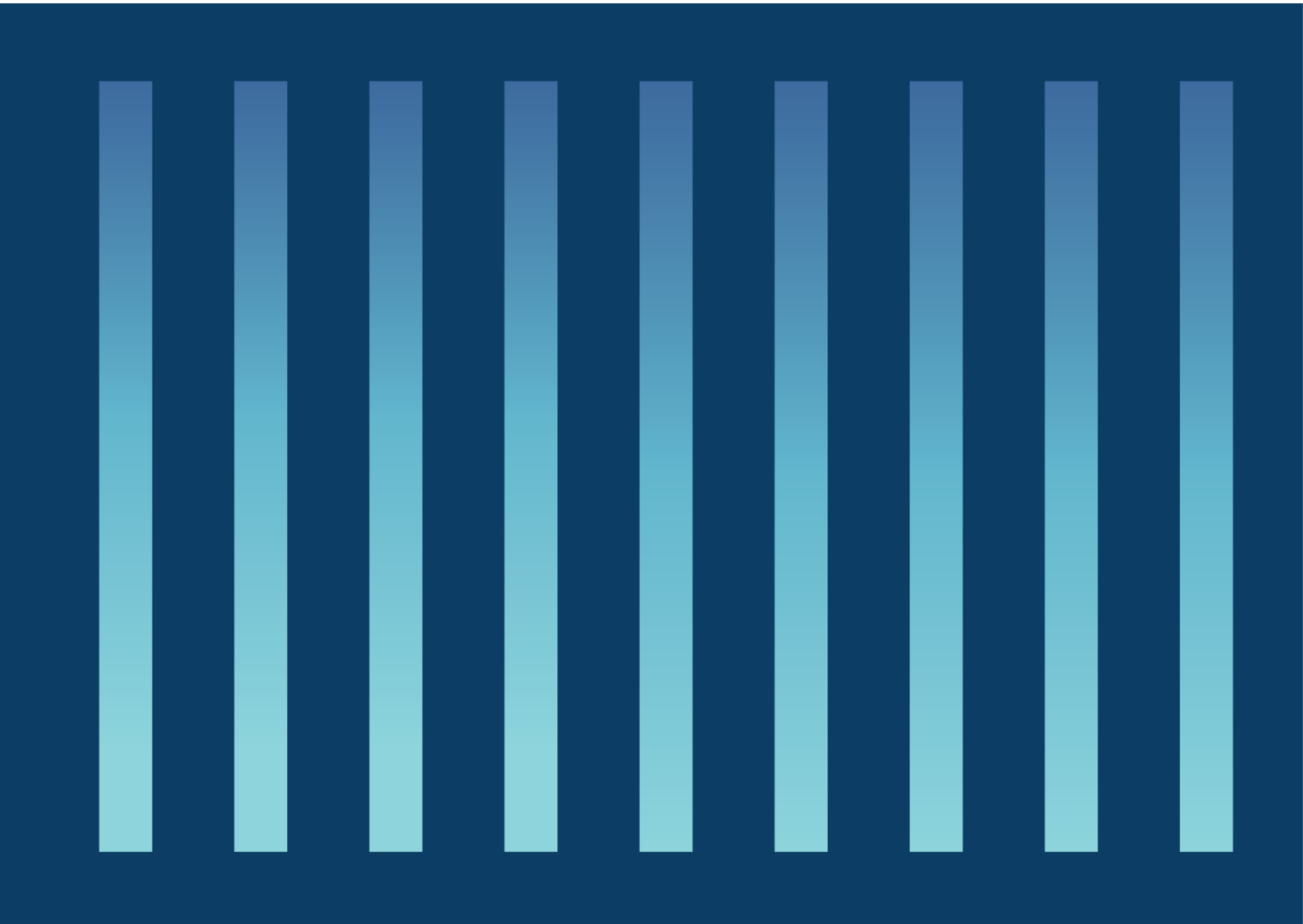
NASJONAL
SIKKERHETSMYNDIGHET

Veileder i verdivurdering av informasjon

Versjon: 1.1



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.

INNHOLD

1. Innledning

Dette dokumentet er en veileder i sikkerhetslovens og virksomhetssikkerhetsforskriftens bestemmelser om skjermingsverdig og sikkerhetsgradert informasjon. Informasjon er skjermingsverdig om informasjonens konfidensialitet, tilgjengelighet og/eller integritet må beskyttes av hensyn til nasjonale sikkerhetsinteresser. Sikkerhetsgradert informasjon er skjermingsverdig informasjon hvor konfidensialiteten må beskyttes av hensyn til nasjonale sikkerhetsinteresser. Ugradert skjermingsverdig informasjon er informasjon hvor tilgjengelighet og integritet må beskyttes av hensyn til nasjonale sikkerhetsinteresser.

Formålet med veilederen er å gi leseren en forståelse av hva skjermingsverdig og sikkerhetsgradert informasjon er, og en forståelse av forskjellene mellom nivåene av skadefølger knyttet til sikkerhetsgradert informasjon.

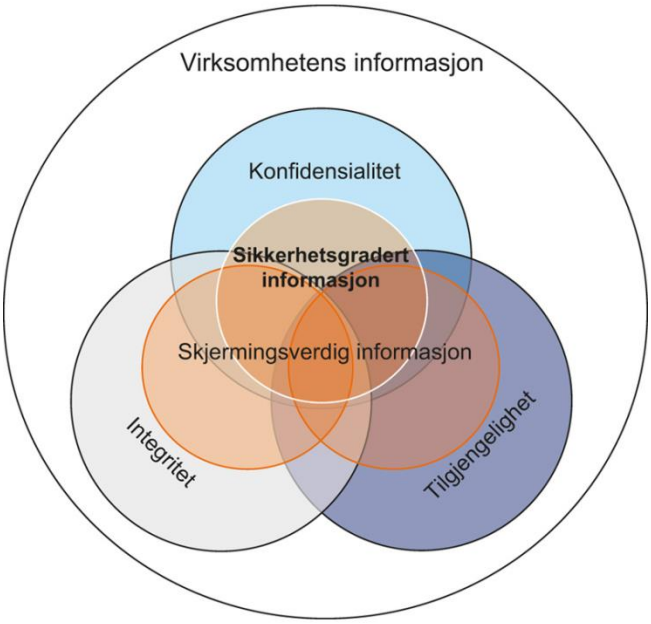
Nasjonal sikkerhetsmyndighet (NSM) vil på et senere tidspunkt utgi en håndbok som omhandler fremgangsmåte for verdivurdering av skjermingsverdig informasjon.

2. Skjermingsverdig informasjon

§ 5-1. Skjermingsverdig informasjon

Informasjon er skjermingsverdig dersom det kan skade nasjonale sikkerhetsinteresser at informasjonen blir kjent for uvedkommende, går tapt, blir endret eller blir utilgjengelig

Sikkerhetsloven og forskriftenes bruk av begrepet *informasjon* legger til grunn en vid forståelse av hva begrepet kan omfatte. Måten informasjon er tilvirket på og hvilken form informasjonen har er ikke relevante momenter i vurderingen av om noe er å betrakte som informasjon. Begrepet omfatter for eksempel opplysninger gitt i fysiske dokumenter, digitale og maskinlesbare signaler, film, lydopptak og muntlige opplysninger.



Figur 1: Illustrasjonen viser forholdet mellom skjermingsverdig og sikkerhetsgradert informasjon og hvilke sikkerhetsbehov virksomhetens informasjon kan ha. Kilde: Prop. 153 L Lov om nasjonal sikkerhet (sikkerhetsloven) s. 97

Begrepet skjermingsverdig informasjon er en samlebetegnelse som favner all informasjon som skal beskyttes etter loven, av hensyn til de skadefølger som kan påføres nasjonale sikkerhetsinteresser dersom informasjonen blir kjent for uvedkommende, går tapt, blir endret eller blir utilgjengelig. Hva som inngår i begrepet *nasjonale sikkerhetsinteresser* er beskrevet i NSMs veileder i departementenes identifisering av grunnleggende nasjonale funksjoner.

Dersom det kan få skadefølger for nasjonale sikkerhetsinteresser at informasjonen blir kjent for uvedkommende, så må informasjonens *konfidensialitet* beskyttes. Skjermingsverdig informasjon som må beskyttes av hensyn til *konfidensialitet* skal sikkerhetsgraderes. Med uvedkommende menes alle som ikke er sikkerhetsklarert og autorisert for informasjonen, og som ikke har et tjenstlig behov for å være kjent med informasjonen. Om uvedkommende blir kjent med informasjonen anses det som et *konfidensialitetsbrudd.*

Dersom det kan få skadefølger for nasjonale sikkerhetsinteresser at informasjonen går tapt eller blir utilgjengelig, så må informasjonens *tilgjengelighet* beskyttes. Med *tilgjengelighet* menes at informasjonen er tilgjengelig for virksomheten innenfor det tidsrommet som virksomheten har behov for å bruke den. Dersom slik informasjon går tapt, eller blir gjort utilgjengelig, anses det som et *tilgjengelighetsbrudd*. Virksomheten må vurdere tilgjengelighetsbehovene til informasjonen den besitter, og identifisere konsekvenser for nasjonale sikkerhetsinteresser dersom informasjonen ikke er tilgjengelig for de riktige brukerne eller systemene til rett tid.

Dersom det kan få skadefølger for nasjonale sikkerhetsinteresser at informasjonen blir endret, så må informasjonens *integritet* beskyttes. Med *integritet* menes at informasjonen er korrekt og fullstendig sett i sammenheng med emnet og omfanget som informasjonen har til hensikt å omfatte. Integritetsbeskyttelse innebærer å sørge for at det ikke lar seg gjøre urettmessig å endre innholdet i informasjonen.

Begrepet «ugradert skjermingsverdig informasjon» som benyttes i virksomhetssikkerhetsforskriften § 22 brukes om informasjon som er skjermingsverdig etter § 5-1, men som ikke har et skadepotensiale for nasjonale sikkerhetsinteresser om den blir kjent for uvedkommende. «Ugradert skjermingsverdig informasjon» skal beskyttes slik at integritet og tilgjengelighet sikres. Det kan tenkes at ugradert skjermingsverdig informasjon, hvis konfidensialitet ikke må beskyttes etter sikkerhetsloven, likevel har et konfidensialitetsbehov etter annet lovverk og må beskyttes deretter.

Konfidensialitet, integritet og tilgjengelighet er ikke motsetninger. Tilgjengelighet må ikke forveksles med prinsippet meroffentlighet, og er sågar ikke en motpol til konfidensialitet. I mange tilfeller vil en verdivurdering kunne vise at det er behov for å ivareta både konfidensialiteten, integriteten og tilgjengeligheten til en informasjonsmengde. Nasjonale beredskapsplaner er et eksempel på dokumenter med informasjon der alle tre aspektene må ivaretas. Om opplysningene i planene er kjent for en trusselaktør, kan de lett bli mindre effektive. Integriteten må ivaretas slik at man kan stole på at opplysningene i planene er korrekte. Tilgjengeligheten må også ivaretas slik at de som skal iverksette tiltak har planene for hånden når situasjonen krever det.

I andre tilfeller vil informasjonen kunne ha et større tilgjengelighets- og integritetsbehov enn et konfidensialitetsbehov. Et eksempel kan være informasjonen som en flygeleder som overvåker og dirigerer sivil flytrafikk. Flygelederen har som hovedoppgave å forhindre sammenstøt av fly i luften eller på bakken, og for å sørge for rask og effektiv trafikkavvikling. Flygelederens oppgaveløsning er avhengig av en uavbrutt strøm av korrekte opplysninger fra radarsystemer og kommunikasjonssystemer. Dette for å ha et oppdatert situasjonsbilde av hvilke fly som befinner seg i luftrommet, og hvor de befinner seg i forhold til hverandre. Informasjonens tilgjengelighet og integritet er derfor avgjørende for flygelederens evne til å løse sin oppgave. Hvorvidt informasjon om flyenes plassering i luftrommet er åpent tilgjengelig er ikke av betydning for flygelederens oppgaveløsning, og denne informasjonen har derfor ikke et konfidensialitetsbehov.

Forholdet mellom informasjonens behov for konfidensialitet, integritet, og tilgjengelighet ville kunne endres etter omstendighetene. Når det gjelder informasjon av betydning for nasjonale sikkerhetsinteresser vil slike endringer som oftest være forårsaket av pågående sikkerhetstruende virksomhet. Virksomheten må derfor kunne avveie hvilket behov som totalt sett er viktigst å ivareta av hensyn til nasjonale sikkerhetsinteresser.

Leveranser må bli sett i sammenheng med andre leveranser og en mer helhetlig forståelse. Det er den enkelte anskaffelse som normalt utløser en verdivurdering. Men en anskaffelse trenger ikke være et isolert tilfelle hos en leverandør eller en underleverandør. Det kan være flere anskaffelser, også ugradert, som til sammen danner et annet samlet bilde av betydningen av leverandøren, eller betydningen av et sett med leveranser som oppdragsgiveren vil bruke.

En oppdragsgiver må kunne forstå denne betydningen av den samlede informasjonsbildet som blir dannet ved flere anskaffelser hos en leverandør eller hos en underleverandør. En underleverandør som leverer lignende komponenter eller funksjoner til mange deler av et system vil bli mer betydelig for oppdragsgiver. Der en anskaffelse i seg selv ikke er betydelig nok til å utløse et skjermingsbehov, kan den få en annen betydning sammen med tidligere leveranser, eller fremtidige leveranser. Det samlede bildet kan bety at oppdragsgiver må ta initiativ til å revurdere skjermingsbehovene. Det kan altså bli situasjoner hvor det blir behov for å inngå avtale om sikkerhet i anskaffelsen etter

virksomhetssikkerhetsforskriften §18, sikkerhetsgradere anskaffelsen, endre tidligere graderinger og inngå sikkerhetsavtaler, eller tilsvarende. Det er mulig at en virksomhet over tid får en informasjonsmengde eller tilganger til klassifiserte objekter som blir betydelig, eller at leverandøren får en informasjonsmengde eller blir et objekt som skal sikkerhetsgraderes eller klassifiseres eller må vurderes underlagt sikkerhetsloven ved vedtak etter § 1-3.

Det er også viktig å huske at det kan også utløse varsling, også til departementet eller sikkerhetsmyndigheten, jfr. sikkerhetsloven § 9-4 og virksomhetssikkerhetsforskriften §19.

Verdivurdering skal bidra til å oppfylle sikkerhetslovens formål (§1-1). Det er viktig at en verdivurdering ikke gjøres uten sammenheng. Den må bidra til å forstå aktivitetens betydning for å kunne oppfylle lovens formål.

3. Sikkerhetsgradert informasjon

> ***§ 5-3. Sikkerhetsgradert informasjon.*** *En virksomhet som tilvirker informasjon, skal sikkerhetsgradere og merke informasjonen dersom det kan skade nasjonale sikkerhetsinteresser om den blir kjent for uvedkommende. Følgende sikkerhetsgrader skal benyttes:*
>
> *a) STRENGT HEMMELIG dersom det kan få helt avgjørende skadefølger*
>
> *b) HEMMELIG dersom det kan få alvorlige skadefølger*
>
> *c) KONFIDENSIELT dersom det kan få skadefølger*
>
> *d) BEGRENSET dersom det i noen grad kan få skadefølger*
>
> *Sikkerhetsgradering skal ikke brukes i større utstrekning eller for lengre tid enn nødvendig. Dersom ikke annet er bestemt, bortfaller sikkerhetsgraderingen etter 30 år.*
>
> *Kongen kan gi forskrift om sikkerhetsgradering og beskyttelse av informasjon som mottas eller gis innenfor rammen av en gjensidig overenskomst med fremmed stat eller en internasjonal organisasjon.*

Selv om det er et grunnleggende prinsipp i vårt demokrati å tilstrebe mest mulig åpenhet i forvaltningen, så vil det til enhver tid være informasjon som har et konfidensialitetsbehov. Innenfor sikkerhetslovens virkeområde kan dette være informasjon som (1) gir nasjonen en fordel i forholdet til en motpart, og/eller (2) gir en motpart en fordel som kan skade nasjonen. Førstnevnte kategori kan eksempelvis være informasjon som omhandler våpenteknologi eller diplomatiske aktiviteter. Sistnevnte kategori kan eksempelvis være informasjon om hvordan sivil infrastruktur kan settes ut av spill, eller hvordan demokratiske prosesser kan påvirkes negativt. Informasjon i begge disse kategoriene kan ha et behov for beskyttelse av bestemmelsene i sikkerhetsloven.

3.1. Sikkerhetsgradering

Det er virksomheten som tilvirker informasjonen som er ansvarlig for å vurdere hvorvidt informasjonen skal sikkerhetsgraderes. Sikkerhetsgradert informasjon kan også ha behov for at informasjonens integritet og tilgjengelighet ivaretas, av hensyn til nasjonale sikkerhetsinteresser.

Beslutningen om at informasjon skal sikkerhetsgraderes skal være et resultat av en vurdering hvor det konkluderes med at uautorisert tilgang til informasjonen rimelig kan forventes å forårsake skade på nasjonale sikkerhetsinteresser, og at skaden kan identifiseres og beskrives. Det er ikke nødvendig å utarbeide en skriftlig beskrivelse av skadefølgene, men den som graderer må være forberedt på å kunne begrunne beslutningen. En slik begrunnelse vil være sentral i forbindelse med en vurdering av om informasjonen skal omgraderes, iht. virksomhetsikkerhetsforskriften § 30, jf. § 32 og § 33.

Dersom en verdivurdering konkluderer med at konfidensialitetsbrudd ikke i noen grad kan medføre skadefølger for nasjonale sikkerhetsinteresser, skal informasjonen ikke sikkerhetsgraderes. Informasjonen skal dermed heller ikke beskyttes etter de særlige bestemmelsene for sikkerhetsgradert

informasjon i §§ 5-4 til 5-6. Dette utelukker imidlertid ikke at informasjonen skal beskyttes etter andre regelverk.

Dersom en verdivurdering konkluderer med at en informasjonsmengde skal sikkerhetsgraderes, skal en av de fire sikkerhetsgradene benyttes for å angi i hvor stor grad konfidensialitetsbrudd kan medføre skadefølger for nasjonale sikkerhetsinteresser.

3.2. Skadefølger

Formuleringen i § 5-3 *«(…) dersom det kan skade nasjonale sikkerhetsinteresser om den blir kjent for uvedkommende.»* omhandles som *skadepotensial* i den videre teksten. NSM legger til grunn at vurderingen av skadepotensial er en vurdering av hvorvidt, og i hvor stor grad, tap av konfidensialitet kan føre til *svekkelse*, *forringelse* eller *forhindring* av nasjonale sikkerhetsinteresser. Følgende liste er en ikke uttømmende oversikt over kategorier av informasjon som kan ha et skadepotensial:

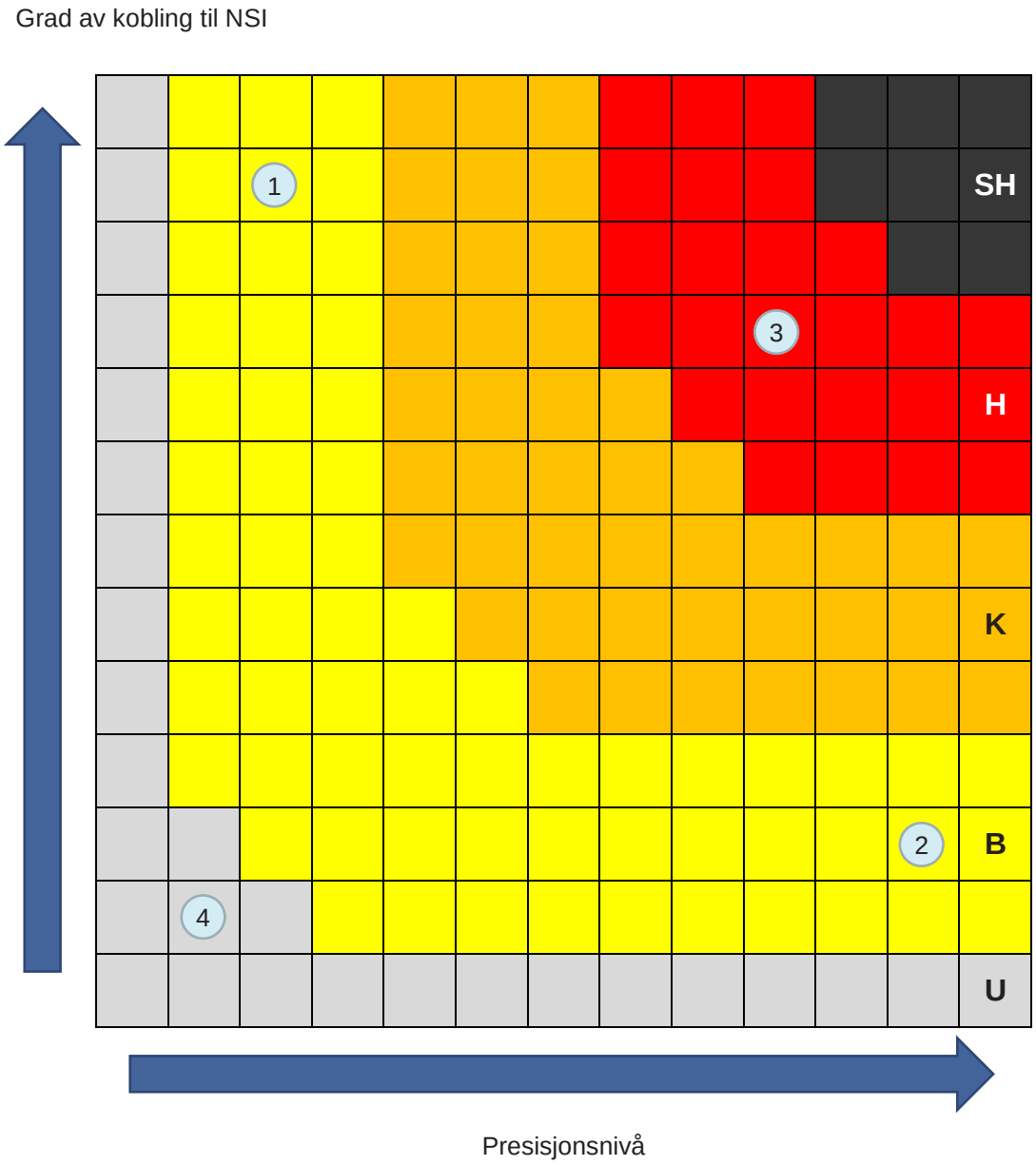
- Skadevurderinger
- Sårbarhetsvurderinger
- Konsekvensvurderinger
- Trusselvurderinger
- Etterretning
- Sivilt- og militært beredskapsplanverk
- Opplysninger om spesifikasjoner, kapasiteter og kapabiliteter
- Opplysninger om kryptologi
- Opplysninger om Norges diplomati
- Opplysninger som omhandler vitenskap og teknologi
- Opplysninger om sikkerhetstiltak
- Opplysninger om hendelser i fortid (f.eks. rapporter om sikkerhetsbrudd eller gjennomførte øvelser)
- Opplysninger om hendelser i fremtid (f.eks. scenarioer, besøk eller utvikling)
- Opplysninger om militære og sivile operasjoner
- EOS-tjenestenes kilder og metoder

Hvorvidt slike opplysninger faktisk *har* et skadepotensial avhenger av grad av kobling informasjonen har til de nasjonale sikkerhetsinteressene, og informasjonens presisjonsnivå. Med «*grad av kobling*» menes hvor stor betydning forholdet som opplysningen omhandler har for nasjonale sikkerhetsinteresser. Eksempelvis har planverkene for nasjonal beredskap og krisehåndtering høy grad av kobling til de nasjonale sikkerhetsinteressene.

Med «*presisjonsnivå*» menes hvor nøyaktig og konkret opplysningen er. Jo høyere presisjonsnivå, dess mer kunnskap overføres til uvedkommende ved tap av konfidensialitet. Denne kunnskapen kan øke en trusselaktørs kapasitet til å skade nasjonale sikkerhetsinteresser. Presisjonsnivået kan variere i angivelser av tid, sted, navn, antall og så videre.

Matrisen nedenfor gir en figurativ fremstilling av hvordan opplysninger kan ha (1) høy grad av kobling til nasjonale sikkerhetsinteresser, men et lavt presisjonsnivå, og dermed ha et skadepotensial som indikerer en lavere sikkerhetsgrad. Tilsvarende kan opplysninger ha (2) mindre kobling til de nasjonale sikkerhetsinteressene, men et høyt presisjonsnivå, og dermed også ha et skadepotensial som indikerer en lavere sikkerhetsgrad. Opplysninger med (3) høy grad av kobling til nasjonale sikkerhetsinteresser og med et høyt presisjonsnivå vil ha et høyt skadepotensial, og dermed måtte graderes høyt. Opplysninger med (4) lav kobling til de nasjonale sikkerhetsinteressene og lavt

presisjonsnivå vil ikke ha et skadepotensial som tilsier at opplysningene må sikkerhetsgraderes. Fargene i matrisen er ment å visualisere et økende skadepotensial ved høyere sikkerhetsgrad.



Figur 2.

3.3. Sikkerhetsgraden STRENGT HEMMELIG

NSM mener at formuleringen «*helt avgjørende skadefølger*» for nasjonale sikkerhetsinteresser må forstås som at et konfidensialitetsbrudd kan føre til:

- Bortfall eller svært kraftig svekkelse av regjeringens, stortingets eller høyesteretts funksjonsevne
- Bortfall eller svært kraftig svekkelse av funksjonsevnen til prioriterte deler av forvaltningen
- Bortfall eller svært kraftig svekkelse av Norges evne til suverenitetshevdelse
- Bortfall eller svært kraftig svekkelse av evne til å opprettholde nasjonal beredskap og krisehåndtering
- Bortfall eller svært kraftig svekkelse av evne til å håndtere sikkerhetspolitiske kriser og forsvar av norsk territorium
- Stans av bilateralt samarbeid om sikkerhet og etterretning, inkl. deltakelse i internasjonale operasjoner
- Ødeleggelse av samarbeidsrelasjoner med andre land og internasjonale organisasjoner (NATO, EU) om statssikkerhet
- Helt avgjørende skadefølger for allierte staters sikkerhet
- Stans av en stabil utvikling i makroøkonomiske hovedstørrelser som inflasjon, valutakurs, vekst og sysselsetting
- Bortfall eller svært kraftig svekkelse av velfungerende systemer for å håndtere offentlige ytelser og inntekter
- Bortfall eller svært kraftig svekkelse av stabile kapitalforhold overfor utlandet
- Bortfall eller svært kraftig svekkelse av stabilitet i finansiell infrastruktur og i finansmarkedene
  Bortfall eller svært kraftig svekkelse av infrastruktur og tjenester som er avgjørende for at sivilsamfunnet skal kunne fungere på en slik måte at øvrige nasjonale sikkerhetsinteresser kan ivaretas.

3.4. Sikkerhetsgraden HEMMELIG

NSM mener at formuleringen «*alvorlige skadefølger*» for nasjonale sikkerhetsinteresser må forstås som at et konfidensialitetsbrudd kan føre til:

- Kraftig svekkelse av regjeringens, stortingets eller høyesteretts funksjonsevne
- Kraftig svekkelse av funksjonsevnen til prioriterte deler av forvaltningen
- Kraftig svekkelse av Norges evne til suverenitetshevdelse
- Kraftig svekkelse av evne til å opprettholde nasjonal beredskap og krisehåndtering
- Kraftig svekkelse av evne til å håndtere sikkerhetspolitiske kriser og forsvar av norsk territorium
- Kraftig forhindring av bilateralt samarbeid om sikkerhet og etterretning, inkl. deltakelse i internasjonale operasjoner

- Kraftig forringelse av samarbeidsrelasjoner med andre land og internasjonale organisasjoner (NATO, EU) om statssikkerhet
- Alvorlige skadefølger for allierte staters sikkerhet
- Kraftig forhindring en stabil utvikling i makroøkonomiske hovedstørrelser som inflasjon, valutakurs, vekst og sysselsetting
- Kraftig svekkelse av velfungerende systemer for å håndtere offentlige ytelser og inntekter
- Kraftig svekkelse av stabile kapitalforhold overfor utlandet
- Kraftig svekkelse av stabilitet i finansiell infrastruktur og i finansmarkedene
- Kraftig svekkelse av infrastruktur og tjenester som er avgjørende for at sivilsamfunnet skal kunne fungere på en slik måte at øvrige nasjonale sikkerhetsinteresser kan ivaretas.

3.5. Sikkerhetsgraden KONFIDENSIELT

NSM mener at formuleringen «*skadefølger*» for nasjonale sikkerhetsinteresser må forstås som at et konfidensialitetsbrudd kan føre til:

- Svekkelse av regjeringens, stortingets eller høyesteretts funksjonsevne
- Svekkelse av funksjonsevnen til prioriterte deler av forvaltningen
- Svekkelse av Norges evne til suverenitetshevdelse
- Svekkelse av evne til å opprettholde nasjonal beredskap og krisehåndtering
- Svekkelse av evne til å håndtere sikkerhetspolitiske kriser og forsvar av norsk territorium
- Forhindring av bilateralt samarbeid om sikkerhet og etterretning, inkl. deltakelse i internasjonale operasjoner
- Forringelse av samarbeidsrelasjoner med andre land og internasjonale organisasjoner (NATO, EU) om statssikkerhet
- Skadefølger for allierte staters sikkerhet
- Forhindring av en stabil utvikling i makroøkonomiske hovedstørrelser som inflasjon, valutakurs, vekst og sysselsetting
- Svekkelse av velfungerende systemer for å håndtere offentlige ytelser og inntekter
- Svekkelse av stabile kapitalforhold overfor utlandet
- Svekkelse av stabilitet i finansiell infrastruktur og i finansmarkedene
- Svekkelse av infrastruktur og tjenester som er avgjørende for at sivilsamfunnet skal kunne fungere på en slik måte at øvrige nasjonale sikkerhetsinteresser kan ivaretas.

3.6. Sikkerhetsgraden BEGRENSET

NSM mener at formuleringen «*i noen grad kan få skadefølger*» for nasjonale sikkerhetsinteresser må forstås som at et konfidensialitetsbrudd kan føre til:

- Noe svekkelse av regjeringens, stortingets eller høyesteretts funksjonsevne
- Noe svekkelse av funksjonsevnen til prioriterte deler av forvaltningen
- Noe svekkelse av Norges evne til suverenitetshevdelse

- Noe svekkelse av evne til å opprettholde nasjonal beredskap og krisehåndtering
- Noe svekkelse av evne til å håndtere sikkerhetspolitiske kriser og forsvar av norsk territorium
- Noe forhindring av bilateralt samarbeid om sikkerhet og etterretning, inkl. deltakelse i internasjonale operasjoner
- Noe forringelse av samarbeidsrelasjoner med andre land og internasjonale organisasjoner (NATO, EU) om statssikkerhet
- Noe skadefølger for allierte staters sikkerhet
- Noe forhindring av en stabil utvikling i makroøkonomiske hovedstørrelser som inflasjon, valutakurs, vekst og sysselsetting
- Noe svekkelse av velfungerende systemer for å håndtere offentlige ytelser og inntekter
- Noe svekkelse av stabile kapitalforhold overfor utlandet
- Noe svekkelse av stabilitet i finansiell infrastruktur og i finansmarkedene
- Noe svekkelse av infrastruktur og tjenester som er avgjørende for at sivilsamfunnet skal kunne fungere på en slik måte at øvrige nasjonale sikkerhetsinteresser kan ivaretas.

4. Tidspunkt for avgradering

§ 5-3. Sikkerhetsgradert informasjon. (…)

Sikkerhetsgradering skal ikke brukes i større utstrekning eller for lengre tid enn nødvendig. Dersom ikke annet er bestemt, bortfaller sikkerhetsgraderingen etter 30 år.

Kongen kan gi forskrift om sikkerhetsgradering og beskyttelse av informasjon som mottas eller gis innenfor rammen av en gjensidig overenskomst med fremmed stat eller en internasjonal organisasjon.

For å unngå at det benyttes ressurser for å beskytte informasjon som ikke lenger har et konfidensialitetsbehov, skal en sikkerhetsgrad ikke gjelde for en lenger tidsperiode enn nødvendig. Å vurdere tidspunkt for avgradering er derfor en viktig del av verdivurderingen. Når informasjon gis en sikkerhetsgrad vil det i noen tilfeller være mulig å fastsette et spesifikt tidspunkt hvor informasjonens konfidensialitetsbehov endres eller opphører. Det kan eksempelvis være informasjon som omhandler planverk, besøk eller øvelser, som ikke har et konfidensialitetsbehov etter at aktiviteten er gjennomført. Sikkerhetsgraden bortfaller etter 30 år dersom ikke annet er bestemt. Hvis informasjon fortsatt har behov for beskyttelse etter 30 år, skal avgradering vurderes etter 40 år etter utstedelsen, og deretter hvert tiende år, jf. virksomhetssikkerhetsforskriften § 29. Det kan eksempelvis gjelde informasjon som inngår i strategiske planverk, og som er eldre enn 30 år, men som fortsatt er gjeldende og i bruk og dermed fortsatt skal beskyttes i henhold til kravene i sikkerhetsloven. Et dokument eller lagringsmedium skal merkes med sikkerhetsgradens varighet. NSMs veileder i håndtering og beskyttelse av sikkerhetsgradert informasjon angir utforming på slik merking.

5. Omgradering

Virksomhetsikkerhetsforskriften § 31. Hvem som kan omgradere

Informasjon med norsk sikkerhetsgradering kan omgraderes av virksomheten som har utstedt informasjonen, en overordnet virksomhet, det departementet som er ansvarlig for det forebyggende sikkerhetsarbeidet innenfor sektoren, og av Nasjonal sikkerhetsmyndighet. Informasjon med utenlandsk sikkerhetsgradering kan bare omgraderes av eller etter samtykke fra den staten eller organisasjonen som har utstedt informasjonen.

Med utgangspunkt i prinsippet om utsteders kontroll, er hovedregelen at det er utstedende virksomhet som skal vurdere og fatte beslutning om å omgradere sikkerhetsgradert informasjon. Øvrige virksomheters myndighet til å omgradere må derfor ses i sammenheng med § 33, hvor det fremgår at spørsmålet om omgradering skal legges frem for det departementet som er ansvarlig for det forebyggende sikkerhetsarbeidet innenfor sektoren, eller for Nasjonal sikkerhetsmyndighet i tilfeller hvor utstedende virksomhet ikke kan kontaktes. Dette vil i hovedsak gjelde tilfeller hvor utstedende virksomhet er nedlagt. Det vil likevel kunne oppstå tilfeller hvor utstedende virksomhet og overordnet virksomhet er uenige i hvorvidt informasjon skal omgraderes eller ikke. I slike tilfeller legges det til grunn at overordnet virksomhet eller departement kan, innenfor sin alminnelige instruksjonsmyndighet, instruere underordet virksomhet til å omgradere. NSM vil kunne benytte sin myndighet til å overprøve beslutninger om omgradering ved åpenbare feilvurderinger som kan resultere i skadefølger for nasjonale sikkerhetsinteresser.

Virksomhetsikkerhetsforskriften § 30. Omgradering av sikkerhetsgradert informasjon.

Virksomheten skal vurdere å omgradere sikkerhetsgradert informasjon dersom

a) den mottar et varsel om feil gradering etter § 32

b) den mottar en henvendelse om innsyn som nevnt i § 33

c) den avleverer dokumenter til Arkivverket

d) det ellers oppstår grunn til å tro at beskyttelsesbehovet for informasjonen har endret seg

En omgradering kan gå ut på å fastsette en annen sikkerhetsgrad etter sikkerhetsloven § 5-3 første ledd eller å avgradere informasjonen.

Bestemmelsens 2. ledd beskriver hva en omgradering kan innebære. I tillegg til å fastsette en annen grad (oppgradere eller nedgradere) eller å avgradere informasjonen, så må begrepet omgradering også anses å favne endringer vedrørende tidspunkt for avgradering etter sikkerhetsloven § 5-3. En vurdering av behov for omgradering vil utløses ved forhold som beskrevet i bestemmelsens bokstav a til d, og innebærer at man ser den opprinnelige beslutningen om sikkerhetsgrad opp mot eventuelle nye opplysninger, eller nye eller endrede forhold og forutsetninger.

En beslutning om ikke å omgradere sikkerhetsgradert informasjon skal være et resultat av en vurdering hvor det konkluderes med at konfidensialitetsbrudd rimelig kan forventes å fortsatt forårsake samme skade på nasjonale sikkerhetsinteresser.

En beslutning om å oppgradere sikkerhetsgradert informasjon skal være et resultat av en vurdering hvor det konkluderes med at konfidensialitetsbrudd rimelig kan forventes fortsatt å forårsake skade på

nasjonale sikkerhetsinteresser, men at skadefølgene anses å være mer omfattende enn ved den opprinnelige verdivurderingen.

En beslutning om å nedgradere sikkerhetsgradert informasjon skal være et resultat av en vurdering hvor det konkluderes med at konfidensialitetsbrudd rimelig kan forventes fortsatt å forårsake skade på nasjonale sikkerhetsinteresser, men at skadefølgene anses å være mindre omfattende enn ved den opprinnelige verdivurderingen.

En beslutning om å avgradere sikkerhetsgradert informasjon skal være et resultat av en vurdering hvor det konkluderes med at konfidensialitetsbrudd rimelig kan forventes ikke å lengre kunne forårsake skade på nasjonale sikkerhetsinteresser.

Virksomhetsikkerhetsforskriften § 33. Prosedyrer ved henvendelse om innsyn

En utsteder av sikkerhetsgradert informasjon som mottar et krav om innsyn i informasjon etter offentleglova eller miljøinformasjonsloven, eller om partsinnsyn etter forvaltningsloven, sla uten ugrunnet opphold vurdere om den samlede informasjonen eller deler av den skal omgraderes etter § 30.

En virksomhet som får en henvendelse om innsyn i sikkerhetsgradert informasjon den ikke har utstedt selv, skal uten ugrunnet opphold be utstederen om å vurdere omgradering. Utstederen skal uten ugrunnet opphold vurdere spørsmålet og gi tilbakemelding. Kan ikke utstederen kontaktes, skal spørsmålet om omgradering legges frem for det departementet som er ansvarlig for det forebyggende sikkerhetsarbeidet innenfor sektoren, eller for Nasjonal sikkerhetsmyndighet.

Dersom informasjon som er omfattet av retten til partsinnsyn etter forvaltningsloven, er gradert BEGRENSET, kan en autorisasjonsansvarlig autorisere en fysisk person som er part i saken, slik at det kan gis partsinnsyn.

Ved henvendelse om innsyn skal virksomheten gjennomføre en vurdering og fatte beslutning om hvorvidt informasjonen skal omgraderes eller ikke. Beslutning om ikke å omgradere tilsvarer avslag på innsynskrav, jf. offentleglova § 31. Bestemmelsen krever at avslag skal være skriftlig, og det skal vises til den konkrete bestemmelsen som er grunnlag for avslaget. For avslag med grunnlag i sikkerhetslovens bestemmelser skal det henvises til den konkrete bestemmelsen, samt offentleglova § 13.

Den som har fått avslag på innsynskrav kan kreve en nærmere begrunnelse, jf. offentleglova § 31, 2. ledd. En nærmere begrunnelse skal nevne hvilke overordnede hensyn som har vært avgjørende for avslaget, og hvorfor virksomheten mener at dette er grunnlag for avslag. Det er ikke krav om at begrunnelsen skal være uttømmende eller omfattende. Krav til innhold blir ytterligere avgrenset ved at virksomhetens begrunnelse ikke skal røpe informasjon som den skal eller kan og bør unnta for innsyn.

For øvrig vises til Rettleiar i offentleglova, og særlig kapittel 9 om håndtering av innsynskrav, samt underkapitlene 9.3 (om hvor lang tid organet kan bruke til å avgjøre innsynskrav), 9.4 (om hvordan organet kan gi innsyn), og 9.5 (om avslag og begrunnelse).

6. Punktgradering og sammenstilling

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 samme sikkerhetsgraderingen, så skal merkingen, så langt det er praktisk mulig, vise hvilke deler som er av 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.

6.1. Punktgradering

Sikkerhetsgrader skal ikke benyttes i større utstrekning enn nødvendig. Dersom ikke all informasjon i et dokument eller i et lagringsmedium har samme sikkerhetsgrad, skal merkingen, så langt det er praktisk mulig, vise hvilke deler som har hvilken sikkerhetsgrad eller ingen sikkerhetsgrad, jf. virksomhetssikkerhetsforskriften § 28. Dette kalles å punktgradere informasjon. Det fullstendige dokumentet eller lagringsmediet skal graderes med minst den høyeste sikkerhetsgrad som er benyttet i dokumentet eller lagringsmediet. Punktgradering kan forenkle håndteringen av sikkerhetsgradert informasjon på flere måter. Eksempelvis blir det enklere å distribuere et dokument til en større brukergruppe hvis en kan utelate de høyest graderte avsnittene eller samle dem i et vedlegg til slutt som ikke nødvendigvis tilflyter alle mottakere av hoveddokumentet. Et annet moment er at det blir lettere for mottakere av sikkerhetsgradert informasjon å gjenbruke deler av den i sine dokumenter.

6.2. Sammenstilling

Som nevnt i forrige delkapittel er det den høyeste sikkerhetsgraden brukt i informasjonsmengden som er førende for hvilken sikkerhetsgrad den samlede informasjonsmengden får. Sammenstilling av opplysninger kan likevel føre til at den samlede informasjonsmengden får et større skadepotensial enn enkeltopplysningene. Det er derfor være nødvendig å verdivurdere den samlede informasjonsmengden. Det vil også være nødvendig å gjøre nye verdivurderinger ved ny sammenstilling med annen informasjon.

En sammenstilling av ugraderte opplysninger skal sikkerhetsgraderes om sammenstillingen avslører ytterligere assosiasjoner eller relasjoner som (1) ikke på annen måte er avslørt i de individuelle

opplysningene, og (2) der disse ytterligere assosiasjonene eller relasjonene i seg selv har et skadepotensial for nasjonale sikkerhetsinteresser.

Tilsvarende skal en sammenstilling av lavere graderte opplysninger gis en høyere sikkerhetsgrad om sammenstillingen avslører ytterligere assosiasjoner eller relasjoner som (1) ikke på annen måte er avslørt i de individuelle opplysningene, og (2) der disse ytterligere assosiasjonene eller relasjonene i seg selv har et større skadepotensial for nasjonale sikkerhetsinteresser enn enkeltopplysningene.

Den som verdivurderer må også vurdere om en sammenstilling av lavere graderte opplysninger innebærer et akkumulert skadepotensial som krever en høyere sikkerhetsgrad enn enkeltopplysningene. Eksempelvis er opplysninger om klassifiseringsnivåene for skjermingsverdige objekter og infrastruktur sikkerhetsgradert BEGRENSET eller høyere. En oversikt over samtlige eller et større antall klassifiserte objekter og infrastrukturer skal derimot sikkerhetsgraderes KONFIDENSIELT eller høyere (§ 57 i virksomhetssikkerhetsforskriften).

Virksomheten må vurdere om en samlet informasjonsmengde representerer et mer omfattende eller alvorlig skadepotensial enn skadepotensialet relatert til de enkelte opplysningene. Utfallet av en slik vurdering kan være:

- Informasjonsmengden har ikke et større skadepotensial enn enkeltopplysningene, og informasjonsmengden blir derfor gitt samme gradsnivå som enkeltopplysningen(e) med høyeste sikkerhetsgrad, eller
- Informasjonsmengden har et større skadepotensial enn enkeltopplysningene, dermed beholder hver enkelt opplysning som inngår i informasjonsmengden sin sikkerhetsgrad, mens den samlede informasjonsmengden gis en høyere sikkerhetsgrad.

Sammenstilt sikkerhetsgradert informasjon som inneholder komponenter fra ulike utenlandske myndigheter og/eller internasjonale organisasjoner skal ikke nedgraderes eller avgraderes uten skriftlig forhåndssamtykke fra kompetent myndighet i det aktuelle land eller organisasjon. Ved gjenbruk og sammenstilling av ulike opplysninger med ulike utstedende virksomheter, må det klart kunne identifiseres hvem som er informasjonseier av de enkelte delene.

6.2.1. Verdivurdering ved innkjøp eller anskaffelser

Ved anskaffelser skal oppdragsgiver vurdere om anskaffelsen faller inn under kapittel 9 i sikkerhetsloven. Bestemmelsene, vurderingene og virkemidlene er knyttet til den enkelte anskaffelse og risikoen den kan medføre. Det er imidlertid sentralt at anskaffelsens verdi vurderes helhetlig, slik at all informasjon leverandøren vil få tilgang til, direkte eller indirekte, tas i betraktning. Verdivurderingen må være bredt anlagt. Den skal ikke bare omfatte informasjon leverandøren fysisk får utlevert fra oppdragsgiver, men må også omfatte den innsikt og den kunnskap leverandøren samlet sett vil opparbeide gjennom oppdraget. En anskaffelse har alltid en kontekst. En situasjon hvor et samlet bilde blir sikkerhetsgradert, kan like godt oppstå hos en underleverandør som hos hovedleverandøren. Oppdragsgiver skal ha oversikt over leverandørkjeden og inngå sikkerhetsavtaler også med underleverandører.

Verdi- og risikovurderingen bør omfatte hvilken betydning underleverandørforhold kan få for skjermingsverdige verdier eller tilganger. Oppdragsgiver skal ha, eller skaffe seg oversikt over den aktuelle underleverandørkjeden som vil kunne ha betydning for tilgang til skjermingsverdige verdier eller objekter. På bakgrunn av den vil oppdragsgiver kunne vurdere om det skal stilles spesielle krav i sikkerhetsavtalen og/eller kontrakts-/avtaleforhold som gir oppdragsgiver innsikt, varsling, eller annen oppdatert informasjon, f.eks. konkrete krav til oppdatering av informasjon om underleverandører. Det må legges til grunn at leverandøren skal varsle oppdragsgiver om endringer i underleverandørforholdene, regulert ved avtale, unntaket er hvis det åpenbart ikke vil være relevant for beskyttelsen av eller tilgangen til de skjermingsverdige verdiene.

Det er viktig at verdivurderingen gjøres tidlig i anskaffelsesløpet, med en kontekst og i et levetidsperspektiv, slik at verdivurderingen kan omfatte de avhengigheter som skapes og at oppdragsgiver han ha et informert syn på den informasjonen som kan sammenstilles hos leverandører.

Hvis verdivurderingen blir gjort tidlig nok, kan oppdragsgiver etablere en anskaffelsesstrategi i tråd med beskyttelsesbehovene, sammen med de andre behovene som ligger til grunn for anskaffelsesstrategien. Oppdragsgiver kan da velge anskaffelsesmetodene innenfor de mulighetene lovverket gir.

I et anskaffelsesløp kan det også være nødvendig å revurdere verdivurderingen når nye forhold blir kjent, enten det gjelder vurderinger som er gjort tidligere eller ikke. Det er ikke gitt at alle avhengigheter eller underleverandørkjeden kan være kjent på forhånd. En revurdert verdivurdering basert på nye forhold kan utløse et behov for å inngå egne sikkerhetsavtaler med underleverandører, der det før anskaffelsen ikke var et behov for dette. En revurdert verdivurdering kan også utløse behov for å iverksette en leverandørklareringsprosess, varsling eller andre sikkerhetstiltak i den aktuelle anskaffelsen, eller i andre anskaffelser.

Verdivurdering skal bidra til å oppfylle sikkerhetslovens formål (§1-1). Det er viktig at en verdivurdering ikke gjøres uten sammenheng. Den må bidra til å forstå aktivitetens betydning for å kunne oppfylle lovens formål.

Nasjonal sikkerhetsmyndighet

Postboks 814
1306 Sandvika

post@nsm.stat.no
www.nsm.stat.no