



POLITIET
KRIPOS

Seksjon for operative tjenester

**Behandling av opplysninger om personer med
adressesperre**

Veiledning

ÅPEN

1.0/13. januar 2023

Innhold

1. Innledning	3
1.1. Formålet med veiledningen.....	3
1.2. Om adressesperre	3
1.3. Hjemmelsgrunnlag	4
1.4. Definisjoner.....	4
2. Oversikt over utvalgt relevant lovverk	5
3. Effekten av en adressesperre	7
3.1. I folkeregisteret	7
3.2. For den trusselutsatte.....	7
4. Beskyttelse av personer med adressesperre	8
4.1. Hva skal beskyttes?.....	8
4.2. Hva er geolokaliserende opplysninger?.....	8
4.3. Hvordan kan opplysningene beskyttes?.....	8
4.4. Kommunikasjon med den trusselutsatte.....	9
4.4.1. Post.....	9
4.4.2. E-post og digipost	9
5. Informasjonssikkerhet og risikovurdering	10
5.1. Forhold som kan påvirke risiko.....	10
5.2. Konsekvenser av et sikkerhetsbrudd.....	10
5.3. Avviksbehandling	11
6. Taushetsplikt, innsyn i og utlevering av opplysninger	12
6.1. Taushetsplikt	12
6.1.1. Forvaltningsorganer.....	12
6.1.2. Virksomheter som ikke er underlagt lovbestemt taushetsplikt.....	12
6.2. Innsyn og utlevering	12
6.2.1. Innsyn i opplysninger registrert om en selv	12
6.2.2. Utlevering eller innsyn i opplysninger om andre	12
7. Referanser.....	14
.....	15

1. Innledning

1.1. Formålet med veiledningen

Omkring 450 mennesker i Norge lever til enhver tid med beskyttelsestiltaket adressesperre. Adressesperre kan iverksettes i de tilfellene hvor det finnes en reell og alvorlig trussel mot en persons liv, helse eller frihet og hvor mindre inngripende tiltak ikke anses tilstrekkelige.

Mange aktører i det norske samfunnet behandler opplysninger om personer med adressesperre. Det er svært viktig at opplysninger som kan si noe om hvor den trusselutsatte befinner seg ikke kommer uvedkommende i hende. Formålet med dette dokumentet er å gi aktørene veiledning om behandling av opplysninger om personer med adressesperre, og bidra til å sette aktørene i stand til å foreta gode vurderinger av behandling av opplysninger om denne gruppen.

Det understrekes at hver enkelt aktør har ansvaret for å sikre etterlevelse av personvernregelverket, herunder utarbeide nødvendige interne rutiner.

Målgruppen for dokumentet er offentlige og private aktører som leverer tjenester til fysiske personer. Det omfatter blant annet:

- Barnehage, skole og andre utdanningsinstitusjoner
- NAV, barnevernet og andre offentlige organer som yter offentlige tjenester
- DIFI, Skattedirektoratet, E-helsedirektoratet og andre offentlige leverandører av elektroniske innbyggertjenester
- Tilbydere av helsetjenester, herunder de kommunale helsetjenestene, spesialisthelsetjenesten, privatpraktiserende leger, tannleger, fysioterapeuter oa.
- Domstolene
- Leverandører av e-komptjenester, for eksempel mobiltelefoni, internett og apper til bruk i skole mv.
- Private leverandører av offentlige ytelser
- Posten og andre leverandører av kommunikasjonstjenester
- Strømlleverandører
- Utryknings- og redningstjenester
- Forskningsinstitusjoner

1.2. Om adressesperre

Adressesperre er et tiltak som kan iverksettes for å beskytte trusselutsatte personer. At en person er trusselutsatt vil si at personen står i fare for å bli utsatt for alvorlig kriminalitet rettet mot liv, helse eller frihet. Det vil si at trusselutøveren er vurdert å ha kapasitet til og intensjon om å skade den trusselutsatte, potensielt med dødelig utgang. Det kan typisk være ofre for vold i nære relasjoner eller æresrelatert vold, vitner eller informanter.

Det finnes to typer adressesperre. Adressesperre kode 7 innebærer at den trusselutsattes adresse ikke skal utgis til private. Adresseopplysninger er likevel tilgjengelig for alle offentlige myndigheter som har tilgang til opplysninger fra folkeregisteret. Kode 7-adresseopplysninger er gradert FORTROLIG i henhold til beskyttelsesinstruksen.

En adressesperre kode 6 innebærer at opplysninger om den trusselutsattes adresse ikke er tilgjengelig for brukere av folkeregisteret. Kode 6-adresseopplysninger er gradert STRENGT FORTROLIG i henhold til beskyttelsesinstruksen.

Kripos er nasjonalt kontaktpunkt for adressesperre, og forvalter og utvikler adressesperre som metode.

1.3. Hjemmelsgrunnlag

Politiet og barnevernet kan beslutte iverksettelse av adressesperre, jf. folkeregisterloven § 10-4. Barnevernet beslutter adressesperre i barnevernssaker, politiet i alle andre saker.

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

1.4. Definisjoner

Trusselutsatt	Personer som står i fare for å bli utsatt for alvorlig kriminalitet rettet mot liv, helse eller frihet.
Trusselutøver	Person, gruppering eller organisasjon som utgjør en trussel.
Geolokaliserende opplysninger	Alle opplysninger som kan si noe om hvor en trusselutsatt har vært, befinner seg eller kommer til å befinne seg i fremtiden. Se punkt. 4.2.

2. Oversikt over utvalgt relevant lovverk

Folkeregisterloven

Folkeregisterloven¹ regulerer registrering og behandling av personopplysninger i folkeregisteret. I henhold til folkeregisterloven § 10-4 skal opplysninger som er gradert etter beskyttelsesinstruksen sperres i folkeregisteret. Politiet beslutter gradering i alle saker unntatt barnevernssaker.

Beskyttelsesinstruksen

Beskyttelsesinstruksen² § 3 gir anledning til å gradere opplysninger dersom skadevirkninger som nevnt i § 4 kan oppstå. Opplysningene som graderes må kunne unntas offentlighet i henhold til offentlighetsloven.

Politiet er graderende myndighet ved gjennomføring av adressesperre. Adressesperren kan således kun oppheves av politiet.

Beskyttelsesinstruksen er hjemlet i Kongens instruksjonsmyndighet og kan derfor bare gjøres gjeldende overfor statlige organer.

Personopplysningsloven og personvernforordningen

Personopplysningsloven³ gjennomfører EUs generelle personvernforordning⁴ i norsk rett. I tillegg gir loven noen utfyllende regler om behandling av personopplysninger, herunder om behandling av personopplysninger for arkivformål i allmennhetens interesse, formål knyttet til vitenskapelig eller historisk forskning eller statistiske formål i kapittel 3, og noen unntak fra de registrertes rettigheter i kapittel 4.

Personvernforordningen tar sikte på å verne fysiske mennesker i forbindelse med behandling av personopplysninger. Forordningen fastsetter grunnleggende personvernprinsipper som må være oppfylt ved all behandling av personopplysninger, herunder vern mot uautorisert eller ulovlig behandling og mot utilsiktet tap, ødeleggelse eller skade ("integritet og konfidensialitet").⁵ Den behandlingsansvarlige eller databehandleren skal gjennomføre egnede tekniske og organisatoriske tiltak for å oppnå et egnet sikkerhetsnivå for behandlingen av personopplysningene. Hvilke tiltak som anses egnede, avhenger av hvor sannsynlig det er at et sikkerhetsbrudd oppstår og hvor alvorlige konsekvenser sikkerhetsbruddet kan få for de registrertes rettigheter og friheter.⁶ Tiltakene skal blant annet være egnet til å sikre "vedvarende konfidensialitet" når det er behov for det.⁷

¹ LOV-2016-12-09-88 Lov om folkeregistrering (folkeregisterloven)

² FOR-1972-03-17-3352 Instruks for behandling av dokumenter som trenger beskyttelse av andre grunner enn nevnt i sikkerhetsloven med forskrifter (beskyttelsesinstruksen)

³ LOV-2018-06-15-38 Lov om behandling av personopplysninger (personopplysningsloven)

⁴ Europaparlaments- og rådsforordning (EU) 2016/679 av 27. april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger samt om oppheving av direktiv 95/46/EF (generell personvernforordning) (General Data Protection Regulation) (GDPR)

⁵ Personvernforordningen artikkel 5 bokstav f

⁶ Personvernforordningen artikkel 32 nr 1.

⁷ Personvernforordningen artikkel 32 nr. 1 bokstav b.

Forvaltningsloven

Forvaltningsloven⁸ regulerer virksomhet som drives av forvaltningsorganer. Som forvaltningsorgan regnes blant annet ethvert organ for stat eller kommune.⁹ Loven inneholder blant annet de generelle taushetspliktsbestemmelsene for forvaltningen.

En beslutning om adressesperre er å anse som et enkeltvedtak i henhold til forvaltningsloven § 2 første ledd bokstav b. Politiet må ved behandling av saker om adressesperre følge bestemmelsene for enkeltvedtak. Dette betyr at bestemmelser om blant annet utrednings- og informasjonsplikt, partsinnsyn, begrunnelse, notoritet, likebehandling og klagerett kommer til anvendelse.

Offentlighetsloven

Offentlighetsloven¹⁰ regulerer allmennhetens rett til innsyn i opplysninger om og knyttet til offentlig virksomhetsutøvelse. Loven gjelder blant annet for staten, fylkeskommunene og kommunene.

⁸ LOV-1967-02-10 Lov om behandlingsmåten i forvaltningssaker (forvaltningsloven)

⁹ Forvaltningsloven § 1

¹⁰ LOV-2006-05-19-16 Lov om rett til innsyn i dokument i offentlig verksemd (offentlighetsloven)

3. Effekten av en adressesperre

3.1. I folkeregisteret

Når politiet har fattet beslutning om at en trusselutsatt skal ha adressesperre, medfører det at den trusselutsattes adresse og andre geolokaliserende opplysninger¹¹ blir sperret i folkeregisteret. Det kreves at den trusselutsatte flytter før en adressesperre kode 6 blir iverksatt. Andre geolokaliserende opplysninger som blir sperret i folkeregisteret kan for eksempel være kommunenummer, postnummer, grunnkrets og valgkrets. Den registrerte adressen når beslutning om adressesperre fattes, samt alle fremtidige adresser frem til adressesperren oppheves, blir sperret.

I tillegg blir personer som får innvilget kode 6 ofte anbefalt å bytte navn, slik at vedkommende ikke kan identifiseres ved hjelp av dokumenter hvor navn fremkommer.

3.2. For den trusselutsatte

For at en adressesperre skal være et effektivt beskyttelsestiltak, kreves høy grad av egeninnsats fra den trusselutsatte. Livet til personer som lever på sperret adresse kan føles begrensende og komplisert på mange områder. Å holde seg skjult over lang tid er svært vanskelig. De fleste trusselutsatte med adressesperre er i en situasjon hvor de har vært nødt til å forsøke å kutte alle bånd til fortiden, samtidig som en adressesperre vanskeliggjør utviklingen av nye bekjenskaper og relasjoner.

Den viktigste konsekvensen av adressesperre er at den trusselutsatte flytter fra hjemmet sitt. I noen tilfeller kan flyttingen føre til tap av viktige eiendeler. Enkelte rekker ikke å ta med seg pass, nødvendige medisiner eller arbeidsattester og skolepapirer. Trusselutsatte må også slutte i sitt tidligere arbeid, bytte bank, bryte kontakten med fastlege, helsestasjon, skolekrets og alle fritidsaktiviteter. Tjenester som krever at man oppgir adresse kan i mange tilfeller ikke brukes og spredning av annen geolokaliserende informasjon må begrenses til et minimum. Bruk av sosiale medier er i mange tilfeller utelukket. Det er svært krevende å i enhver sammenheng måtte huske på å ikke foreta seg noe som gjør at man kan bli avslørt. Tiltaket er således en stor belastning for den trusselutsatte og eventuelle andre som berøres av tiltaket.

¹¹ Se nærmere om geolokaliserende opplysninger i punkt 4.2

4. Beskyttelse av personer med adressesperre

4.1. Hva skal beskyttes?

Virksomheter som behandler opplysninger om trusselutsatte med adressesperre må beskytte geolokaliserende opplysninger om den trusselutsatte.

Opplysning om at en person har adressesperre er i utgangspunktet ikke beskyttelsesverdig. Det bør imidlertid utvises stor forsiktighet med å utarbeide eller sammenstille lister over alle personer med adressesperre innenfor et område eller en nærmere bestemt krets av personer.

4.2. Hva er geolokaliserende opplysninger?

Geolokaliserende opplysninger er alle opplysninger som kan si noe om hvor en trusselutsatt befinner seg eller kommer til å befinne seg i fremtiden, eller hvor hen har oppholdt seg tidligere. Dette innebærer at alle opplysninger om bosted, arbeidsplass, skole, barnehage og andre daglige oppholdssteder må beskyttes. I tillegg må andre opplysninger som kan fortelle noe om den trusselutsattes oppholdssted beskyttes, herunder opplysninger om offentlige og private brukersteder, for eksempel opplysninger om fastlege, barnevernstjeneste og hvilket sykehus den trusselutsatte sogner til.

Alle opplysninger om avtaler med offentlige eller private virksomheter må beskyttes, for eksempel timer hos lege, sykehus, fritidsaktiviteter og andre støtte- eller brukertjenester.

4.3. Hvordan kan opplysningene beskyttes?

Det hviler et selvstendig ansvar på hver enkelt aktør å sikre etterlevelse av personvernregelverket, og det må blant annet utarbeides nødvendige rutiner for å sikre etterlevelse. Personregelverket stiller krav om at det etableres internkontroll for å ivareta virksomhetens ansvar samt demonstrere etterlevelse etter personvernregelverket. Internkontroll fungerer samtidig som de ansattes verktøy for å utføre oppgaver på en forsvarlig og sikker måte.

Opplysningene kan beskyttes for eksempel gjennom merking, tilgangsstyring, sperring og restriktiv behandling.

Når man behandler opplysninger om personer som bor på adressesperre, er det viktig at det fremkommer tydelig at opplysningene har et særskilt beskyttelsesbehov. Geolokaliserende opplysninger om personer på adressesperre bør derfor som hovedregel merkes som sådan, slik at de som behandler opplysningene vet at opplysningene har et særskilt beskyttelsesbehov.

Tilgangsstyring kan brukes til å sørge for at beskyttelsesverdige opplysninger om personer som bor på adressesperre ikke er tilgjengelige for alle brukere av et informasjonssystem. Som hovedregel er tilgangsstyring et informasjonssikkerhetstiltak som må vurderes ved behandling av geolokaliserende opplysninger om personer med adressesperre.

Sperring kan benyttes der enkelte av opplysningene om en person på adressesperre må være tilgjengelig for brukere av et informasjonssystem, men de geolokaliserende opplysningene ikke må være tilgjengelige.

I tilfeller hvor man ikke anser at geolokaliserende opplysninger om personer med adressesperre kan beskyttes tilfredsstillende på andre måter, kan man beslutte at geolokaliserende opplysninger om en person med adressesperre ikke skal behandles i et system eller at opplysningene kun skal behandles manuelt. Dersom opplysningene behandles av en offentlig tjenesteyter, er det viktig å huske på at personer med adressesperre i utgangspunktet har rett til det samme tilbudet fra offentlige myndigheter som personer uten adressesperre. For personer med adressesperre må imidlertid sikkerhetsaspektet veie svært tungt.

4.4. Kommunikasjon med den trusselutsatte

4.4.1. Post

Post til den trusselutsatte skal sendes til registrert postadresse i folkeregisteret. Dersom man ikke har tilgang til postadressen i folkeregisteret, eller er i tvil om hvilken adresse som skal brukes, kan man sende til følgende adresse:

SOT 6
Postboks 2094 Vika
0125 Oslo

Den trusselutsattes navn må påføres konvolutten. Eksempel på riktig adressering:

Ola Nordmann
SOT 6
Postboks 2094 Vika
0125 Oslo

4.4.2. E-post og digipost

Det er en fordel for personer med adressesperre å motta post digitalt.

Offentlige myndigheter kan benytte seg av kontakt- og reservasjonsregisteret (KRR) ved digital kommunikasjon med trusselutsatte. I KRR skal det blant annet ligge en e-postadresse til den trusselutsatte. Videre kan kommunikasjon gjennom Digipost og Altinn benyttes.

Private kan i tillegg til Digipost benytte e-post dersom de har fått oppgitt e-postadresse fra den trusselutsatte.

5. Informasjonssikkerhet og risikovurdering

5.1. Forhold som kan påvirke risiko

En rekke forhold kan påvirke hvordan risikoen for sikkerhetsbrudd skal vurderes, og hvilke tiltak som er nødvendige for å sikre et tilstrekkelig sikkerhetsnivå for geolokaliserende opplysninger. Det følgende omtales noen momenter:

- Delt foreldreansvar. Dersom den trusselutsatte og trusselutøveren har felles barn, kan trusselutøveren ha foreldreansvaret i behold til tross for at den trusselutsatte og barna bor på sperret adresse. Ved leveranse av tjenester hvor foreldre skal kunne utøve rettigheter eller kontakte det offentlige på vegne av sine barn, er det viktig at kun foreldre som bor på sperret adresse sammen med barna, kan utøve rettigheter på vegne av barnet.
- Dersom den trusselutsatte er under vergemål, er informasjon om hvem som er verge å anse som geolokaliserende opplysninger. Opplysninger om vergen til en person med adressesperre må således skjermes på lik linje med andre geolokaliserende opplysninger.
- Dersom det er registrert fullmakter på den trusselutsatte fra før adressesperren ble iverksatt, må disse fullmaktene fjernes. Kun fullmakter gitt etter at adressesperren ble iverksatt kan være aktive.

5.2. Konsekvenser av et sikkerhetsbrudd

Personvernforordningen krever at virksomheter har en risikobasert tilnærming til informasjonssikkerhet.¹² Når behandling av geolokaliserende opplysninger om personer som bor på adressesperre skal risikovurderes, er det viktig å forstå konsekvensene av at geolokaliserende opplysninger om personer med adressesperre kommer uvedkommende i hende.

En adressesperre er et av de mest alvorlige tiltakene politiet kan iverksette for å beskytte enkeltpersoner. Tiltaket iverksettes kun i de tilfellene hvor mindre inngripende tiltak ikke anses tilstrekkelige. Når politiet har innvilget en adressesperre, må det legges til grunn at trusselutøveren har kapasitet til å benytte de verktøy som er tilgjengelig til å lokalisere og skade den trusselutsatte, i verste fall med døden til følge. Konsekvensene for den trusselutsatte ved et sikkerhetsbrudd kan således være svært alvorlige. Selv om et sikkerhetsbrudd ikke fører til at trusselutøveren klarer å lokalisere den trusselutsatte, vil bruddet kunne være svært belastende for den trusselutsatte. Dersom den trusselutsattes oppholdssted har blitt kjent for uvedkommende, må politiet vurdere om den trusselutsatte skal relokaliseres. Det vil si at den trusselutsatte og eventuelle barn må flytte til et nytt sted, med ny jobb, ny skole eller barnehage og må jobbe for å bygge opp kontakter i nærmiljøet på nytt. Dette kan medføre retraumatisering av både den trusselutsatte og eventuelle barn. For barna kan de tapene de lider sammenlignes med de tap barn lider når de flykter fra krig og nød.

Konsekvensene ved sikkerhetsbrudd kan således være svært alvorlige. Dette må tillegges vekt ved vurderingen av hvilke sikkerhetstiltak som er nødvendige å iverksette,

¹² Personvernforordningen artikkel 32 nr. 1.

noe som tilsier at det kan være riktig med strenge sikkerhetstiltak selv om sannsynligheten for sikkerhetsbrudd anses som lav.

5.3. Avviksbehandling

Dersom det skulle oppstå et sikkerhetsbrudd og geolokaliserende opplysninger om en eller flere trusselutsatte kommer på avveie, kan det være av meget stor betydning for den trusselutsatte og politiet at det kan fastslås *hvem* som har fått tilgang til opplysningene og *hvilke* opplysninger de har hatt tilgang til.

For å sikre nødvendig oppfølging av den eller de trusselutsatte ved et sikkerhetsbrudd, er det viktig at den behandlingsansvarlige snarest mulig kontakter sitt lokale politidistrikt eller Kripos for å orientere om sikkerhetsbruddet.

Kontaktinformasjon finnes på <https://www.politiet.no>.

6. Taushetsplikt, innsyn i og utlevering av opplysninger

6.1. Taushetsplikt

6.1.1. Forvaltningsorganer

Forvaltningsloven § 13 er den generelle taushetspliktsbestemmelsen for blant annet statlige og kommunale organer. Bestemmelsen kommer til anvendelse med mindre særlovgivning fastsetter taushetsplikt.

I henhold til forvaltningsloven § 13 første ledd nr. 1 plikter enhver som gjør tjeneste for et forvaltningsorgan å hindre at andre får adgang eller kjennskap til opplysninger om personlige forhold. Bestemmelsens annet ledd fastslår at blant annet bopel og arbeidssted ikke anses som personlige forhold med mindre slike opplysninger røper "...andre forhold som må anses som personlige". Geolokaliserende opplysninger om personer som bor på adressesperre faller inn under forvaltningsloven § 13 annet ledd første punktum, og opplysningene må anses som taushetsbelagte.¹³

6.1.2. Virksomheter som ikke er underlagt lovbestemt taushetsplikt

For virksomheter som ikke er underlagt lovbestemt taushetsplikt vil anledningen til å dele personopplysninger med andre bero på om behandlingen kan gjennomføres i henhold til bestemmelsene i personvernforordningen. Når det gjelder deling av geolokaliserende opplysninger om personer med adressesperre, må det gjennomføres en risikovurdering hvor det tas hensyn til de alvorlige konsekvensene det kan få for de trusselutsatte dersom opplysninger kommer uvedkommende i hende.

6.2. Innsyn og utlevering

6.2.1. Innsyn i opplysninger registrert om en selv

En adressesperre er ikke til hinder for at den trusselutsatte får innsyn i opplysninger om seg selv. En begjæring om innsyn må behandles i henhold til aktuelt regelverk. Resultatet av begjæringen må formidles eller sendes til den trusselutsatte på en sikker måte som sørger for konfidensialitet.

6.2.2. Utlevering eller innsyn i opplysninger om andre

Det kan oppstå spørsmål om utlevering av opplysninger om personer som bor på adressesperre. Dette kan for eksempel være aktuelt ved spørsmål om innsyn etter offentlighetsloven, partsinnsyn eller ved spørsmål om foreldres rett til informasjon om sine barn.

Ved behandling av begjæringer om innsyn i opplysninger om personer som bor på adressesperre, er det viktig å huske på at også opplysninger om hvilket kontor eller

¹³ For ytterligere informasjon om innholdet i taushetsplikten, se veileder til offentlighetsloven (G-0419) punkt 6.2.3.1.

hvilken instans som har behandlet begjæringen om innsyn eller på annen måte hatt befatning med saken kan si noe om hvor den trusselutsatte oppholder seg.

Ved behandling av innsynsbegjæringer etter offentlighetsloven, vil geolokaliserende opplysninger om personer med adressesperre som hovedregel kunne unntas med hjemmel i offentlighetsloven § 13 nr. 1 jf. fvl. § 13 annet ledd første punktum eller med henvisning til annen taushetspliktsbestemmelse. Videre vil man kunne vurdere om offl. § 24 tredje ledd annet punktum første alternativ kan komme til anvendelse.

Når det oppstår spørsmål om partsinnsyn i saker hvor en person med adressesperre er part, kan det vurderes om forvaltningsloven § 19 annet ledd bokstav b kan komme til anvendelse for de geolokaliserende opplysningene.

Dersom en forelder som ikke bor på adressesperre anmoder om opplysninger om sitt barn som bor på adressesperre, kan det vurderes om barneloven § 47 første ledd siste punktum kan komme til anvendelse for de geolokaliserende opplysningene.

7. Referanser

LOV-1967-02-10 om behandlingsmåten i forvaltningssaker (forvaltningsloven)

LOV-1981-04-08-7 om foreldre og barn (barneloven)

LOV-2006-05-19-16 om rett til innsyn i dokument i offentlig verksemd
(offentlighetsloven)

LOV-2016-12-09-88 om folkeregistrering (folkeregisterloven)

LOV-2018-06-15-38 om behandling av personopplysninger (personopplysningsloven)

FOR-1972-03-17-3352 Instruks for behandling av dokumenter som trenger beskyttelse
av andre grunner enn nevnt i sikkerhetsloven med forskrifter (beskyttelsesinstruksen)

Veileder – behandling av opplysninger om personer med adressesperre

Utgitt: 13. januar 2023

Utgiver: Kripos