NSM

Veiledning ugradert skjermingsverdig informasjon og informasjonssystem

onsdag 23. 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.

Innhold

1 Innledning

Denne veilederen gir en oversikt over hvordan NSM tolker sikkerhetsloven hva gjelder ugradert skjermingsverdig informasjon og informasjonssystem.

2 Sammendrag

Det følger av definisjonen av skjermingsverdig informasjon i sikkerhetsloven § 5-1, jf. § 5-3 at det eksisterer en kategori informasjon som skal beskyttes som følge av skadepotensiale for nasjonale sikkerhetsinteresser hvis informasjonen blir endret, går tapt eller blir gjort utilgjengelig, men som ikke har tilsvarende skadepotensiale dersom den blir kjent for uvedkommende. Slik informasjon omtales som **ugradert skjermingsverdig.** Dette vil sjelden dreie seg om enkeltopplysninger, men primært gjelde større mengder informasjon samlet i et informasjonssystem.

Ugradert skjermingsverdig informasjon skal beskyttes i henhold til regler gitt i sikkerhetsloven kapittel 5.

Et informasjonssystem er skjermingsverdig etter sikkerhetsloven § 6-1 dersom systemet *i seg selv* har avgjørende **betydning** for en grunnleggende nasjonal funksjon. Dette gjelder uavhengig av om den avgjørende betydningen skyldes informasjonen som behandles i informasjonssystemet, systemet som sådan, eller en kombinasjon av disse to.

Et informasjonssystem med slik betydning for grunnleggende nasjonale funksjoner vil sannsynligvis også ha et visst **skadepotensiale** for de samme grunnleggende nasjonale funksjoner, dersom informasjonssystemet får redusert funksjonalitet eller blir utsatt for skadeverk, ødeleggelse eller rettsstridig overtakelse. I så tilfelle skal systemet utpekes og klassifiseres etter sikkerhetsloven kapittel 7. Denne typen ugraderte skjermingsverdige systemer vil altså i det vesentlige også omfattes av reglene om objekt- og infrastruktursikkerhet i kapittel 7.

Informasjonssystemer som behandler ugradert skjermingsverdig informasjon vil også være ugradert skjermingsverdig etter sikkerhetsloven § 6-1. I praksis vil et informasjonssystem med et slikt skadepotensiale for nasjonale sikkerhetsinteresser antakelig også ha et visst **skadepotensiale** for grunnleggende nasjonale funksjoner om det får redusert funksjonalitet, blir utsatt for skadeverk, ødeleggelse eller rettsstridig overtakelse. I så tilfelle skal også slike systemer utpekes og klassifiseres etter sikkerhetsloven kapittel 7. Denne typen ugraderte skjermingsverdige systemer vil derfor i det vesentlige også omfattes av reglene om objekt- og infrastruktursikkerhet i kapittel 7.

Ugraderte skjermingsverdige verdier vil på denne bakgrunn stort sett falle inn under regler om objekt- og infrastruktursikkerhet. Begrepet «ugradert skjermingsverdig» vil derfor primært få selvstendig betydning for *skjermingsverdige informasjonssystemer* hvor skadepotensiale ved redusert funksjonalitet, skadeverk eller rettsstridig overtakelse er lite, og ikke når opp til skadefølgen for skjermingsverdig infrastruktur som skal klassifiseres som VIKTIG. Disse informasjonssystemene skal beskyttes etter reglene gitt i kapitlene 5 og 6.

3 Ugradert skjermingsverdig informasjon

3.1 Konfidensialitet, integritet og tilgjengelighet

Det fremkommer av sikkerhetsloven § 5-1, jf. § 5-3, at informasjon er skjermingsverdig dersom det kan skade nasjonale sikkerhetsinteresser at informasjonen blir kjent for uvedkommende, går tapt, blir endret *eller* blir utilgjengelig. Disse behovene for å ivareta henholdsvis informasjonens **konfidensialitet**, **integritet** og **tilgjengelighet** er alternative vilkår, og medfører at informasjon er skjermingsverdig etter sikkerhetsloven dersom ett, eller flere, av disse vilkårene er oppfylt.

Dersom det kan skade nasjonale sikkerhetsinteresser at informasjonen blir kjent for uvedkommende, og informasjonen må beskyttes som følge av behov for **konfidensialitet**, skal informasjonen sikkerhetsgraderes, jf. § 5-3.

Informasjon som skal sikkerhetsgraderes grunnet konfidensialitetsbehov, kan også ha skadepotensiale knyttet til tilgjengelighets- og integritetsbrudd. Dette er det viktig å være klar over, både ved verdivurdering og ved valg av tiltak for beskyttelse. Skjermingsverdig informasjon skal beskyttes slik at informasjonen ikke går tapt eller blir endret, og er tilgjengelig ved behov (integritet og tilgjengelighet). Dette gjelder uavhengig av om informasjonen er gradert eller ikke, og følger direkte av sikkerhetsloven § 5-2.

3.2 Informasjonen går tapt, blir endret eller utilgjengelig

Det følger av definisjonen av skjermingsverdig informasjon, at det kan eksistere skjermingsverdig informasjon som ikke har behov for konfidensialitetsbeskyttelse. Loven har ikke noe begrep for denne typen informasjon, men virksomhetsikkerhetsforskriften § 22 første ledd bruker begrepet «ugradert skjermingsverdig informasjon.». **Ugradert skjermingsverdig informasjon er således informasjon med skadepotensiale for nasjonale sikkerhetsinteresser knyttet til tilgjengelighets- og/eller integritetsbehov, men hvor det ikke er behov for å beskytte informasjonens konfidensialitet i henhold til sikkerhetsloven.**

3.3 Andre hensyn enn nasjonale sikkerhetsinteresser

Det kan naturligvis være behov for å beskytte ugradert informasjons konfidensialitet – men da av andre årsaker enn skadepotensiale for nasjonale sikkerhetsinteresser, som for eksempel, sensitive personopplysninger, børssensitiv informasjon eller annen taushetsbelagt informasjon. Denne typen konfidensialitetsbehov faller utenfor sikkerhetsloven og begrepet «ugradert skjermingsverdig», og dermed også denne veilederen.

3.4 Krav til beskyttelse av skjermingsverdig informasjon

Ugradert skjermingsverdig informasjon som går tapt eller blir endret, kan ha like stort skadepotensiale for nasjonale sikkerhetsinteresser som sikkerhetsgradert informasjon som blir kjent for uvedkommende. Det er i regelverket ikke oppstilt ulike skadenivåer for skjermingsverdig informasjon med beskyttelsesbehov knyttet til integritet og/eller tilgjengelighet, eller krav til merking, slik som det er for sikkerhetsgradert informasjon.

Etter sikkerhetsloven § 5-2 skal virksomheten sørge for et forsvarlig sikkerhetsnivå for skjermingsverdig informasjon. Etter loven omfatter dette både skjermingsverdig gradert (informasjon) og ugradert skjermingsverdig informasjon. Virksomhetene skal selv vurdere informasjonens verdi, og iverksette nødvendige sikkerhetstiltak.

Virksomhetsikkerhetsforskriften § 22 første ledd stiller krav om at tiltak for beskyttelse av ugradert skjermingsverdig informasjon som et minimum skal sørge for at informasjonen ikke kan gå tapt, endres eller gjøres utilgjengelig med enkle midler. Videre fremkommer det i § 22, at dersom risikoen tilsier det, skal informasjonen også beskyttes mot avanserte angrepsmetoder. Også dette er opp til den enkelte virksomhet å vurdere.

4 Ugradert skjermingsverdig informasjonssystem

4.1 Skjermingsverdig informasjonssystem – sikkerhetsloven kapittel 6

Etter sikkerhetsloven § 6-1 er et informasjonssystem skjermingsverdig dersom det enten «behandler skjermingsverdig informasjon» (alternativ 1) eller det «i seg selv har avgjørende betydning for grunnleggende nasjonale funksjoner» (alternativ 2). Det finnes altså flere varianter ugradert skjermingsverdig informasjonssystem.

Beskyttelsesbehovet, og lovens anvendelse, kan utløses både av informasjonens skadepotensiale for nasjonale sikkerhetsinteresser, og av informasjonssystemet som sådan som følge av systemets betydning for grunnleggende nasjonale funksjoner.

Ved vurdering av informasjonens verdi, vil det ofte være vanskelig å avgjøre om skadepotensialet er knyttet til informasjonen som sådan, eller om den egentlig er knyttet til informasjonssystemets funksjon, eller en kombinasjon av disse. Antakelig vil skadepotensialet ofte være knyttet til begge disse to faktorene. Informasjonssystem som er ugradert skjermingsverdig fordi det behandler ugradert skjermingsverdig informasjon (§ 6-1 første ledd alternativ 1), vil dermed sannsynligvis også ofte ha avgjørende betydning for en grunnleggende nasjonal funksjon (§ 6-1 første ledd alternativ 2).

Sikkerhetsloven kapittel 6 inneholder krav til beskyttelse av skjermingsverdig informasjonssystem. Virksomheten skal sørge for et forsvarlig sikkerhetsnivå for skjermingsverdig informasjonssystem, jf. § 6-2. Kravene i kapittel 6 gjelder generelt for ethvert skjermingsverdig informasjonssystem, uavhengig av om informasjonssystemet er skjermingsverdig fordi det behandler skjermingsverdig informasjon, eller fordi det i seg selv har avgjørende betydning for grunnleggende nasjonale funksjoner.

4.2 Skjermingsverdig objekt og infrastruktur – sikkerhetsloven kapittel 7

Sikkerhetsloven kapittel 7 omhandler utpeking og klassifisering av skjermingsverdige objekt og infrastruktur, samt krav til beskyttelse av disse, jf. § 7-1 til 7-3. Etter § 7-1 første ledd er et objekt eller en infrastruktur skjermingsverdig «dersom det kan skade grunnleggende nasjonale funksjoner om de får redusert funksjonalitet eller blir utsatt for skadeverk,

ødeleggelse eller rettsstridig overtakelse.» Definisjonen er altså styrt av objektets eller infrastrukturens potensiale til å ***skade*** grunnleggende nasjonale funksjoner.

Bestemmelsene i kapittel 7 kommer kun til anvendelse dersom departementet etter § 7-1 andre ledd eller i visse tilfeller NSM (§ 7-1 tredje ledd), faktisk har utpekt og klassifisert objektet eller infrastrukturen som skjermingsverdig. Bestemmelsene i kapittel 7 gjelder også for informasjonssystem som anses som, eller er del av, skjermingsverdig infrastruktur, herunder ugradert skjermingsverdig informasjonssystem. Bestemmelsene i kapittel 7 kommer ikke til anvendelse dersom verken departementet eller NSM har utpekt informasjonssystemet etter § 7-1. I Prop. 153 L (2016-2017) pkt. 10.5.3.4 vises det til at det i flere tilfeller kan være aktuelt å peke ut skjermingsverdig informasjonssystem som skjermingsverdig objekt eller infrastruktur.

Lovens § 6-3 stiller krav om at skjermingsverdige informasjonssystemer skal godkjennes av en godkjenningsmyndighet. Dette gjelder også ugraderte skjermingsverdige informasjonssystemer. Hvis informasjonssystemet er utpekt som, eller har avgjørende betydning for funksjonen til, et objekt eller infrastruktur klassifisert KRITISK eller MEGET KRITISK, er det NSM som er godkjenningsmyndighet, jf. virksomhetsikkerhetsforskriften § 51 første ledd.

Det er virksomheten selv som skal godkjenne informasjonssystem som behandler ugradert skjermingsverdig informasjon, men ikke er utpekt og klassifisert etter kapittel 7, jf. virksomhetsikkerhetsforskriften § 51 tredje ledd. Det er også virksomheten selv som skal godkjenne ugradert skjermingsverdig informasjonssystem som er utpekt som eller har avgjørende betydning for objekt eller infrastruktur klassifisert VIKTIG, jf. virksomhetsikkerhetsforskriften § 51 tredje ledd.

4.3 Sammenhengen mellom § 6-1 og § 7-1

Både § 6-1 og § 7-1 gir en definisjon av hva som er å anse som skjermingsverdig – av henholdsvis informasjonssystem og objekt og infrastruktur. Ordlyden i de to bestemmelsene er imidlertid ulik.

- Som skjermingsverdig informasjonssystem regnes blant annet informasjonssystem som «har avgjørende **betydning** for grunnleggende nasjonale funksjoner».
- Som skjermingsverdig objekt eller infrastruktur regnes objekt eller infrastruktur «som kan **skade** grunnleggende nasjonale funksjoner om de får redusert funksjonalitet eller blir utsatt for skadeverk, ødeleggelse eller rettsstridig overtakelse.»

Vurderingstemaene er altså ulike – henholdsvis **betydning** for – og **skadepotensiale** for grunnleggende nasjonale funksjoner.

Et informasjonssystem vil kunne være skjermingsverdig etter § 6-1, men ikke etter § 7-1, og omvendt. Det antas imidlertid at informasjonssystemer med avgjørende betydning for grunnleggende nasjonale funksjoner, også vil ha et visst skadepotensiale for samme funksjon, dersom systemet får redusert funksjonalitet eller blir utsatt for skadeverk, ødeleggelse eller rettsstridig overtakelse. Der hvor skadepotensialet er av en slik grad at det vil nå opp til terskelen for skjermingsverdighet gitt i § 7-1, skal systemet utpekes og klassifiseres. Etter § 7-2 første ledd bokstav c, skal objekt/infrastruktur klassifiseres VIKTIG, som er det laveste klassifiseringsnivået, «dersom det kan få skadefølger» for grunnleggende

nasjonale funksjoner, dersom det får redusert funksjonalitet, eller blir utsatt for skadeverk, ødeleggelse eller rettsstridig overtakelse. Slike informasjonssystemer skal pekes ut og klassifiseres, og beskyttes i henhold til reglene i sikkerhetsloven kapitlene 6 og 7.

Krav om autorisasjon og adgangsklarering for tilgang til informasjonssystem pekt ut som skjermingsverdig objekt/infrastruktur etter kapittel 7, er utelukkende aktuelt dersom vedkommende sektordepartement har fattet vedtak om krav om adgangsklarering.

Det kan også eksistere ugraderte skjermingsverdig informasjonssystemer etter sikkerhetsloven § 6-1 alternativ 2, som har et visst skadepotensiale for grunnleggende nasjonale funksjoner, uten at dette når opp til skadepotensialet for objekt/infrastruktur klassifisert VIKTIG. Disse informasjonssystemene kan omtales som informasjonssystemer som **i noen grad kan skade** grunnleggende nasjonale funksjoner dersom de får redusert funksjonalitet, eller blir utsatt for skadeverk, ødeleggelse eller rettsstridig overtakelse. Slike informasjonssystemer skal beskyttes i henhold til reglene i kapittel 6, men ikke kapittel 7, ettersom de ikke skal utpekes og klassifiseres som skjermingsverdig infrastruktur.