NSM

Veileder i håndtering og beskyttelse av sikkerhetsgradert informasjon

torsdag 24. november 2022

Nasjonal sikkerhetsmyndighet (NSM) er fagorgan for forebyggende sikkerhet, og sikkerhetsmyndighet etter lov om nasjonal sikkerhet (sikkerhetsloven). NSM skal gi informasjon, råd og veiledning om forebyggende sikkerhetsarbeid.

Sikkerhetsloven med tilhørende forskrifter trådte i kraft 1. januar 2019. Loven skal bidra til å forebygge, avdekke og motvirke tilsiktede handlinger som direkte eller indirekte kan skade nasjonale sikkerhetsinteresser.

Sikkerhetsloven gjelder for statlige, fylkeskommunale og kommunale organer, og for leverandører av varer eller tjenester i forbindelse med sikkerhetsgraderte anskaffelser. De enkelte departementer skal innenfor sitt ansvarsområde vedta at andre virksomheter skal underlegges loven dersom de behandler sikkerhetsgradert informasjon, eller råder over informasjon, informasjonssystemer, objekter eller infrastruktur som har avgjørende betydning for grunnleggende nasjonale funksjoner, eller driver aktivitet som har avgjørende betydning for disse funksjonene.

NSMs håndbøker og tekniske råd gir utfyllende anbefalinger om hvordan regelverkets funksjonelle krav kan oppfylles. Håndbøkene og de tekniske rådene beskriver fremgangsmåter, prosedyrer og gir eksempler på tiltak for å hjelpe virksomhetene i regelverksanvendelsen. Disse må ses i sammenheng med NSMs veiledere til lov og forskrift.

NSM gir i tillegg ut veiledere som gir uttrykk for NSMs syn på hvordan lov og forskrift er å forstå.

Håndboken anbefales lest i sammenheng med lov og forskrift, samt NSMs øvrige relevante veiledere, håndbøker og tekniske råd.

Innhold

Om denne veilederen

Nasjonal sikkerhetsmyndighet (NSM) er fagorgan for forebyggende sikkerhet, og sikkerhetsmyndighet etter lov om nasjonal sikkerhet (sikkerhetsloven). NSM skal gi informasjon, råd og veiledning om forebyggende sikkerhetsarbeid.

Sikkerhetsloven med tilhørende forskrifter trådte i kraft 1. januar 2019. Loven skal bidra til å forebygge, avdekke og motvirke tilsiktede handlinger som direkte eller indirekte kan skade nasjonale sikkerhetsinteresser.

Sikkerhetsloven gjelder for statlige, fylkeskommunale og kommunale organer og for leverandører av varer eller tjenester i forbindelse med sikkerhetsgraderte anskaffelser. De enkelte departementer skal innenfor sitt ansvarsområde vedta at andre virksomheter skal underlegges loven dersom de behandler sikkerhetsgradert informasjon eller råder over informasjon, informasjonssystemer, objekter eller infrastruktur som har avgjørende betydning for grunnleggende nasjonale funksjoner, eller driver aktivitet som har avgjørende betydning for disse funksjonene.

NSMs veiledninger utdyper regelverkforståelsen, herunder den tematiske sammenhengen mellom ulike bestemmelser i sikkerhetsloven og tilhørende forskrifter. Veilederne representerer NSMs syn på hvordan lov og forskrifter er å forstå, og danner et grunnlag for virksomhetenes arbeid med å etterleve regelverket.

NSM gir i tillegg ut håndbøker og tekniske råd som gir mer utfyllende anbefalinger om hvordan lovens funksjonelle krav kan oppfylles. Håndbøkene og de tekniske rådene beskriver fremgangsmåter, prosedyrer og gir eksempler på tiltak for å hjelpe virksomhetene i regelverksanvendelsen.

Veilederen anbefales lest i sammenheng med lov og forskrift, samt NSMs øvrige relevante veiledere, håndbøker og tekniske råd.

1 Innledning

Denne veilederen omhandler håndtering og beskyttelse av sikkerhetsgradert informasjon lagret på dokument eller lagringsmedium. Målgruppen for veilederen er virksomheter som kommer i befatning med sikkerhetsgradert informasjon.

Sikkerhetsloven § 5-2 stiller krav om at virksomheten skal sørge for et forsvarlig sikkerhetsnivå for skjermingsverdig informasjon, slik at informasjonen (a) ikke blir kjent for uvedkommende, (b) ikke går tapt eller blir endret, (c) er tilgjengelig ved tjenstlig behov. For veiledning om forsvarlig sikkerhetsnivå vises det til Nasjonal sikkerhetsmyndighets (NSM) Veileder i sikkerhetsstyring. Foruten nevnte veileder må denne veilederen også sees i sammenheng med Veileder i verdivurdering av informasjon og Veileder i fysisk sikkerhet.

Prop. 153 L (2016-2017) s. 175: «Begrepet informasjon skal forstås vidt. Måten informasjonen er tilvirket på og hvilken form informasjonen har, er ikke relevante momenter i vurderingen av om noe er informasjon. Begrepet omfatter for eksempel informasjon i form av fysiske dokumenter, digitale og maskinlesbare signaler, film, lydopptak og muntlige opplysninger.»

Sikkerhetsgradert Informasjon kan lagres og formidles på flere måter. Informasjon kan meddeles både muntlig og skriftlig, og kan nedtegnes og lagres på ulike formater. Sikkerhetsgradert informasjon må beskyttes, da denne har skadepotensial for nasjonale sikkerhetsinteresser om den blir kjent for uvedkommende. I denne sammenheng er det viktig å erkjenne at fysisk små lagringsmedier kan romme enorme mengder informasjon, og således ha et langt større iboende skadepotensiale for nasjonale sikkerhetsinteresser enn en samling av papirdokumenter.

Begrepene dokument og lagringsmedium er definert i forskrift om virksomheters arbeid med forebyggende sikkerhet (virksomhetsikkerhetsforskriften), jf. § 2 bokstav b og bokstav c.

b) dokument: en logisk avgrenset mengde med informasjon som er lagret på et medium for senere lesing, lytting, framføring, overføring eller lignende.

c) lagringsmedium: en elektronisk eller fysisk enhet for lagring av informasjon til bruk for senere lesing, lytting, framføring, overføring eller lignende.

I utgangspunktet beskyttes informasjon sikkerhetsgradert av NATO på samme måte som norsk sikkerhetsgradert informasjon. I den utstrekning NATOs krav avviker fra det som følger av bestemmelser i eller i medhold av sikkerhetsloven skal imidlertid NATOs krav legges til grunn, jf virksomhetssikkerhetsforskriften § 21. Ved beskyttelse av NATO sikkerhetsgradert informasjon vil NATO Security Policy, C-

M(49)2002 Enclosure E og AC/35-D/2002 gjelde i tillegg til krav i sikkerhetsloven og virksomhetsikkerhetsforskriften.

Sikkerhetsgradert informasjon mottatt fra fremmed stat eller internasjonal organisasjon skal behandles i samsvar med hva som er nedfelt i sikkerhetsavtalen med den aktuelle stat. Det bærende prinsipp i disse avtalene er at den annen stats informasjon skal behandles som norsk sikkerhetsgradert informasjon på tilsvarende gradsnivå.

2 Merking av informasjon

> Virksomhetsikkerhetsforskriften § 28 Merking av dokumenter og lagringsmedier som inneholder sikkerhetsgradert informasjon. Dokumenter og lagringsmedier skal merkes med den høyeste sikkerhetsgraden som gjelder for informasjon i dokumentet eller lagringsmediet, og med hvor lenge graderingen varer. Merkingen skal være lett synlig og lett kunne gjøres kjent for alle i og utenfor virksomheten som skal håndtere informasjonen. Dersom ikke all informasjon i et dokument eller et lagringsmedium har den samme sikkerhetsgraderingen, skal merkingen, så langt det er praktisk mulig, vise hvilke deler som har hvilken gradering eller ingen gradering. Dokumenter og lagringsmedier med informasjon som utleveres til en annen stat eller internasjonal organisasjon etter § 25, skal merkes med hvilken stat eller organisasjon utleveringen gjelder

Sikkerhetsgradert informasjon merkes på bakgrunn av sikkerhetsloven § 5-3. Bestemmelsen angir de ulike sikkerhetsgraderingene, og hva som skal til for at informasjon skal graderes på de ulike nivåene. Den høyeste graderingen er STRENGT HEMMELIG etter § 5-4 første ledd bokstav a). Informasjon som skal graderes STRENGT HEMMELIG er informasjon som kan få helt avgjørende skadefølger for nasjonale sikkerhetsinteresser dersom den blir gjort kjent for uvedkommende. Informasjon som skal graderes HEMMELIG etter § 5-3 første ledd bokstav b), er informasjon som kan få alvorlige skadefølger dersom den blir gjort kjent for uvedkommende. Informasjon som skal graderes KONFIDENSIELT er informasjon som § 5-3 første ledd bokstav c), kan få skadefølger for nasjonale sikkerhetsinteresser dersom de blir gjort kjent for uvedkommende. Informasjon som i noen grad kan få skadefølger for nasjonale sikkerhetsinteresser dersom de blir gjort kjent for uvedkommende, skal etter § 5-3, første ledd bokstav d) graderes BEGRENSET.

En sikkerhetsgradering bortfaller etter 30 år hvis ikke annet er bestemt, jf. sikkerhetsloven § 5-3, andre ledd. Der informasjon ikke skal avgraderes automatisk etter 30 år eller der graderingen skal ha en kortere varighet enn 30 år bør dette fremgå av merkingen av dokumentet.

NSM anbefaler som hovedregel at merkingen har rød farge og er påført med store bokstaver (majuskler) i en lett leselig skrifttype (font) for tydeliggjøring av den aktuelle merkingen. For dokumenter med rød eller en mørk bakgrunnsfarge, må andre fargevalg på merkingen vurderes, slik at kravet om lett synlig merking ivaretas.

Merkingen bør på dokumenter påføres øverst og nederst på alle dokumentets sider. For elektroniske filer anbefaler NSM at graderingen fremkommer i filnavnet, f.eks. slik: «(B) filnavn». Ved oversendelse av sikkerhetsgradert informasjon på e-post, anbefaler NSM at sikkerhetsgraden fremkommer i tittelfeltet, f.eks. slik: «(B) Tittel».

Stempler og graderingsmerker i dokumentmaler kan av utseende fremkomme som vist under:

STRENGT HEMMELIG

jf. sikkerhetsloven § 5-3 første ledd bokstav a).

Unntatt offentlighet, jf. offentleglova § 13, jf. sikkerhetsloven § 5-4 andre ledd.

HEMMELIG

jf. sikkerhetsloven § 5-3 første ledd bokstav b).

Unntatt offentlighet, jf. offentleglova § 13, jf. sikkerhetsloven § 5-4 andre ledd.

KONFIDENSIELT

jf. sikkerhetsloven § 5-3 første ledd bokstav c).

Unntatt offentlighet, jf. offentleglova § 13, jf. sikkerhetsloven § 5-4 andre ledd.

BEGRENSET

Jf. sikkerhetsloven § 5-3 første ledd bokstav d).

Unntatt offentlighet, jf. offentleglova § 13, jf. sikkerhetsloven § 5-4 andre ledd.

UNNTATT FRA AUTOMATISK AVGRADERING

jf. sikkerhetsloven § 5-3 andre ledd og virksomhetsikkerhetsforskriften § 29

AVGRADERES AUTOMATISK ETTER X ÅR

jf. sikkerhetsloven § 5-3 andre ledd

AVGRADERES AUTOMATISK DD.MM.YYYY

jf. sikkerhetsloven § 5-3 andre ledd

Dersom informasjonens beskyttelsesbehov har kortere varighet enn 30 år, skal dette fremgå av merkingen. Det kan gjøres ved å sette avgradering til etter et visst antall år, eller på en konkret angitt dato. Dersom varigheten er 30 år, er det ikke nødvendig å angi markeringens levetid, da dette er hovedregelen.

Plikten til å merke sikkergradert informasjon gjelder der informasjonen er logisk avgrenset og fysisk lagret på et medium som det er mulig å merke. Der hvor lagringsmediet på grunn av sin fysiske utforming, f.eks. størrelse, gjør det vanskelig å merke, skal det allikevel kunne identifiseres ved at det er oppført i virksomhetens oversikt. Dette kan f.eks. gjelde små minnebrikker til kameraer, hvor størrelsen på lagringsmediet vanskeliggjør merking. Man kan da beskrive lagringsmediet i virksomhetens oversikt på en slik måte at det identifiseres som sikkerhetsgradert, eksempelvis slik: Minnebrikke tilhørende kamera type xx modellnr yy – gradert KONFIDENSIELT.

Der hvor det av plasshensyn er vanskelig å merke lagringsmedier med gradsnivå og lovhjemmel, kan det merkes med forkortelse, eks graderingens første bokstav, fortrinnsvis med rød farge slik: B, K, H.

Dersom informasjonen i et dokument består av deler med forskjellig beskyttelsesbehov, anbefales det at de enkelte deler graderes og merkes deretter, der dette er praktisk mulig. Delgradering kan benyttes i de tilfeller hvor forfatteren av et dokument sammenstiller informasjon fra ulike kilder og hvor informasjonen skal graderes ulikt. Informasjonen markeres da gjerne med sikkerhetsgradens forbokstav/er i parentesen foran en setning eller et avsnitt på denne måten:

(B) for BEGRENSET

(K) for KONFIDENSIELT

(H) for HEMMELIG

(SH) for STRENGT HEMMELIG

NSM har fra 24. november 2022 endret anbefalingen til hvordan hjemmelshenvisninger skal påføres ved merking av sikkerhetsgradert informasjon. Årsaken til at anbefalingen endres er et behov for en mer korrekt og presis angivelse av hjemmelsgrunnlaget.

NSM har forståelse for at det vil ta noe tid for virksomheter som tilvirker og behandler sikkerhetsgradert informasjon å oppdatere sine maler og merkinger slik at de er i tråd med de nye rådene. NSM ber likevel virksomhetene om å prioritere dette arbeidet slik at sikkerhetsgradert informasjon merkes likt på tvers av virksomheter, og i samsvar med gjeldende regelverk.

3 Soneinndeling og oppbevaring av dokumenter og lagringsmedier

3.1 Soneinndeling

Alle virksomheter som tilvirker sikkerhetsgradert informasjon eller som oppbevarer dokumenter eller lagringsmedier med sikkerhetsgradert informasjon gradert KONFIDENSIELT eller høyere plikter å dele inn sine lokaler i fysiske soner. Hensikten med de ulike sonene er at de gradvis skal gi bedre sikkerhet for informasjonen som skal beskyttes, og således fungere som flere lag med beskyttelse. Sonene defineres som *kontrollert*, *beskyttet* og *sperret* – hvorav *kontrollert* er det minst vitale og *sperret* mest sensitivt.

Virksomhetsikkerhetsforskriften § 38

Soneinndeling for informasjon gradert KONFIDENSIELT eller høyere Virksomheter som har informasjon som er gradert KONFIDENSIELT eller høyere, skal etablere en kontrollert og beskyttet sone for å beskytte den sikkerhetsgraderte informasjonen. Dersom virksomheten har et område med direkte tilgang til informasjon gradert KONFIDENSIELT eller høyere, skal det etableres en sperret sone rundt området.

Virksomhetsikkerhetsforskriften §39 Kontrollert sone

En kontrollert sone skal være et tydelig avgrenset område der virksomheten skal kunne ha kontroll med personer, kjøretøy og annen aktivitet. Ved særlig høy risiko skal adgang og ferdsel kontrolleres med en fysisk avgrensning.

Virksomhetsikkerhetsforskriften § 40 Beskyttet sone
En beskyttet sone skal ha en fysisk avgrensing der sikkerhetstruende virksomhet skal kunne oppdages.

I en beskyttet sone skal dokumenter og lagringsmedier med informasjon som er gradert KONFIDENSIELT eller høyere, lagres i en oppbevaringsenhet godkjent av Nasjonal sikkerhetsmyndighet, eller være under stedlig vakthold.

Personer som skal gis permanent adgang til en beskyttet sone, skal være sikkerhetsklarert for KONFIDENSIELT. Dersom andre personer skal gis adgang, skal adgangen registreres, og personene skal følges av personer med permanent adgang.

Det skal være kontroll med adgangen til en beskyttet sone, og det skal være synlig hvem som har permanent adgang dit.

Virksomhetsikkerhetsforskriften § 41 Sperret sone

En sperret sone skal være tydelig merket med det høyeste tillatte graderingsnivået og sikres i samsvar med dette graderingsnivået.

Personer som skal gis permanent adgang til en sperret sone, skal være sikkerhetsklarert og autorisert for informasjonen i området. Dersom andre personer skal gis adgang, skal adgangen registreres, og personene følges av personell som har permanent adgang.

Det skal være kontroll med adgangen til en sperret sone, og det skal være synlig hvem som har permanent adgang til sonen.

Utforming av de ulike sonene må sees i sammenheng med de prinsipper som ligger til grunn for valg og utforming av sikkerhetstiltak etter virksomhetsikkerhetsforskriften § 15, se særlig paragrafens første ledd bokstav a-e.

Virksomhetsikkerhetsforskriften § 15 Prinsipper ved valg og utforming av sikkerhetstiltak

Første ledd bokstav a-e:

Sikkerhetstiltakene skal ikke ha en annen funksjonalitet eller større kompleksitet enn nødvendig.

Det skal ikke gis en mer omfattende tilgang til skjermingsverdige verdier enn nødvendig.

Svikt i ett enkelt tiltak skal ikke kunne føre til kompromittering av skjermingsverdige verdier.

Sikkerhetstiltak skal i minst mulig grad være avhengig av hverandre, og flere sikkerhetstiltak skal dermed ikke kunne svekkes eller settes ut av funksjon samtidig, for eksempel som følge av én enkelt feil eller hendelse.

Effekten av sikkerhetstiltakene skal være tilnærmet lik for alle skjermingsverdige verdier med samme sikkerhetsbehov.

NSM legger ellers det følgende til grunn som retningslinjer for de ulike sonene:

Sperret sone forstås som sone der adgang gir direkte tilgang til sikkerhetsgradert informasjon gradert KONFIDENSIELT eller høyere. Typiske sperrede soner vil være arkiver og dokumenthvelv, operasjonsrom, kommunikasjons- og serverrom eller lokaler der det lages sikkerhetsgraderte produkter. Dette er altså spesialrom hvor sikkerhetsgradert informasjon er åpent eller lett tilgjengelig for den som har adgang. Felles for disse rommene er at det personellet som gis adgang skal være autorisert for den informasjonen og det utstyret som er i rommet. For at beskyttelsen skal være reell må det være en form for fysisk barriere inn til sperret sone, som faktisk forhindrer innsyn og direkte tilgang til gradert informasjon.

Hvem som har adgang i sperret sone må være synlig for de som har en kontrollfunksjon virksomheten. Ved bortfall av en persons behov for tilgang til sperret sone må virksomheten ha rutiner som forhindrer fortsatt faktisk tilgang – elektroniske tilganger må fjernes, nøkler inndras, relevante passord/koder endres og navn fjernes fra tilgangsliste.

Beskyttet sone forstås som sone hvor det behandles sikkerhetsgradert informasjon gradert KONFIDENSIELT eller høyere og/eller oppbevares dokumenter og lagringsmedier med slik sikkerhetsgradert informasjon, og/eller det oppbevares sikkerhetsgraderte informasjonssystemer godkjent for gradsnivå KONFIDENSIELT eller høyere. De som gis permanent adgang (har egen nøkkel / adgangskort og kan ferdes fritt alene) skal ha gyldig sikkerhetsklarering.

Kontrollert sone forstås som en sone som omgir beskyttet eller sperret område. En kontrollert sone fungerer som en buffersone mellom beskyttet eller sperret område på den ene siden, og et område med allmenn ferdsel på den andre. En kontrollert sone vil kunne fungere som et ytre lag med beskyttelse mellom beskyttet sone på den ene side og et område med allmenn ferdsel på den andre, men en kontrollert sone vil også kunne være en sone som benyttes til å behandle sikkerhetsgradert informasjon BEGRENSET, forutsatt at informasjonen beskyttes i henhold til kravene om forsvarlig sikkerhetsnivå, jf kapittel 4 under.

3.2 Oppbevaring

Med oppbevaring forstås her fysisk lagring av et dokument eller et lagringsmedium. Avhengig av størrelse, kan slik oppbevaring utføres på ulike lokasjoner, herunder i tilknytning til personlig varetekt i forbindelse med transport. Ved avhending av dokumenter og lagringsmedier fra personlig varetekt til fysisk plassering i rom og/eller enhet for lagring, med hensikt om å kunne gjenoppta personlig varetekt senere, kommer prinsippet om soneinndeling til anvendelse. Dess høyere gradert informasjon dokumentet eller lagringsmediet som skal oppbevares inneholder, dess

strengere krav til beskyttelse av det fysiske rommet for oppbevaring følger. Hensikten med soneinndeling ble omtalt over. I tråd med denne hensikten om lagdelt sikring for å oppnå forsvarlig sikkerhetsnivå etter forskriftens §§ 22 og 34, anbefaler NSM at:

- Dokument eller lagringsmedium inneholdende informasjon sikkerhetsgradert BEGRENSET oppbevares i avlåst rom eller nedlåst i oppbevaringsenhet VEILEDER I HÅNDTERING OG BESKYTTELSE AV SIKKERHETSGRADERT INFORMASJON NASJONAL SIKKERHETSMYNDIGHET | 10

- Dokument eller lagringsmedium inneholdende informasjon sikkerhetsgradert KONFIDENSIELT oppbevares i sperret sone sikret for å oppnå forsvarlig sikkerhet for dette gradsnivået eller i oppbevaringsenhet evaluert etter § 16, plassert innenfor beskyttet sone.

- Dokument eller lagringsmedium inneholdende informasjon sikkerhetsgradert HEMMELIG oppbevares i sperret sone sikret for å oppnå forsvarlig sikkerhet for dette gradsnivået eller i oppbevaringsenhet evaluert etter § 16, plassert innenfor beskyttet sone.

- Dokument eller lagringsmedium inneholdende informasjon sikkerhetsgradert STRENGT HEMMELIG oppbevares i sperret sone sikret for å oppnå forsvarlig sikkerhet for dette gradsnivået eller i oppbevaringsenhet evaluert etter § 16, plassert innenfor beskyttet sone. For ytterligere og mer detaljert veiledning om fysiske soner og oppbevaring, herunder anbefalinger til dører, vegger, låser, vinduer og konkrete oppb

Det er laget en egen **veileder for kriterier for godkjenning av oppbevaringsenheter.** ***(PDF, 830KB)***

4 Behandling av dokumenter og lagringsmedier med sikkerhetsgradert informasjon

4.1 Behandling av BEGRENSET

Kravet til forsvarlig sikkerhetsnivå ved behandling av informasjon sikkerhetsgradert BEGRENSET er regulert av sikkerhetsloven § 5-2 og virksomhetsikkerhetsforskriften § 22. For nærmere veiledning om hva som ligger til grunn for forståelsen av forsvarlig sikkerhetsnivå, se NSMs veileder i sikkerhetsstyring kapittel 2 om risikostyring.

Når virksomheten håndterer risiko knyttet til informasjon gradert BEGRENSET, er kravet til et forsvarlig sikkerhetsnivå oppfylt dersom informasjonen ikke med enkle midler kan bli kjent for uautoriserte personer. Dette muliggjør at virksomheten på visse betingelser kan tillate behandling av BEGRENSET informasjon utenfor områder virksomheten kontrollerer, f.eks. hjemmekontor. Informasjonen må hele tiden beskyttes på en slik måte at den ikke blir gjort tilgjengelig for uautorisert personell. Under vises tre tenkte eksempler på hva som ikke vil være å anse som tilstrekkelig beskyttelse av sikkerhetsgradert informasjon.

Eksempel A

Situasjon: En sikkerhetsklarert ansatt i en virksomhet omfattet av sikkerhetsloven medbringer et dokument med innhold sikkerhetsgradert BEGRENSET.

Scenario: Den ansatte leser dokumentet på offentlig transportmiddel.

Vurdering: Øvrige passasjerer (uautorisert personell) vil relativt enkelt kunne stille seg bak eller ved siden av den ansatte som leser dokumentet, og således forsettlig, selv med liten kapasitet kunne tilegne seg informasjonen i dokumentet. Dette er å anse som «med enkle midler». Beskyttelsen ikke tilstrekkelig. *Sikkerhetsnivået er ikke forsvarlig*.

Eksempel B

Situasjon: En sikkerhetsklarert ansatt i en virksomhet omfattet av sikkerhetsloven medbringer et dokument med innhold sikkerhetsgradert BEGRENSET. Dokumentet er forskriftsmessig emballert.

Scenario: Den ansatte har plassert brevpakken med dokumentet på nabosetet i togkupéen, og holder ikke øye med denne.

Vurdering: Øvrige passasjerer (uautorisert personell) vil da uten store vanskeligheter i et ubevoktet øyeblikk kunne gripe og ta med seg pakken (forsettlig, selv med liten kapasitet), dersom den ansatte ikke er tilstrekkelig påpasselig. Manglende reell kontroll muliggjør et handlingsrom for at en uautorisert person «med enkle midler» kan tilegne seg pakken, og med det kunne få tilgang til informasjonen. Beskyttelsen kan ikke ansees som tilstrekkelig. *Sikkerhetsnivået er ikke forsvarlig*.

Eksempel C

Situasjon: En sikkerhetsklarert ansatt i en virksomhet omfattet av sikkerhetsloven medbringer et fysisk lite lagringsmedium (minnepinne) inneholdende informasjon sikkerhetsgradert BEGRENSET, tenkt til bruk i et møte. Lagringsmediet er ikke passordbeskyttet.

Scenario: Den ansatte mister kontroll over lagringsmediet, og kan ikke gjøre rede for hvordan det har blitt borte eller hvor det kan ha blitt av.

Vurdering: Et fysisk lite lagringsmedium som en minnepinne vil meget enkelt og umerkelig kunne komme på avveie om man ikke er tilstrekkelig årvåken, og vil da kunne være vanskelig å gjenfinne. Det vil da være utfordrende å forhindre at «uautorisert personell ikke med enkle midler», vil kunne tilegne seg lagringsmediet og dermed også informasjonen dette inneholder, med mindre lagringsmediet er godt beskyttet gjennom elektroniske barrierer. Beskyttelsen i dette eksempelet kan ikke anses som tilstrekkelig. *Sikkerhetsnivået er ikke forsvarlig.*

4.2 Behandling av KONFIDENSIELT og høyere

Kravet til forsvarlig sikkerhetsnivå ved behandling av informasjon sikkerhetsgradert KONFIDENSIELT og høyere er regulert av sikkerhetsloven § 5-2 og virksomhetsikkerhetsforskriften § 34. For veiledning om forsvarlig sikkerhetsnivå, se NSMs veileder i sikkerhetsstyring kapittel 2 om risikostyring.

I utgangspunktet skal informasjon sikkerhetsgradert KONFIDENSIELT eller høyere bare behandles i beskyttet eller sperret sone. Virksomhetsikkerhetsforskriften § 42 andre til fjerde ledd åpner imidlertid for unntak fra dette.

Virksomhetsikkerhetsforskriften § 42 Behandling av informasjon gradert KONFIDENSIELT eller høyere

Dokumenter eller lagringsmedier med informasjon som er gradert KONFIDENSIELT eller høyere, skal bare oppbevares og behandles i beskyttet eller sperret sone.

Slike dokumenter eller lagringsmedier kan likevel oppbevares og behandles utenfor

beskyttet eller sperret område når dette er godkjent av virksomheten på bakgrunn av en vurdering av risiko. Virksomheten skal holde en oversikt over slike godkjenninger.

Dersom sikkerhetsgradert informasjon behandles eller oppbevares utenfor en beskyttet eller sperret sone, skal virksomheten gjennomføre nødvendige tiltak for å beskytte informasjonen, slik at den ikke blir kjent for uautoriserte personer, går tapt, blir endret eller gjort utilgjengelig.

Dokumenter eller lagringsmedier med informasjon gradert KONFIDENSIELT kan tas med til et NATOland eller en stat Norge har en sikkerhetsavtale med, dersom en person som er klarert for innholdet, tar vare på informasjonen gjennom hele reisen, og det er mulig å deponere informasjonen ved en norsk utenriksstasjon eller et annet norskkontrollert område ved ankomst. Informasjon gradert HEMMELIG eller STRENGT HEMMELIG må sendes med en kurér, jf. § 45.

Bestemmelsens andre ledd må forstås slik at en virksomhets personell kan medbringe dokumenter og lagringsmedier med sikkerhetsgradert innhold ut fra beskyttet sone, f. eks for å jobbe med dette utenfor ordinært arbeidssted eller bringe dette til og fra møter, så lenge tilstrekkelig beskyttelse ivaretas på bakgrunn av en risikovurdering hos virksomheten. En virksomhet kan gi en generell tillatelse til dette forutsatt at virksomheten vurderer hvilken risiko dette innebærer og implementerer tilstrekkelig med risikoreduserende tiltak.

Begrepet «medbringe» forstås i utgangspunktet dithen at den som medbringer er autorisert for innholdet, og at informasjonen som medbringes er til eget bruk, og at formatet denne er lagret på (dokument eller lagringsmedium) skal returneres til virksomheten, eventuelt destrueres i henhold til gjeldende bestemmelser for dette, jf virksomhetsikkerhet § 23, omtalt nærmere i kapittel 8 under.

§ 42 har et unntak fra reglene om kurérforsendelse i det typetilfellet som omhandler at «[d]okumenter eller lagringsmedier med informasjon gradert KONFIDENSIELT kan tas med til et NATO-land eller en stat Norge har en sikkerhetsavtale med». Nærmere vilkår fremgår i paragrafen. Formålet med reglene om behandling av sikkerhetsgradert informasjon – å sikre forsvarlig sikkerhetsnivå – tilsier at regler og rutiner for kurérforsendelse bør følges så langt det er mulig også ved slik medbringelse etter unntaksregelen i virksomhetsikkerhetsforskriften § 42.

I tilfeller der en person som frakter dokumenter eller lagringsmedier med informasjon sikkerhetsgradert KONFIDENSIELT eller høyere, ikke er autorisert for innholdet, eller ikke vil ha en reell mulighet til å ha dokumentet eller lagringsmediet i personlig varetekt gjennom hele reisen, eller der hvor det er usikkerhet knyttet til reiseveien og reisemåten, skal som hovedregel bestemmelsene om kurér benyttes.

5 Forsendelse – med og uten bruk av kurér

5.1 Elektronisk overføring og fysisk forsendelse

NSM vil anbefale virksomhetene å velge sikker elektronisk overføring fremfor fysisk forsendelse der dette er mulig, ved å ta i bruk sikkerhetsgodkjente elektroniske løsninger for sikker overføring av informasjon. Dette vil gi bedre sikkerhet og være mer effektivt, da store mengder informasjon kan overføres raskt og på en bedre beskyttet måte enn fysisk beskyttelse og forflytning av informasjonen.

Virksomhetsikkerhetsforskriften § 35 Sending av informasjon gradert KONFIDENSIELT eller høyere

Når informasjon som er gradert KONFIDENSIELT eller høyere, skal sendes fysisk, skal det brukes en kurér. Dersom informasjonen er gradert HEMMELIG eller STRENGT HEMMELIG, skal i tillegg mottakeren kvittere for at sendingen er mottatt.

Dersom informasjon med ulik sikkerhetsgradering sendes sammen, skal det ligge ved en liste med oversikt over informasjonen og sikkerhetsgradene.

Virksomhetsikkerhetsforskriften § 45 Krav til forsendelse med kurér

Virksomheter som utfører kurérposttjeneste, skal sikre at informasjonen ikke blir kjent for uautoriserte personer. Avsenderen skal utstede et kurérsertifikat for hvert oppdrag og legge en plan for gjennomføringen av oppdraget. Kuréren skal være sikkerhetsklarert for sikkerhetsgraden på den informasjonen som fraktes.

Med mindre Nasjonal sikkerhetsmyndighet gir tillatelse til noe annet, skal kurérpost til utlandet sendes som diplomatisk post, eller med en kurér fra Forsvaret eller utenrikstjenesten.

Virksomhetsikkerhetsforskriften § 43 Særlige krav for informasjon gradert HEMMELIG eller høyere

Når dokumenter eller lagringsmedier gradert HEMMELIG eller høyere skal fordeles internt i en virksomhet, skal mottakeren bekrefte mottaket.

Destruering av informasjon gradert HEMMELIG eller høyere skal kontrolleres og bekreftes av minst to autoriserte personer.

Ved overlevering av dokumenter eller lagringsmedier med informasjon sikkerhetsgradert HEMMELIG eller høyere skal mottaker bekrefte mottaket overfor avsender. Bekreftelsen bør være elektronisk, eksempelvis via e-post fra personlig bruker på sikkerhetsgodkjent informasjonssystem.

5.2 Kurértransport

Fysisk forsendelse av dokumenter og lagringsmedier med informasjon gradert KONFIDENSIELT og høyere må utføres med bruk av kurér. For transportering av kryptomateriell, se egen forskrift om kryptosikkerhet.

De nye kravene til forsendelsesmetode i § 35 er en innstramming sammenlignet med tidligere regelverk. En viktig praktisk endring i det nye regelverket er at det ikke lenger er tillatt å sende informasjon gradert HEMMELIG eller KONFIDENSIELT som registrert post. Bakgrunnen for innstrammingen er opphevelsen av det statlige postmonopolet.

Postforsendelse av informasjon gradert BEGRENSET er ikke eksplisitt regulert. Nasjonal sikkerhetsmyndighets anser at postforsendelse av informasjon gradert BEGRENSET vil kunne oppfylle kravet til forsvarlig sikkerhetsnivå. Sikkerhetsnivået kan oppnås ved at forsendelsen er anonym, som et umerket brev/pakke blant et stort antall andre pakker og brev vil være.

Kravet i forskrift om virksomheters arbeid med forebyggende sikkerhet § 45 første ledd om at «virksomheter som utfører kurérposttjeneste skal sikre at informasjonen ikke blir kjent for uautoriserte personer», må forstås som et krav om å sikre informasjonens konfidensialitet og integritet, herunder under transport. Dette er kurérens hovedfunksjon. Lov og forskrift stiller derfor enkelte krav til kuréren og gjennomføring av kurértransporten.

Virksomheter som fysisk skal sende dokumenter og lagringsmedier med informasjon gradert KONFIDENSIELT og høyere, bør kjenne til også andre regelverk som gjelder for forsendelsen, særlig ved kurérforsendelse utenlands. Å kjenne reglene er avsenderens ansvar. Nasjonal sikkerhetsmyndighet eller en etablert kurértjeneste kan gi nærmere råd.

5.2.1 Kurérsertifikat

Kuréren må ha tilstrekkelig kompetanse om sikkerhet, jf forskrift om virksomheters arbeid med forebyggende sikkerhet § 7, sikkerhetsklarering for riktig nivå og kurérsertifikat utstedt av den relevante virksomheten.

Kravet om kurérsertifikat er funksjonelt. Eksempelvis vil gyldig id-kort sammen med oppdragsbekreftelse fra virksomheten kunne tilfredsstille kravet. Et kurérsertifikat vil imidlertid som hovedregel ikke gi en sikkerhetsmessig beskyttelse av forsendelsens innhold, men kan ha en legitimerende effekt som kan forhindre forsendelsen fra å bli åpnet, eventuelt forhindret i å bli åpnet i offentlig rom med mulig eksponering av innhold for publikum. Avsender kan vurdere om forsendelsen bør påføres merking som uttrykker at forsendelsen kun skal åpnes av autorisert personell.

Gjennomlysning i sikkerhetskontroll må dog påregnes, se ellers forskrift om forebyggelse av anslag mot sikkerheten i luftfarten § 23 om alternativ sikkerhetskontroll.

Under reisen må kuréren ha kontroll på dokumentet eller lagringsmediet. Kuréren skal sikre at forsendelsen ikke blir gjort tilgjengelig for uvedkommende, slik at informasjonen i den ikke kompromitteres, dvs ikke kan bli endret eller gjort tilgjengelig for uvedkommende.

For mal kurérsertifikat, se vedlegg 1. Virksomheten kan velge å utstede kurérsertifikat med annen utforming og ytterligere innhold.

5.2.2 Transportplan

Planen for gjennomføringen av oppdraget (§ 45) – transportplanen – bør gi virksomheten oversikt over hvor forsendelsen befinner seg, jf virksomhetsikkerhetsforskriften § 37, og hva som skal gjøres dersom denne kommer på avveie. Virksomheten og kuréren må ha reell kontroll, slik at beskyttelsen av informasjonen ivaretas. Kuréren må kjenne transportplanen for oppdraget og eventuelle særlige forhold ved forsendelsen.

NSM anbefaler at en vurdering av ulike transportmidler og reiseruter ligger til grunn for transportplanen. Reiser med visse transportmidler innebærer at den reisende må passere gjennom sikkerhetskontroll. Virksomheten må foreta en vurdering av dette forholdet opp mot kravet om ivaretagelse av forsvarlig sikkerhetsnivå etter sikkerhetsloven og eventuelt velge alternativ transport eller elektronisk overføring av informasjonen, i den utstrekning det er mulig.

Virksomheten kan gjenbruke planer for gjennomføring av oppdrag ved regelmessig transport mellom lokasjoner.

Mal for mulig skriftlig nedtegnet transportplan, se vedlegg 2.

5.2.3 Kvittering for mottak

Virksomhetsikkerhetsforskriften § 35 første ledd annet punktum setter krav til kvittering for mottatt forsendelse, dersom informasjonen er gradert HEMMELIG eller STRENGT HEMMELIG. Bestemmelsen kan med fordel også følges for forsendelse av lavere gradert informasjon. Kvittering for mottak tydeliggjør ansvarsforholdet ved forsendelsen. Kvittering for mottak bør ha en viss umiddelbarhet i forbindelse med overleveringstidspunktet. Kvittering kan gjøres ugradert, så fremt innholdet i denne kan holdes på et ugradert nivå, herunder referanse til aktuell forsendelse.

Kvittering bør også innbefatte at forsendelsens integritet er intakt ved mottak. Det vil si at den som kvitterer går god for å ha mottatt forsendelsen uten synlige tegn til at

denne kan ha vært åpnet eller på annen måte håndtert på et vis som kan så tvil om innholdet av forsendelsen kan ha blitt endret under frakten fra avsender til mottager.

5.2.4 Hvem kan være kurér – innenlands

- Virksomheten selv
- Andre virksomheter omfattet av sikkerhetsloven
- Eksterne fraktselskaper – dette må da gjøres i samsvar med bestemmelsene om sikkerhetsgraderte anskaffelser. Private foretak som utfører kurértjeneste vil da bli å regne som en leverandør av en tjeneste. Denne tjenesten vil måtte foregå innenfor rammene av en sikkerhetsgradert anskaffelse, jf Lov om nasjonal sikkerhet kapittel 9 og klareringsforskriften

5.2.5 Hvem kan være kurér – utenlands

- Forsvaret og Utenriksdepartementets kurértjeneste
- Andre virksomheter etter tillatelse fra NSM.

6 Krav til oversikt over dokumenter og lagringsmedier

Virksomhetsikkerhetsforskriften § 37 Krav til oversikt over informasjon gradert KONFIDENSIELT eller høyere

En virksomhet skal ha en oversikt over hvor dens egne dokumenter og lagringsmedier med informasjon som er gradert KONFIDENSIELT eller høyere, til enhver tid befinner seg. I tillegg skal virksomheten ha en oversikt over hvilke dokumenter og lagringsmedier med informasjon som er gradert KONFIDENSIELT eller høyere, som er mottatt fra eller sendt til andre virksomheter.

Virksomheten skal ha en oversikt over hvor dokumenter og lagringsmedier med innhold sikkerhetsgradert KONFIDENSIELT eller høyere, til enhver tid befinner seg. Oversikt over sikkerhetsgraderte dokumenter og lagringsmedier skal inneholde tilstrekkelig informasjon til å identifisere og gjenfinne informasjonen. Dette betyr at dokumenter og lagringsmediers fysiske plassering skal nedtegnes, og all inn- og utgående trafikk av graderte dokumenter og lagringsmedier fra virksomheten skal dokumenteres.

I tillegg til opplysninger om dokumentets avsender, mottaker og innhold, bør også opplysning om gradsnivå inngå i oversikten. For informasjon sikkerhetsgradert HEMMELIG og høyere bør i tillegg antall sider og eksemplarnummer inngå i oversikten der dette er praktisk mulig å oppføre.

For informasjon gradert HEMMELIG og høyere anbefaler NSM at virksomheten paginerer og eksemplarnummererer dokumentene der dette er praktisk mulig, for med dette å oppnå høyere kvalitet på virksomhetens oversikt – dette for å sikre reelt samsvar mellom oversikten og hva oversikten viser til. Informasjonen skal være korrekt, fullstendig og tilgjengelig.

For elektroniske lagringsmedier skal oversikten inneholde opplysninger om lagringsmediet, samt om hvilke dokumenter som er lagret på det.

Krav til oversikt må sees i sammenheng med eventuell mangfoldiggjøring og spredning av sikkerhetsgradert informasjon. Virksomheten må ha rutiner som sikrer nødvendig kontroll på kopier og utskrifter av gradert informasjon gradert KONFIDENSIELT eller høyere. Antall kopier og utskrifter bør ikke være større enn at det er mulig å holde en reell oversikt over disse. NSM anbefaler at virksomheten tilintetgjør kopier og utskrifter når behovet for disse opphører.

Bestemmelsen i Forskrift om virksomheters arbeid med forebyggende sikkerhet § 37 gjelder i tillegg til bestemmelser om journalføringsplikt i forskrift om offentlige arkiv.

7 Destruksjon av dokument eller lagringsmedium

Virksomhetsikkerhetsforskriften § 23 Destruering av dokumenter og lagringsmedier med sikkerhetsgradert informasjon

Ved destruering av dokumenter og lagringsmedier som inneholder eller har inneholdt sikkerhetsgradert informasjon, skal det brukes en metode som gjør at det ikke er mulig å rekonstruere og lese informasjonen.

Dersom informasjonen er eller har vært gradert KONFIDENSIELT eller høyere, skal det benyttes et produkt som er evaluert etter § 16, til å destruere dokumentet eller lagringsmediet.

Virksomhet som skal destruere dokument eller lagringsmedium inneholdende sikkerhetsgradert informasjon må benytte en fremgangsmåte som utelukker mulighet for rekonstruksjon, og dermed forhindrer gjenoppretting av tilgang til informasjonen. Det er selve informasjonen som skal beskyttes, og dette skal så langt det er mulig, utføres med samme grad av sikkerhet uavhengig av hvilket format informasjonen er lagret på.

I utgangspunktet vil enhver metode som målbærer hensikten om å forhindre rekonstruksjon, for med det å forhindre gjenoppretting for tilgang til informasjonen, kunne benyttes. Produktet som benyttes for slik destruksjon skal imidlertid være evaluert av NSM eller akkreditert laboratorium utpekt av NSM, alternativt sertifisert i andre land der disse er godkjent av NSM. Mulige metoder for destruksjon kan for eksempel være forbrenning eller annen kjemisk prosessering, krysskutting, avmagnetisering, sliping og knusing.

NSM jobber fortløpende med å utarbeide kriterier for evaluering av produkter til bruk for destruksjon som nevnt over. Det må her sees hen til overgangsreglene i § 95 for korrekt prosedyre. Det vises ellers til NATOs regelverk og NATOs krav for destruksjon av dokumenter og lagringsmedier med gradert innhold, se https://www.ia.nato.int/NIAPC.

Virksomhetsikkerhetsforskriften § 95 Overgangsregler

Destrueringsmetoder og oppbevaringsenheter som er godkjent etter forskrift 1. juli 2001 nr. 744 om informasjonssikkerhet § 4-36, § 6-11 og § 6-12, skal anses godkjent inntil godkjenningen opphører, eller det av andre grunner er behov for ny godkjenning av destrueringsmetoden eller oppbevaringsenheten.

Et rom som er godkjent etter forskrift 1. juli 2001 nr. 744 om informasjonssikkerhet § 9-1, skal anses å oppfylle kravene i § 46.

En klage på klassifisering eller godkjenning etter første eller andre ledd skal avgjøres etter de reglene som gjelder når klageinstansen treffer vedtak i saken.

For enkelte lagringsmedier med informasjon opp til og med HEMMELIG, vil det ikke være nødvendig med fullstendig destruksjon av selve lagringsmediet, så fremt informasjonen kan slettes på en slik måte at den ikke kan rekonstrueres. Liste over NSM-godkjent sletteverktøy kommer på NSMs nettsider. Denne oppdateres løpende.

Notoritet med hensyn til destruksjon ivaretas ved å registrere slik destruksjon i oversikten der dokumentet eller lagringsmediet er registrert.

Virksomhetsikkerhetsforskriften § 43 Særlige krav for informasjon gradert HEMMELIG eller høyere

Når dokumenter eller lagringsmedier gradert HEMMELIG eller høyere skal fordeles internt i en virksomhet, skal mottakeren bekrefte mottaket.

Destruering av informasjon gradert HEMMELIG eller høyere skal kontrolleres og bekreftes av minst to autoriserte personer.

Uavhengig av hva slags produkt som benyttes for destruksjon, anbefaler NSM generelt at virksomhetene følger destruksjonsprosessen nøye, for å sikre at denne fullendes slik at hensikten oppnås – å forhindre mulig rekonstruksjon, og med det forhindre tilgang til informasjonen for uautorisert personell.

En virksomhet kan velge å benytte ekstern tjenesteleverandør til destruksjon. Dersom tjenesteleverandøren ikke er klarert og autorisert for innholdet i informasjonen, må personell fra virksomheten bevitne destruksjonen for å forhindre uautorisert tilgang til informasjonen. Alternativt kan kommersiell tilbyder utføre tjenesten som leverandør etter regelverket om sikkerhetsgraderte anskaffelser.

Virksomhetsikkerhetsforskriften § 24 Evakuering og ekstraordinær destruering i nødsituasjoner

En virksomhet skal for nødsituasjoner ha en evakueringsplan og en plan for destruering av dokumenter og lagringsmedier med skjermingsverdig informasjon.

Virksomheten skal, i forbindelse med arbeidet med evakueringsplan og plan for destruksjon av dokumenter og lagringsmedier, foreta en risikovurdering som vil være styrende for planarbeidet. For en virksomhet som er lokalisert i et område der det med stor sannsynlighet vil være behov for evakuering og destruksjon, vil utforming av planene og behov for øving ha en annen karakter enn for en virksomhet som er lokalisert i et område med lavere risiko. Det vil da kanskje ikke være relevant med planverk for evakuering, da dette ikke i alle settinger betraktes som aktuelt, men heller fokusere på destruksjon.

NSM anbefaler at en plan for evakuering som minimum bør inneholde:

- Oversikt over dokumenter og lagringsmedier og deres plassering
- Prioriteringsliste
- Hvem skal bidra i evakueringen
- Hvordan skal evakueringen foregå, herunder
    - pakking
    - frakt ut av lokasjon
    - alternativer ved strømbrudd
    - frakt fra bygning til bestemmelsessted
- Bestemmelsessted
    - hvor det skal evakueres til
    - alternative ruter
    - tilgjengelighet

NSM anbefaler at en plan for destruksjon som minimum bør inneholde:

- Oversikt over dokumenter og lagringsmedier og deres plassering
- Prioriteringsliste
- Destruksjonsmetode for papirdokumenter
- Destruksjonsmetode for lagringsmedier - alternativer ved fravær av elektrisitet, vannforsyning mm.

Planene må evalueres jevnlig. Behov og krav vil kunne endres ved endringer i risikobildet og samfunnsutviklingen generelt. Planene bør også være en del av ledelsens årlige evaluering. Planene må også øves for å sikre at evakuering og/eller destruksjon kan gjennomføres sikkert og effektivt. Virksomheten må se dette i sammenheng med sin øvrige sikkerhetsstyring.

8 Rapportering av informasjon gradert STRENGT HEMMELIG

Virksomhetsikkerhetsforskriften § 44 Rapportering av informasjon gradert STRENGT HEMMELIG

Virksomheter som har dokumenter eller lagringsmedier med informasjon gradert STRENGT HEMMELIG, skal hvert år kontrollere at dokumentene og lagringsmediene befinner seg i virksomheten. Kontrollen skal foretas på grunnlag av oversikten per 31. desember. Virksomheten skal innen utgangen av januar hvert år sende en oversikt over slike dokumenter og lagringsmedier til det departementet som er ansvarlig for det forebyggende sikkerhetsarbeidet innenfor sektoren. Departementet skal innen utløpet av februar hvert år sende Nasjonal sikkerhetsmyndighet en samlet oversikt over dokumenter og lagringsmedier med informasjon gradert STRENGT HEMMELIG innenfor sin sektor. Oversiktene skal graderes HEMMELIG.

Forsvarsdepartementet kan dispensere fra kravet i første ledd tredje punktum.

9 Utlevering av sikkerhetsgradert informasjon til fremmede stater og internasjonale organisasjoner (§§25-26)

Virksomhetsikkerhetsforskriften § 25 Utlevering av sikkerhetsgradert informasjon til fremmede stater og internasjonale organisasjoner

Fremmede stater og internasjonale organisasjoner kan bare gis tilgang til norsk sikkerhetsgradert informasjon dersom det
a) er i samsvar med nasjonale sikkerhetsinteresser
b) ikke er i strid med lovbestemt taushetsplikt og
c) foreligger en sikkerhetsavtale mellom Norge og den aktuelle staten eller internasjonale organisasjonen.

Når myndigheter eller virksomheter i andre stater eller internasjonale organisasjoner skal ha tilgang til sikkerhetsgradert informasjon, skal informasjonen behandles i samsvar med bestemmelsene i sikkerhetsavtalen som er inngått mellom Norge og den aktuelle staten eller organisasjonen.

Dersom det ikke er praktisk mulig å inngå en sikkerhetsavtale, men det likevel er i Norges interesse å utlevere informasjonen, kan Forsvarsdepartementet og Justis- og beredskapsdepartementet gjøre unntak fra kravet til sikkerhetsavtale innenfor sine fagsektorer.

Virksomhetsikkerhetsforskriften § 26 Tilsvarende sikkerhetsgrader

Informasjon som er sikkerhetsgradert av en fremmed stat eller internasjonal organisasjon, skal beskyttes på samme måte som informasjon gradert med en tilsvarende norsk sikkerhetsgrad etter sikkerhetsloven § 5-3.

Nasjonal sikkerhetsmyndighet fastsetter hvilke sikkerhetsgrader fastsatt av fremmede stater eller internasjonale organisasjoner som tilsvarer de norske sikkerhetsgradene etter sikkerhetsloven § 5-3.

Fremmede stater og internasjonale organisasjoner kan bare gis tilgang til norsk sikkerhetsgradert informasjon dersom det er i samsvar med norske interesser og ikke er i strid med taushetsplikt. For at slik tilgang skal gis er det en forutsetning at det foreligger en sikkerhetsavtale med den aktuelle stat eller organisasjon om utveksling av informasjonen og sikkerhetsmessige forhold. Sikkerhetsavtaler mellom samarbeidende stater og internasjonale organisasjoner forplikter partene til gjensidig beskyttelse av hverandres graderte informasjon.

Fremmed stat som gis tilgang til norsk gradert informasjon er således forpliktet til å beskytte denne som om det var sin egen – og Norge er forpliktet til å beskytte andre staters og internasjonale organisasjoners graderte informasjon på samme måte som vi beskytter vår egen graderte informasjon, så fremt Norge har undertegnet en statlig

bilateral sikkerhetsavtale med de aktuelle statene og/eller internasjonale organisasjonene. De bilaterale sikkerhetsavtalene vil spesifisere ekvivalenter i de ulike staters og organisasjoners graderingssystemer, som sikrer at informasjonen skal bli korrekt beskyttet.

Dersom det ikke foreligger en bilateral sikkerhetsavtale mellom en fremmed stat og Norge kan det som hovedregel ikke utleveres norsk sikkerhetsgradert informasjon til representanter fra den aktuelle fremmede staten. Unntaksvis vil det kunne forekomme i forbindelse med operativ aktivitet, som i internasjonale operasjoner.

For NATO er C-M49(2002) den overordnede sikkerhetsavtalen mellom alle NATOs medlemsland. Denne avtalen innebærer en gjensidig forpliktelse til å beskytte sikkerhetsgradert informasjon utstedt av andre parter eller av NATO som organisasjon. Avtalen innebærer også at slik informasjon ikke skal frigis til andre parter enn dem omfattet av avtalen, uten utsteders forhåndsgodkjenning. Dette kalles prinsippet om Utsteders kontroll, eller principle of originators control/consent, og er et generelt prinsipp for behandling av sikkerhetsgradert informasjon. Prinsippet gjelder også ved frigivelse av norsk sikkerhetsgradert informasjon; informasjon som er sikkerhetsgradert av andre skal ikke frigis uten samtykke fra utstedende virksomhet. Dette betyr for eksempel at Forsvaret ikke vil kunne frigi til NATO norsk informasjon som er utstedt av en annen virksomhet enn Forsvaret (et forvaltningsorgan eller rettssubjekt).

Videre innebærer dette at en om en virksomhet benytter sikkerhetsgradert informasjon fra en annen virksomhet som grunnlag eller del av egne dokumenter, så må den andre virksomheten godkjenne at delmengden av informasjon som den har utstedt blir frigitt. En virksomhet står fritt til å frigi informasjon som er utstedt i egen organisasjon, uavhengig av nivå for utstedelse, såfremt dette er i samsvar med norske interesser og ikke er i strid med taushetsplikt. Ved beslutning om frigivelse påføres informasjonen gradering og merking i samsvar med inngått sikkerhetsavtale.

10 Referanser

Lovdata – https://lovdata.no

Lov om nasjonal sikkerhet (sikkerhetsloven) LOV-2018-06-01-24

Forskrift om virksomheters arbeid med forebyggende sikkerhet (virksomhetsikkerhetsforskriften) FOR2018-12-20-2053: Fastsatt ved kgl.res. 20. desember 2018 med hjemmel i lov 1. juni 2018 nr. 24 om nasjonal sikkerhet (sikkerhetsloven)

Høringsnotat – Forslag til forskrifter til ny sikkerhetslov. Forsvarsdepartementet. 2. juli 2018. Hentet fra https://www.regjeringen.no

NOU 2016: 19 Samhandling for sikkerhet – Beskyttelse av grunnleggende samfunnsfunksjoner i en omskiftelig tid. Hentet fra https://www.regjeringen.no

Prop 153L Forsvarsdepartementet (2017). Lov om nasjonal sikkerhet (sikkerhetsloven) Proposisjon 153 L (2016-2017). Hentet fra https://www.regjeringen.no

NATOs nettsider: https://www.ia.nato.int/niapc

NSMs øvrige veiledere:

- Sikkerhetsstyring
- Fysisk sikkerhet
- Sikkerhetsgodkjenning av informasjonssystemer
- Virksomheters håndtering av uønskede hendelser
- Tilsyn med forebyggende sikkerhetsarbeid
- Personellsikkerhet

11 Vedlegg

Vedlegg A - Mal kurérsertifikat *(PDF, 124KB)*

Vedlegg B - Mal transportplan *(PDF, 443KB)*