesperre kan være både pasienter, brukere og ansatte i virksomheten.

Dette dokumentet omtaler adressesperre i helse- og omsorgssektoren. For generell informasjon om adressesperre henvises det til Kripos.

Dersom opplysningene behandles av en offentlig tjenesteyter, er det viktig å huske på at personer med adressesperre har rett til det samme tilbudet fra offentlige helsemyndigheter som personer uten adressesperre. For personer med adressesperre må imidlertid sikkerhetsaspektet veie svært tungt. Det skal likevel etterstrebes at disse får et tilbud som er så normalt som mulig.

Det finnes ingen særskilte regler i lov eller forskrift som direkte omhandler helsehjelp til pasienter med adressesperre. Det er heller ikke gitt nasjonale retningslinjer som direkte omhandler denne pasientgruppen.

1.2 Regler for adressesperre

Folkeregisterloven § 10-4 hjemler sperring av graderte opplysninger i medhold av beskyttelesinstruksen i folkeregisteret.

To offentlige etater kan beslutte å gi personer adressesperre og legge det inn i folkeregisteret:

- Politiet kan, i samråd med den trusselutsatte, beslutte å gi adressesperre som beskyttelsestiltak til voksne. Ved en slik beslutning sperres også adressen til eventuelle barn og resten av husstanden.
- Fylkesnemnda for barnevern og sosiale saker vurderer og kan beslutte adressesperre for barnet i saker om omsorgsovertakelse. I hastesaker kan også barnevernsleder i kommunen beslutte adressesperre for barnet. Barnevernlovens § 4-19 gir fylkesnemnda for barnevern og sosiale saker hjemmel til å bestemme at foreldrene ikke skal ha rett til å vite hvor barnet er.

Avgjørelsen om adressesperre skal i begge tilfeller skje på grunnlag av en trusselvurdering med etterfølgende beslutning og være basert på en helhetsvurdering. Adressesperre er et tidsbegrenset beskyttelsestiltak som er gjenstand for en løpende vurdering og gjelder så lenge det er behov for det.

Adressen sperres FORTROLIG eller STRENGT FORTROLIG i henhold til beskyttelsesinstruksen § 4 jf. § 3 jf. offentlighetsloven § 24 tredje ledd annet punktum første alternativ.

Beslutningen om adressesperre forplikter alle virksomheter som på noen måte er i befatning med personen som beskyttes og dennes opplysninger. Hver virksomhet må følge opp beslutningen og håndtere graderte opplysninger på en slik måte at beskyttelsen av trusselutsatte ikke reduseres eller fjernes.

Alle bestemmelser om taushetsplikt om andre typer opplysninger om personer gjelder i tillegg til reglene om beskyttelse etter beskyttelsesinstruksen. Det samme gjelder informasjonssikkerhetsbestemmelser i helselovgivningen og personopplysningsloven.

1.3 Virkningene av adressesperre

Adressesperre innebærer at tilgangen til den trusselutsattes adresse i folkeregistret begrenses. Det er imidlertid også viktig at den trusselutsattes opplysninger håndteres på en trygg måte utenfor folkeregisteret.

Dette er særlig viktig for geolokaliserende opplysninger, som er alle opplysninger som kan si noe om hvor en trusselutsatt befinner seg eller kommer til å befinne seg i fremtiden, eller hvor vedkommende har oppholdt seg tidligere.

Dette innebærer at alle opplysninger om bosted, arbeidsplass, skole, barnehage og andre daglige oppholdssteder kan være beskyttelsesverdige. I tillegg må andre opplysninger som kan fortelle noe om den trusselutsattes oppholdssted beskyttes, for eksempel opplysninger om offentlige og private brukersteder, for eksempel opplysninger om fastlege, uthenting av resepter, hjemmebesøk, barnevernstjeneste og hvilket sykehus den trusselutsatte sogner til.

Alle opplysninger om avtaler med offentlige eller private virksomheter kan derfor være relevante å beskytte for eksempel timer hos lege, sykehus, fritidsaktiviteter og andre støtte- eller brukertjenester.

Merk: opplysninger om at en person er trusselutsatt og har adressesperre, er ikke konfidensielt og kan deles med andre.

Adressesperringen skjer i folkeregisteret. Helse- og omsorgssektorens egen versjon – *Personregisteret* – oppdateres i samsvar med folkeregisteret. For å sikre at sektoren følger opp adressesperringen er det derfor avgjørende å ha oppdatert folkeregisterinformasjon og at virksomhetens øvrige systemer oppdateres i samsvar med folkeregisteret fortløpende.

Det finnes to varianter av adressesperre:

- «Fortrolig adresse»
- «Strengt fortrolig adresse»

Tidligere ble begrepene «kode 7» og «kode 6» benyttet. Etter moderniseringen av folkeregisteret falt disse bort, og vil ikke bli benyttet her.

«Fortrolig adresse» innebærer at adressen til den trusselutsatte ikke leveres til private, men er tilgjengelig for den delen av det offentlige som har hjemmel til opplysninger fra folkeregisteret.

«Strengt fortrolig adresse» innebærer at opplysninger om adressen ikke leveres til noen. Postforsendelser til de det gjelder skal sendes postboksen SOT 6 2094 Vika, 0125 Oslo.

For både strengt fortrolig adresse og fortrolig adresse kan man bruke SOT6-postboksen til Kripos, da Kripos videresender post til brukere med både strengt fortrolig adresse og fortrolig adresse.

1.4 Virksomhetens ansvar

Hver virksomhet i helse- og omsorgssektoren må fastsette og følge egne rutiner og prosedyrer for bruk av folkeregisteropplysninger og annen geolokaliserende informasjon om trusselutsatte. Dette gjelder også virksomheter som behandler informasjon fra helse- og omsorgstjenesten, for eksempel NAV.

Overholdelse av denne plikten bør i størst mulig grad sikres i virksomhetens styringssystem, jf. Normen kap. 2. Kripos har et tett samarbeid med helse- og omsorgssektoren og kan bistå og gi råd i aktuelle spørsmål.

2. Risikovurdering

Etter helselovgivningen og personvernlovgivningen plikter enhver virksomhet som behandler helse- og personopplysninger å gjennomføre tekniske og organisatoriske tiltak som sikrer overholdelse av krav til informasjonssikkerhet og personvern.

Virksomhetene må gjennomføre tilstrekkelige risikovurderinger for å unngå at informasjonsbehandlingen i virksomheten gir uakseptabel risiko for oppsporing av trusselutsatte personer. Arbeidet bør være risikobasert, dvs. at risikovurdering og -håndtering prioriteres på de områdene med (antatt/vurdert) høyest risiko.

Det er viktig at personellet som gjennomfører risikovurderingen er riktig sammensatt og består av kompetanse som forstår hele verdikjeden. Dette er særlig viktig der geolokaliserende opplysninger skal behandles av en databehandler.

2.1 Hva bør risikovurderes?

Som minimum bør virksomheten vurdere følgende scenarier som kan sette trusselutøver i stand til å spore opp den trusselutsatte:

1. Oppsporing ved at utro tjenere snoker
2. Oppsporing ved at ansatte utsettes for sosial manipulering
3. Oppsporing ved at informasjon sendes til kontaktpunkter som trusselutøveren har kontroll over, typisk til gamle adresser.

2.2 Vurdering av tiltak

Basert på risikovurderingen skal det vurderes hvilke tiltak som skal iverksettes for å redusere risikoen. Relevante tiltak omfatter blant annet:

1. Krav til tilgangsstyringen, inkl. logging og logganalyse (Se også faktaark 15 om logging og logginnsyn) (Scenario 1)
2. Tiltak for å sikre at ansatte er oppmerksom på at opplysningene må håndteres med skjerpet aktsomhet, herunder opplæring og tydelig merking i systemer av at en person er trusselutsatt. (Scenario 2)
3. Sikring av at rutinemessige/automatiserte utsendinger kun skjer til oppdaterte adresser. (Scenario 3)
4. Begrense mengden geolokaliserende informasjon i systemene og i kommunikasjon med den trusselutsatte. Bruk av ikke-lokaliserende adresser fra autorative kilder, som folkeregister/kontaktregister, anbefales (alle scenarier).

Tiltakene må vurderes for den enkelte kategori basert på risiko. Det innebærer at det i utgangspunktet ikke er nødvendig med like tiltak for fortrolig og strengt fortrolig adresse. Det må i alle tilfeller vurderes konkret i virksomheten hvilke tiltak som senker risikoen.

2.3 Utarbeidelse av rutiner

Basert på besluttede tiltak må det utarbeides rutiner som sørger for at adresse og annen geolokaliserende informasjon om den trusselutsatte beskyttes. I dette kapittelet gjennomgås noen områder virksomheten bør ha rutiner for å håndtere informasjon om adressesperre og annen geolokaliserende informasjon.

2.3.1 Bruk av adressekilder

Virksomheten må ha kunnskap om hvor adresseopplysninger og andre geolokaliserende opplysninger finnes i virksomhetens systemer og hvordan disse oppdateres mot Personregisteret eller annen folkeregisterkilde som virksomheten bruker.

Det må sikres riktig bruk og hyppig oppdatering av kilder til geolokaliserende informasjon og annen kontaktinformasjon, som for eksempel folkeregisteret, personregisteret og kontakt- og reservasjonsregisteret. Det bør ikke lagres lokale kopier av disse kildene. Dersom det er forsinkelse i oppdatering av Personregisteret eller annen folkeregisterkilde som virksomheten bruker vil det i en periode kunne oppstå behov for at personen selv må opplyse om at han eller hun har adressesperre.

2.3.2 Opplæring og bevisstgjøring

Det må gis opplæring til ansatte i hvordan informasjon om adressesperre skal håndteres. Opplæringen skal skape bevissthet om sensitiviteten av denne informasjonen og opplære de ansatte i forskjellen mellom fortrolig og strengt fortrolig adresse.

De ansatte må ha god kunnskap om personregisteret eller annen folkeregisterkilde som virksomheten bruker. Ved innføring av nye systemer må de ansatte få informasjon om hvordan adressesperre skal håndteres i det aktuelle systemet.

Virksomheten bør ha gode eksempelrutiner. Det kan gå lang tid mellom hver gang en ansatt må forholde seg til pasienter med adressesperre, og det er derfor viktig at informasjon om hvordan dette skal behandles er lett tilgjengelig og holdes oppdatert.

2.3.3 Sikring av mottakere

Virksomheten må ha sikkerhet for at kunnskap om aktuell adressesperre når riktig nivå og riktige brukere i virksomheten, for eksempel skrankepersonell og sentralbord. Dersom det skal sendes informasjon mellom virksomheter, må det vurderes om sendingen kommer til et stort mottaksapparat og hvor mange som potensielt får tilgang til sendingen.

2.3.4 Tilgangsstyring og merking av informasjon

Virksomheten må ha gode rutiner for styring av tilgang til journaler til personer med adressesperre. Tilgang må begrenses elektronisk, dersom det ikke er andre måter å sørge for at bo- eller oppholdssted forblir ukjent. Opplysninger om fortrolig adresse må ikke legges inn andre steder enn der det vurderes som trygt.

2.3.4.1 Behandling av opplysninger i behandlingsrettet helseregister

I pasientjournal skal opplysninger om eventuelt adressesperre være i samsvar med oppdatert folkeregisterinformasjon.

Tilgang til elektronisk journal skal dokumenteres, se Logging og innsyn i logg (faktaark 15). Helsepersonell kan sperre geolokaliserende opplysninger i journal. Dersom journalen ikke har funksjonalitet for sperring eller lignende, må det være manuelle rutiner som sørger for at journal merkes på annet hensiktsmessig måte for å signalisere til ansatte at opplysningene må behandles med ekstra varsomhet.

For nettbaserte "spørretjenester" som for eksempel "Pasientens fastlege" hentes lokaliserende opplysninger fra Helsedirektoratets og Helfos administrative system for fastlegeordningen. Personer med strengt fortrolig adresse inngår ikke i denne spørretjenesten.

Pasienter med kjernejournal som får adressesperre blir automatisk sperret fra kjernejournal når informasjon fra folkeregisteret kommer inn. Kjernejournal oppdateres daglig. Sperring betyr at informasjon i kjernejournal blir utilgjengelig for personen selv og for helsepersonell. Sletting fra databasen skjer etter 30 dager.

2.3.4.2 Midlertidig oppholdssted

Ved midlertidig oppholdssted, for eksempel ved sykehusinnleggelse eller opphold på institusjon er opplysninger om midlertidig oppholdssted er like beskyttelsesverdig som bostedsadressen.

Virksomheten må sørge for:

- Å ha rutiner som sørger for at oppholdet forblir hemmelig.
- At besøk som medfører trussel for personen forhindres. Dette er ikke nødvendigvis bare begrenset til trusselutøver, men kan for eksempel også være journalister eller andre som tar bilder på området der pasienter kan identifiseres.

2.3.5 Kommunikasjon med den trusselutsatte

Det er en stor fordel for personer med adressesperre å motta så mye som mulig via digitale kanaler. Hvis mulig bør det benyttes digitale oversendingsløsninger som krever innlogging med sikker autentifiseringsløsning, for eksempel Digipost eller Altinn.

Offentlige myndigheter kan benytte seg av kontakt- og reservasjonsregisteret (KRR) ved digital kommunikasjon med trusselutsatte. I KKR skal det blant annet ligge e-postadresse til den trusselutsatte. Private virksomheter kan benytte annen, privat e-postadresse dersom denne er oppgitt av den trusselutsatte.

Kontakt- og reservasjonsregisteret inneholder innbyggernes digitale kontaktinformasjon, til bruk for offentlige virksomheter. Ved adressesperre skjer det ingen endring i KRR for personer som får strengt fortrolig adresse og fortrolig adresse i folkeregisteret, ettersom KRR ikke har informasjon om adresser. Det er viktig at det ikke finnes lokaliserende informasjon i f.eks. e-postadressen som er registrert i KRR.

Innbyggere med adressesperre har et særlig behov for sikker tilgang til digitale tjenester for å redusere risiko for å møte trusselutøver ved fysisk oppmøte. Digitale tjenestetilbud må iverksette tilstrekkelige tiltak for kontroll over opplysningsflyt for denne gruppen av innbyggere.Et annet tiltak er at innbyggere med sperret adresse ikke kan la seg representere ved fullmakt eller ved foreldre-representasjon digitalt.

Det må vurderes særskilt om personer med adressesperre kan benytte seg av for eksempel digitale skjematjenester/spørreskjema uten å måtte oppgi geolokaliserende informasjon. Skjema som i utgangspunktet er anonyme kan likevel gi opplysninger om oppholdssted hvis brukeren må oppgi postnummer eller fylke.

Automatiserte meldinger skal sendes til den adressen som fremgår av folkeregisteret. Bruk av tidligere adresse kan medføre fare for den trusselutsatte.

2.3.5.1 Sending av post

Mottakers navn (personen med adressesperre) må påføres konvolutten i tillegg til SOT 6 adressen.

Eksempel på riktig adressering:

Ola Nordmann

SOT 6

Postboks 2094 Vika

0125 Oslo

Er man usikker på postadressen, kan man alltid sende post via SOT 6.

Det er alltid en god regel å dobbeltsjekke adressen før noe sendes - for eksempel prøvesvar, innkallinger osv. Dersom pasenten har fortrolig adresse må det alltid kontrolleres at man kun sender informasjon om adresse til en annen offentlig virksomhet.

2.3.6 Avvikshåndtering

Virksomheten må ha gode rutiner for å følge opp hendelser som angår adressesperrer og annen geolokaliserende informasjon.

Ved uberettiget tilgang til graderte adresseopplysninger, skal den dataansvarlige varsle sitt lokale politidistrikt eller Kripos. For å sikre at kontakt med rette vedkommende opprettes så raskt som mulig, bør virksomheten ha klargjort hva som er rett kontaktpunkt hos politiet. Ved varsling av avvik til Datatilsynet skal det alltid gis samtidig varsel til politiet eller Kripos.

I håndteringen av avviket bør virksomheten så raskt som mulig forsøke å identifisere hvem som kan ha hatt tilgang til opplysningene og hvilke opplysninger det er snakk om.

2.3.7 Spesielt om problemstillinger rundt barn

Det er en del barn som er trusselutsatte, hvor foreldre eller andre nære familiemedlemmer som har foreldreansvar kan være trusselutøvere, og hvor disse har rett til innsyn i medisinske dokumenter pga. foreldreansvar. Barneloven § 47 første ledd siste punktum kan komme til anvendelse for de geolokaliserende opplysningene om barnet.

Disse dokumentene kan gi lokaliserende informasjon, og må derfor håndteres etter virksomhetens rutiner som gjelder spesielt for å ivareta utsatte barn. Det må sikres at trusselutøveren ikke får informasjon som er geolokaliserende, for eksempel tilknyting til et legesenter eller helsestasjon. Helsedirektoratet har utgitt et rundskriv om innsyn i journal, som også omhandler forholdet til barns journaler.