Oslo

Byrådsavdeling for finans

Om mottak og håndtering av informasjon om adressesperre

Dette dokumentet skal gi ansatte og ledere i Oslo kommune økt kunnskap og faglig råd om hva informasjon om adressesperre er og hensyn man må ta ved behandling.

Foto: Claire Dornic

Informasjon om mottak og håndtering av informasjon om adressesperre

Dette dokumentet skal gi ansatte og ledere i Oslo kommune økt kunnskap og faglig råd om hva informasjon om adressesperre er, hensyn man må ta ved behandling av opplysninger om adressesperre og hvilket ansvar som påligger ansatte og kommunens virksomheter m.m.

Virksomheter i Oslo kommune kan ha ulike behov og ulikt utgangspunkt for å motta og håndtere informasjon om adressesperre. Det er derfor viktig at virksomhetene selv foretar de nødvendige vurderingene etter personvernregelverket og annet relevant regelverk, før behandling av denne typen personopplysninger forekommer. Det kan for eksempel være å gjennomføre personvernvurderinger og risiko- og sårbarhetsvurderinger av informasjonssikkerhet (ROS).

Hva menes med adressesperre?

Adressesperre er tiltak som kan iverksettes for å beskytte trusselutsatte personer. Å være trusselutsatt innebærer at en person står i fare for å bli utsatt for alvorlig kriminalitet rettet mot liv, helse eller frihet. Dette kan typisk være personer som er vitner, informanter eller ofre for æresrelatert vold eller vold i nære relasjoner.

Når en adressesperre iverksettes medfører det at all informasjon som kan si noe om hvor den trusselutsatte oppholder seg (GEO-lokaliserende informasjon) er gradert. Dette kan være bostedsadresse, skole, arbeidsplass, barnehage, fastlege, bruk av NAV-kontor og andre lokale støtteordninger m.m. Hvilke opplysninger som anses som GEO-lokaliserende må vurderes konkret i det enkelte tilfellet. Tilgjengeliggjøring av denne typen informasjon kan i verste fall medføre alvorlige konsekvenser for den trusselutsattes liv og helse og bør derfor ikke tilgjengeliggjøres.

Typer adressesperre

I folkeregisterloven blir opplysninger om adresse og andre GEO-lokaliserende opplysninger som er gradert etter beskyttelsesinstruksen sperret. Loven betegner disse opplysningene som “graderte opplysninger” og har også en egen bestemmelse som regulerer utlevering av slik informasjon. Politiet og barnevernstjenesten har adgang til å iverksette adressesperre i samsvar med folkeregisterloven. Barnevernloven inneholder også en bestemmelse for vedtak om “skjult adresse”, som besluttes av fylkesnemnda eller domstolen for tilfeller hvor foreldre ikke skal kunne vite hvor barna oppholder seg. Dette er ikke det samme som adressesperre gradert etter beskyttelsesinstruksen og benyttes som regel bare i barnevernets egne systemer.

Beskyttelsesinstruksen inneholder bestemmelser som anvendes ved behandling av dokumenter som trenger beskyttelse av andre grunner enn de som er nevnt i sikkerhetsloven med sine forskrifter. For personer som er trusselutsatt vil geolokaliserende informasjon knyttet til disse personene graderes som “Fortrolig” eller “Strengt fortrolig” etter beskyttelsesinstruksen.

Vær oppmerksom på at beskyttelsesinstruksen kun gjelder statlig forvaltning, men kommunens virksomheter har likevel en plikt til å etablere tilstrekkelig sikkerhetstiltak som oppfyller kravet etter personvernforordningens art.32, basert på en risikovurdering ved behandling av adressesperreinformasjon. Siden konsekvensen for den registrerte er så høy med potensiell fare for liv og helse uavhengig av sannsynlighetsnivået, er gjengs praksis og oppfordring fra Kripos at kommunens

virksomheter følger kravene i beskyttelsesinstruksen. På denne måten vil man sikre at disse opplysningene blir behandlet likt både i statlig og kommunal sektor.

Adressesperre gradert "Fortrolig" benyttes dersom det vil kunne skade en enkeltperson at dokumentets innhold blir kjent for uvedkommende. Dette innebærer at den trusselutsattes adresse og annen GEO-lokaliserende informasjon i utgangspunktet ikke skal utgis til private og offentlige. Slik informasjon omtales ofte som kode 7.

Hvis kommunens virksomhet har hjemmel til å innhente taushetsbelagt informasjon i samsvar med folkeregisterloven §10-2 kan opplysningene likevel være tilgjengelig.

Adressesperre gradert "Strengt fortrolig" benyttes dersom det vil kunne forårsake betydelig skade for en enkeltperson at dokumentets innhold blir kjent for uvedkommende. Dette innebærer at opplysninger om den trusselutsattes adresse og annen GEO-lokaliserende informasjon ikke skal utgis til noen. Slik gradert informasjon omtales ofte som kode 6.

Personer **med adressesperre "strengt fortrolig"** vil ved tilgang til folkeregisterinformasjon ikke være registrert med bostedsadresse, men markert med "SOT6". Dersom en virksomhet ønsker utlevert denne typen opplysninger må man henvende seg direkte til myndigheten som har gradert opplysningene, enten politiet eller barnevernstjenesten.

Adresseinformasjon om institusjonsopphold

I tillegg til informasjon om adressesperre er det greit for ansatte å kjenne til adresseinformasjon om institusjonsopphold, også kalt kode 4. Kode 4 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 betegnes med klientadresse. Aldershjem, sykehus og syke-/pleiehjem vil derimot falle utenfor. Disse opplysningene skal behandles med varsomhet.

Hvem forvalter adressesperreordningen?

Kripos er nasjonalt knutepunkt for adressesperre, og forvalter og utvikler adressesperre som metode, med unntak for saker etter barnevernloven (barnevernssaker).

Barneverntjenesten forvalter ordningen med skjult adresse for barn som er plassert i fosterhjem eller institusjon etter vedtak om omsorgsovertagelse, vedtak om akuttplassering eller vedtak om forbud mot flytting etter barnevernloven §7-2 tredje ledd. I de tilfellene hvor det er besluttet skjult adresse etter barnevernloven §13-5 må barneverntjenesten kontakte politiet og videreformidle dette, slik at det også kan besluttes adressesperre med hjemmel i beskyttelsesinstruksen.

For den ansatte:

Du som ansatt må huske at dersom du mottar informasjon om adressesperre må dette behandles med varsomhet. Det kan være gjennom saksbehandling, oppslag i folkeregisteret, og andre tjenester kommunen tilbyr. Alle virksomheter i Oslo kommune som kan behandle informasjon om adressesperre

skal ha rutiner for håndtering av slik informasjon. Dette skal du som ansatt kjenne til og benytte dersom du mottar slik informasjon.

Det er viktig å merke seg at politiet gjennomfører en omfattende prosess før adressesperre etter beskyttelsesinstruksen vedtas. I denne perioden oppfordres berørte personer om ikke å oppgi fullt fødsels- og personnummer bl.a til offentlige myndigheter. Det er viktig at Oslo kommunes ansatte respekterer dette dersom man møter innbyggere som ikke ønsker å oppgi fullt fødselsnummer begrunnet i at man er under en slik prosess. I stedet kan man be disse personene om å oppgi sin kontaktperson hos politiet.

Dersom det oppstår avvik, hvor for eksempel opplysninger om adressesperre er på avveie, må du som ansatt følge virksomhetens avviksrutiner. Virksomheten skal sørge for at rette instanser blir varslet slik at disse kan vurdere hvorvidt tiltak skal iverksettes overfor den trusselutsatte.

For virksomheten:

Kommunens virksomheter plikter å hindre at personer eller instanser utenfor kommunen eller innad i kommunen får kjennskap til innbyggers lokaliserende informasjon, når innbygger er registrert på adressesperre i Folkeregisteret. Virksomheten må derfor sørge for gode sikkerhetsmekanismer i deres systemer som behandler informasjon om adressesperre. 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. GEO-lokaliserende opplysninger om personer på adressesperre bør derfor som hovedregel merkes, slik at de som behandler opplysningene vet at opplysningene har et særskilt beskyttelsesbehov.

Det er viktig å merke seg at i forbindelse med beskyttelse av personer kan disse gis et nytt oppholdssted. Det er da avgjørende at ansatte i kommunen ikke registrerer informasjon som kan knytte personen til bostedet i systemer som ikke er godt nok tilgangsstyrt. Dette gjelder GEO-lokaliserende informasjon.

Det er også viktig at virksomheten sørger for å utarbeide rutiner som skal sikre at ansatte i virksomhetene er kjent med håndtering av innbyggerinformasjon ved sperret (fortrolig og strengt fortrolig) adresse og sikre riktig registrering av opplysningene der det er relevant. I tillegg er det nødvendig å sikre at ansatte får opplæring i rutinene virksomheten har for håndtering av informasjon om adressesperre.

Det vil kunne være ulike scenarier hvor ansatte/virksomheten kan røpe informasjon om adressesperre. Under følger eksempler på scenarier hvor oppsporing av personer med adressesperre som er viktige å være oppmerksom på:

- Oppsporing ved at utro ansatt snoker i opplysninger om personer på adressesperre
- Oppsporing ved at ansatte utsettes for sosial manipulering. Det er derfor viktig med ekstra årvåkenhet blant ansatte når de behandler personer med sperret adresse
- Oppsporing ved at informasjon sendes til kontaktpunkter som trusselutøveren har kontroll over, typisk til gamle adresser.

Avvikshåndtering

Virksomheten skal sørge for at avviksrutiner ivaretar også avvik knyttet til opplysninger om adressesperre. Rutinene må være på plass og alle ansatte må vite hva de skal gjøre dersom et slikt avvik oppstår.

Rutinene til virksomheten skal også inneholde varsling til Kripos eller lokale politidistrikt, og eventuelt barnevernstjenesten for å sikre nødvendig oppfølging av den eller de trusselutsatte. Denne varslingen kan være av meget stor betydning for den trusselutsatte og politiet ved at disse selv kan foreta en vurdering av *hvem* som har fått tilgang til opplysning og *hvilke* opplysninger uvedkommende har hatt tilgang til.

Behandling av informasjon om adressesperre i eksisterende eller nye systemer/løsninger

Det er viktig å huske på at i et system/løsning vil man ikke bare behandle opplysninger om adressesperre fordi denne typen informasjon ofte er en del av en større behandling. Det kan for eksempel være i saksbehandlingssystem hvor man tildeler barnehageplass, utstedelse av bibliotekkort, i en pasientjournal, ved bruk av app knyttet til virksomheten mv.

Det er derfor viktig at man i personvernvurdering av virksomhetens system/løsning, løfter frem risikoen for den registrerte ved behandlingen av informasjon om adressesperre og hvilke tiltak man iverksetter for behandling av denne typen informasjon skal forekomme på en sikker måte (der det er relevant). For eksempel bør man særlig løfte frem risikoen knyttet til den registrertes friheter, herunder retten til privatliv og retten til å ikke bli diskriminert. Sistnevnte gjelder spesielt hvor en virksomhet ikke kan tilby digital løsning for personer med adressesperre. Tilsvarende bør også ROS-vurderinger løfte frem risiko knyttet til adressesperre. Både personvernvurderinger og ROS-vurderingene må komme før den planlagte behandlingen starter.