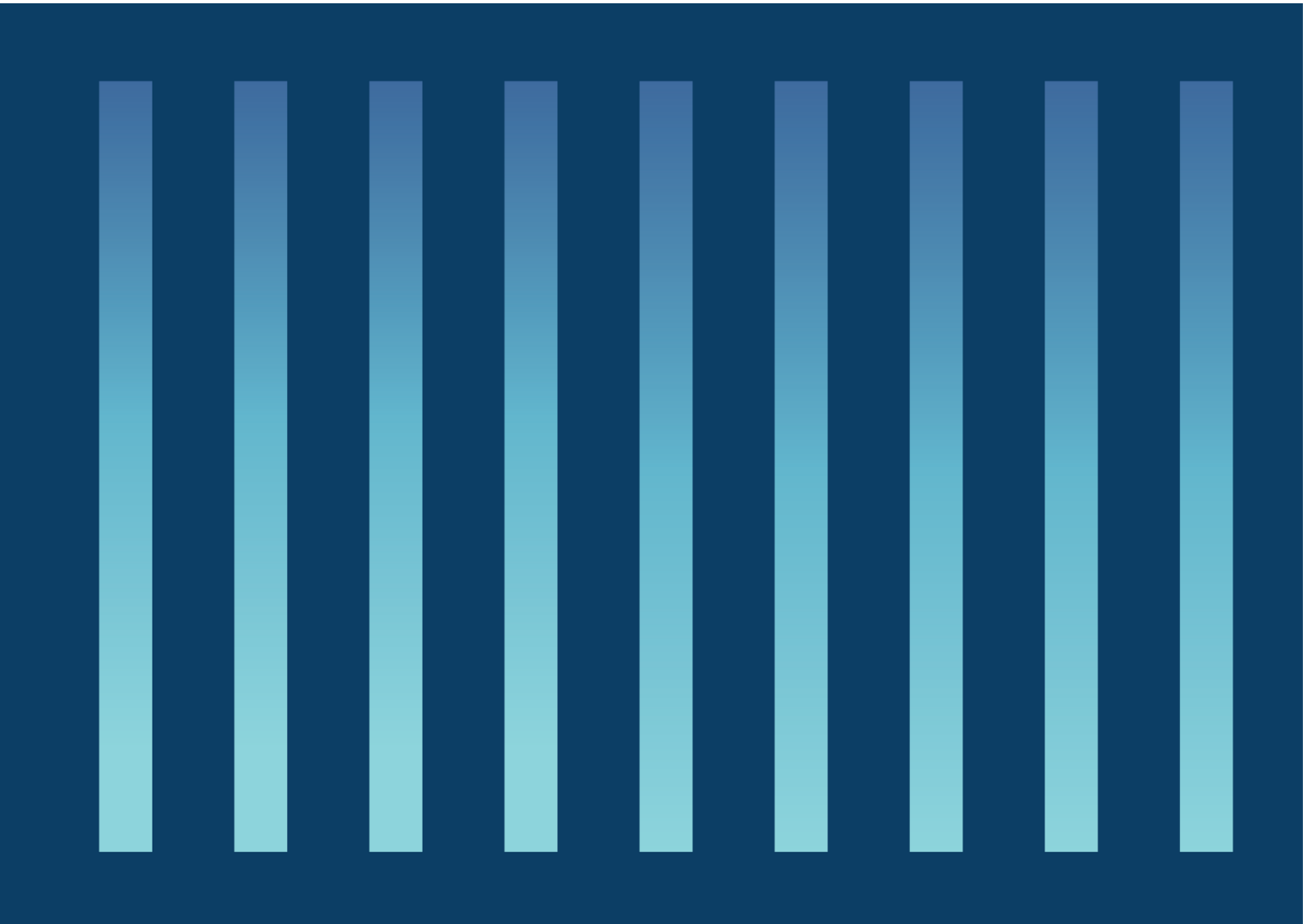
NASJONAL
SIKKERHETSMYNDIGHET

Veileder for virksomheters håndtering av uønskede hendelser

Versjon: 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. Uønskede hendelser

Målgruppen for *Veileder for virksomheters håndtering av uønskede hendelser* er virksomheter underlagt sikkerhetsloven, det vil si personell som skal etablere systemer for håndtering av uønskede hendelser. Dette inkluderer personell som skal rapportere slike hendelser internt i virksomheten samt personellet som har ansvar for rapportering og varsling eksternt.

Et av sikkerhetslovens formål er å bidra til å forebygge, avdekke og motvirke sikkerhetstruende virksomhet. Loven stiller krav om tiltak ved slik virksomhet, samt ved avvik og sikkerhetsbrudd. Håndtering av slike hendelser har fellestrekk, uavhengig av hendelsesforløpet og av om handlingene i seg selv er tilsiktede eller utilsiktede. Begrepet uønskede hendelser benyttes i denne veilederen derfor som fellesbetegnelse for:

- *sikkerhetstruende virksomhet* – tilsiktede handlinger som direkte eller indirekte kan skade nasjonale sikkerhetsinteresser, jf. sikkerhetsloven § 1-5 punkt 4. Dette kan omfatte enhver aktivitet som kan medføre at nasjonale sikkerhetsinteresser blir truet, herunder spionasje, sabotasje og terror.
- *sikkerhetsbrudd* – funksjonsfeil i skjermingsverdige informasjonssystemer, tap av konfidensialitet, integritet eller tilgjengelighet for skjermingsverdig informasjon og redusert funksjonalitet, skadeverk, ødeleggelse eller rettsstridig overtakelse av skjermingsverdige objekter og infrastruktur
- *avvik* – manglende samsvar med krav i eller i medhold av sikkerhetsloven eller virksomhetens styringssystem for sikkerhet

Etablering av systemer for håndtering av hendelser for å oppfylle krav i eller i medhold av sikkerhetsloven må ses i sammenheng med krav i andre regelverk, som nasjonalt beredskapssystem og sektorlovgivning.

1.1. Krav knyttet til hendelser og tiltak

Sikkerhetsloven med forskrifter har flere bestemmelser om ulike hendelser som skal håndteres. Sikkerhetsloven definerer sikkerhetstruende virksomhet i:

> *§ 1-5 Definisjoner (første ledd)*
>
> *…*
> *4. sikkerhetstruende virksomhet: tilsiktede handlinger som direkte eller indirekte kan skade nasjonale sikkerhetsinteresser*

Hendelser som skal håndteres fremgår av virksomhetsikkerhetsforskriften:

> *§ 8 Tiltak ved sikkerhetstruende virksomhet, avvik og kompromittering av sikkerhetsgradert informasjon (første ledd, første setning)*
>
> *Ved sikkerhetstruende virksomhet eller avvik fra styringssystemet for sikkerhet, skal virksomheten gjennomføre umiddelbare tiltak for å redusere skadeomfanget og gjøre tiltak som gjenoppretter det forsvarlige sikkerhetsnivået i virksomheten.*

Videre har sikkerhetsloven krav knyttet til forebyggende sikkerhetstiltak:

- *varsling* – av både sikkerhetstruende virksomhet og alvorlige brudd på krav til sikkerhet (jf. § 4-5 Varslingsplikt)
- *beskyttelse av skjermingsverdig informasjon* – mot kompromittering, tap av integritet og utilgjengelighet (jf. § 5-2 Beskyttelse av skjermingsverdig informasjon*)*
- *beskyttelse av skjermingsverdige informasjonssystemer* – mot funksjonsfeil, samt beskyttelse av informasjonen i systemet mot kompromittering, tap av integritet og utilgjengelighet (jf. § 6-2 Beskyttelse av skjermingsverdige informasjonssystemer)
- *beskyttelse av objekter og infrastruktur* – for opprettholdelse av et forsvarlig sikkerhetsnivå basert på en vurdering av risiko (jf. § 7-3 Beskyttelse av objekter og infrastruktur)

I tillegg har virksomhetsikkerhetsforskriften krav knyttet til:

- *å informere virksomhetens leder* – om saker som er viktige for det forebyggende sikkerhetsarbeidet (jf. § 6 Roller og ansvar i det forebyggende sikkerhetsarbeidet)
- *misbruk* – av skjermingsverdige informasjonssystemer (jf. § 49 Forsvarlig sikkerhetsnivå for skjermingsverdige informasjonssystemer)

2. Håndtering av uønskede hendelser

Uønskede hendelser skal håndteres for å begrense skade, sikre gjenoppretning og hindre gjentagelse. Uønskede hendelser kan innebære alvorlige sikkerhetsutfordringer, men er også et viktig grunnlag for virksomhetens kontinuerlige forbedring av eget forebyggende sikkerhetsarbeid. Håndtering av uønskede hendelser er en del av virksomhetens oppfølging av det forebyggende sikkerhetsarbeidet, og således også av virksomhetens styringssystem for sikkerhet.

Håndtering av uønskede hendelser omfatter deteksjon, varsling, iverksetting av umiddelbare tiltak, etablering av varige tiltak, evaluering av håndteringen og dokumentering.

2.1. Krav om håndtering av uønskede hendelser

Krav om håndtering av uønskede hendelser følger av sikkerhetslovens krav om sikkerhetsstyring i:

> *§ 4-1 Sikkerhetsstyring (første ledd)*
>
> *Virksomhetens leder har ansvaret for det forebyggende sikkerhetsarbeidet. Forebyggende sikkerhetsarbeid skal være en del av virksomhetens styringssystem. Sikkerhetstilstanden i virksomheten skal regelmessig kontrolleres.*

Kravet må forstås slik at sikkerhetsstyring også omfatter håndtering av uønskede hendelser. Krav om sikkerhetsstyring er utdypet i virksomhetsikkerhetsforskriften kapittel 1 med bestemmelse om håndtering av uønskede hendelser i:

> *§ 8 Tiltak ved sikkerhetstruende virksomhet, avvik og kompromittering av sikkerhetsgradert informasjon*
>
> *Ved sikkerhetstruende virksomhet eller avvik fra styringssystemet for sikkerhet skal en virksomhet gjennomføre umiddelbare tiltak for å redusere skadeomfanget og gjenopprette et forsvarlig sikkerhetsnivå. Det skal rapporteres om den sikkerhetstruende virksomheten eller avviket internt og til andre som kan bli berørt i stor grad. Virksomheten skal vurdere konsekvensene av den sikkerhetstruende virksomheten eller avviket.*
>
> *Hvis sikkerhetsgradert informasjon blir kjent for uautoriserte personer, skal virksomheten informere den som har tilvirket informasjonen, om hendelsen, i tillegg til å varsle etter sikkerhetsloven § 4-5.*

I tillegg har sikkerhetsloven krav om varsling ved uønskede hendelser i:

> *§ 4-5 Varslingsplikt*
>
> *Virksomheten skal straks varsle sikkerhetsmyndigheten og andre myndigheter som skal utføre tilsyn i medhold av § 3-1 andre ledd, dersom*
>
> *a) den har blitt rammet av sikkerhetstruende virksomhet*

b) det er begrunnet mistanke om at sikkerhetstruende virksomhet har rammet eller vil kunne ramme virksomheten eller andre virksomheter

c) det har skjedd alvorlige brudd på krav til sikkerhet etter kapittel 5, 6 eller 7.

Virksomheten skal uten hinder av taushetsplikt varsle tilsynsmyndigheten dersom den får kunnskap om en planlagt eller pågående aktivitet som kan medføre en ikke ubetydelig risiko for at nasjonale sikkerhetsinteresser blir truet. Tilsynsmyndigheten skal uten ugrunnet opphold varsle sikkerhetsmyndigheten og videresende varselet til ansvarlig departement for vurdering av vedtak etter § 2-5.

Kongen kan gi forskrift om varslingsplikten etter andre ledd.

Sikkerhetslovens krav om sikkerhetsstyring i § 4-1 må forstås slik at virksomheten skal etablere egne sikkerhetsbestemmelser for håndtering av uønskede hendelser. Disse bestemmelser må omfatte rutiner for deteksjon, varsling, umiddelbare og varige tiltak, evaluering og dokumentering i forbindelse med håndtering av uønskede hendelser. Sikkerhetsbestemmelsene må være kjent for alle som kan få tilgang til skjermingsverdige verdier, jf. virksomhetsikkerhetsforskriften § 7, andre ledd.

2.1.1. Deteksjon

Virksomhetsikkerhetsforskriften § 14 stiller krav om nødvendige tiltak for å oppnå et forsvarlig sikkerhetsnivå, herunder tiltak som muliggjør deteksjon av uønskede hendelser.

Videre har sikkerhetsloven § 6-4 krav om overvåkning av skjermingsverdige informasjonssystemer for blant annet å avdekke uønskede hendelser. Dette er utdypet i virksomhetsikkerhetsforskriften § 49 første ledd bokstav f som stiller krav om registrering av bruk, misbruk og forsøk på misbruk av skjermingsverdige informasjonssystemer.

Som for øvrige sikkerhetstiltak må tiltak for deteksjon av uønskede hendelser velges med utgangspunkt i virksomhetens egne risikovurderinger. Virksomheten må vurdere både fysiske tiltak (eksempelvis forsegling), elektroniske tiltak (eksempelvis overvåkning av datatrafikk og logganalyse), menneskelige tiltak (eksempelvis vakthold) og organisatoriske tiltak (eksempelvis rapportering og kontrollprosedyrer).

2.1.2. Varsling

Virksomhetsikkerhetsforskriften § 8 har krav om intern rapportering av sikkerhetstruende virksomhet, avvik og kompromittering av sikkerhetsgradert informasjon.

I praksis kan intern rapportering og varsling skje til nærmeste overordnede eller til den som virksomheten beslutter skal være ansvarlig for håndtering av uønskede hendelser. Virksomhetens leder skal informeres om saker som er viktige for det forebyggende sikkerhetsarbeidet, jf. virksomhetsikkerhetsforskriften § 6 andre ledd, dette omfatter sikkerhetstruende virksomhet og alvorlige sikkerhetsbrudd. Varslingsplikten omfatter også varsling til autorisasjonsansvarlig i virksomhetene om forhold som kan være av betydning for egen sikkerhetsmessige skikkethet, jf. sikkerhetsloven § 8-11.

Avhengig av den uønskede hendelsens art skal det varsels eksternt, til NSM og/eller til tilsynsmyndigheten[1] samt til andre berørte, jf. sikkerhetsloven § 4-5. Også virksomhetsikkerhetsforskriften § 8 har krav om varsling til andre som kan berøres av hendelsen.

Det følger av disse bestemmelsene at virksomheten skal varsle NSM og tilsynsmyndigheten ved sikkerhetstruende virksomhet eller ved kunnskap om planlagt eller pågående aktivitet som kan medføre en ikke ubetydelig risiko. Dette innebærer varslingsplikt for alt utover det som fremstår som usannsynlig eller som det kun er teoretisk mulighet for.

Videre skal virksomheten også varsle NSM og tilsynsmyndigheten ved mistanke om at egen eller andres virksomhet er, eller kan bli rammet av sikkerhetstruende virksomhet, dersom den vurderer det nødvendig å undersøke forholdet nærmere.

NSM og tilsynsmyndigheten skal også varsles om alvorlige sikkerhetsbrudd som følge av utilsiktede hendelser. Følgende hendelser rapporteres som alvorlige sikkerhetsbrudd:

- mulig eller faktisk kompromittering av informasjon sikkerhetsgradert KONFIDENSIELT eller høyere
- gjentatt kompromittering av informasjon sikkerhetsgradert BEGRENSET
- avbrudd i en grunnleggende nasjonal funksjon
- hendelse overfor eller forhold ved informasjonssystem, objekt eller infrastruktur som kan medføre slikt avbrudd

Også andre skal varsles om uønskede hendelser når hendelsen har betydning for deres forebyggende sikkerhetsarbeid. Blant annet skal tilvirker av skjermingsverdig informasjon som er kompromittert, varsles. Dersom den kompromitterte informasjonen er sikkerhetsgradert av utenlandsk myndighet eller internasjonal organisasjon, skal dette varsles til NSM.

Når uønskede hendelser innebærer mistanke om straffbare forhold etter sikkerhetsloven skal i tillegg Politiets sikkerhetstjeneste varsles, jf. sikkerhetsloven § 11-4.

2.1.3. Umiddelbare tiltak ved uønskede hendelser

Ved uønskede hendelser iverksettes nødvendige tiltak umiddelbart for å avverge eller begrense skade. Slike tiltak kan forberedes gjennom beredskapsplanverk og -systemer, og omfatter alt fra aktiviteter i akutte situasjoner til tiltak i påvente av at varige tiltak etableres.

Den allmenne plikten til å bidra i det forebyggende sikkerhetsarbeidet omfatter også plikt til å avverge hendelser og å begrense skade, så langt dette er mulig for den enkelte. Plikt til å iverksette umiddelbare tiltak og fremgangsmåten ved slik iverksetting, må være kjent for alle den angår.

Umiddelbare tiltak kan etableres av den enkelte, men ansvaret for tiltakene bør på et tidspunkt overtas av overordnede eller av den virksomheten har besluttet skal være ansvarlig for håndtering av uønskede hendelser.

[1] NSM er tilsynsmyndighet for virksomheter i de sektorer hvor overordnet departement ikke har utpekt en egen sektormyndighet med tilsynsansvar

Det er opp til virksomheten selv å vurdere hvilke tiltak som skal forberedes og iverksettes. Det følgende er eksempler på slike tiltak:

eksempler på umiddelbare tiltak	
fysisk	• etablering av vakthold • forsterket adgang-, vare-, post- og / eller kjøretøykontroll • avstengning av områder • evakuering og destruksjon av dokumenter og lagringsmedier
elektronisk	• begrense funksjonalitet, f.eks. frakoble eksterne tilkoblinger • oppdatering av programvare • forberedelse og oppstart av reservesystemer • installasjon av sikkerhetskopier
menneskelig	• repetisjon av sikkerhetsprosedyrer • begrensinger i adgang og tilganger • suspensjon av autorisasjon • nødautorisering
organisatorisk	• forsterke bemanning av sikkerhetskritiske funksjoner i organisasjonen • forberede og etablere kriseorganisering • begrense eller stanse ordinær aktivitet • evakuering av personell

2.1.4. Varige tiltak for grunnsikring og påbygging

Håndtering av uønskede hendelser omfatter også etablering av varige tiltak for å hindre gjentagelse av den uønskede hendelsen. Varige tiltak etableres som grunnsikringstiltak for å oppnå forsvarlig sikkerhetsnivå i normaltilstanden, og som påbygningstiltak forberedt for etablering ved endringer i risiko. Etablering av varige tiltak forutsetter analyse av underliggende årsak til hendelser inkludert undersøkelser av om tilsvarende hendelser har inntruffet tidligere eller andre steder.

Tiltak for grunnsikring og påbygging velges med grunnlag i risikovurdering, jf. virksomhetsikkerhetsforskriften § 13 og etableres i henhold til virksomhetsikkerhetsforskriften § 14 og i samsvar med prinsipper ved valg og utforming av sikkerhetstiltak som angitt i virksomhetsikkerhetsforskriften § 15.

Eksempler på aktuelle tiltak kan være forsterket fysisk eller logisk grunnsikring, økt frekvens av oppdateringer og sikkerhetskopier, kompetanse- og holdningsbyggende tiltak, revisjon av interne rutiner og instrukser, endring eller tilbakekalling av autorisasjon.

2.1.5. Evaluering av tiltakene

Kravet i virksomhetsikkerhetsforskriften § 9 om evaluering forebyggende sikkerhetsarbeid, innebærer at virksomheten må forsikre seg om at tiltak for grunnsikring og påbygging er etablert og fungerer etter hensikten. Dette innebærer at håndteringen av uønskede hendelser må omfattes av slike undersøkelser. Undersøkelsene kan eksempelvis gjennomføres som del av en intern sikkerhetsrevisjon.

Kravet i virksomhetsikkerhetsforskriften § 10 om årlig helhetlig gjennomgang av det forebyggende sikkerhetsarbeidet i innebærer at også håndtering av uønskede hendelser må omfattes av slike gjennomganger.

2.1.6. Dokumentering

Det følger av virksomhetsikkerhetsforskriften § 11 at håndtering av uønskede hendelser skal dokumenteres som del av virksomhetens kontrollerende dokumentasjon for forebyggende sikkerhetsarbeid. Det er aktuelt å dokumentere håndteringen i et systematisk register over alle uønskede hendelser der informasjon om hendelsene og om håndtering og evaluering inngår. Slik dokumentasjon kan blant annet brukes i forbindelse med varsling og ved evaluering av håndteringen.

Uønskede hendelser kan påvirke det forebyggende sikkerhetsarbeidet fremover i tid, og hendelsesregisteret gir viktig erfaringsgrunnlag for å oppnå forsvarlig sikkerhetsnivå. Informasjon fra håndtering av uønskede hendelser må derfor oppbevares for å oppnå et kontinuerlig forsvarlig sikkerhetsnivå. Aktuell lagringstid er fem år.

2.2. Andre krav til håndtering av uønskede hendelser

Sikkerhetsloven og forskrift om kryptosikkerhet har bestemmelser knyttet til håndtering av uønskede hendelser som berører kryptomateriell. Tilsvarende gjelder ved håndtering av uønskede hendelser i forbindelse med sikkerhetsgraderte anskaffelser.

3. Behandling av personopplysninger

Håndtering av uønskede hendelser, inklusiv dokumentering av håndteringen, vil ofte innebære behandling av personopplysninger. Personopplysningene skal i så fall behandles i samsvar med grunnprinsipper for personvern: Lovlighet, rettferdighet og gjennomsiktighet, formålsbegrensning, dataminimering, riktighet, lagringsbegrensing og integritet og fortrolighet.

Personvernprinsippene gir rammer for hvordan personopplysninger kan behandles ved håndtering av uønskede hendelser, blant annet slik at undersøkelser står i forhold til formålet med håndteringen og ikke er mer inngripende enn nødvendig.

3.1. Krav til behandling av personopplysninger

Sikkerhetsloven sammenholdt med virksomhetsikkerhetsforskriften § 8 må forstås slik at personopplysninger kan behandles i forbindelse med håndtering av uønskede hendelser, i den utstrekning dette er relevant og nødvendig ut fra formålet med håndteringen, det vil si i den utstrekning det er nødvendig for reduksjon av skadeomfang, gjenoppretting av forsvarlig sikkerhetsnivå, hindre gjentagelse, samt for å kunne analysere konsekvensene av hendelsen.

Virksomhetsikkerhetsforskriften har krav om forholdsmessighet og nødvendighet ved bruk av inngripende tiltak i:

> *§ 15 Prinsipper ved valg og utforming av sikkerhetstiltak (tredje og fjerde ledd)*
>
> *Virksomheten skal ikke bruke mer inngripende sikkerhetstiltak enn det som er nødvendig for å håndtere den aktuelle risikoen. I vurderingen av hva som er nødvendig, skal virksomheten særlig ta hensyn til enkeltpersoners rettssikkerhet og personvern. Det skal ikke behandles mer personopplysninger enn det som er nødvendig ut fra formålet med sikkerhetstiltaket.*
>
> *Når sikkerhetstiltaket kan gripe inn i enkeltpersoners rettssikkerhet eller personvern, skal virksomheten kunne dokumentere hvorfor inngrepet er nødvendig.*

Ved håndtering av uønskede hendelser ivaretas de grunnleggende prinsipper for personvern slik:

- *lovlighet, rettferdighet og gjennomsiktighet* – ved at personopplysninger behandles for å oppfylle virksomhetens plikter i henhold til bestemmelser gitt i og i medhold av sikkerhetsloven. Dette innebærer at opplysningene behandles med håndtering av uønskede hendelser som formål, og at medarbeidere og andre involverte er kjent med at opplysningene behandles for dette formålet
- *formålsbegrensning* – ved at personopplysninger behandles for å oppnå formålet med håndtering av uønskede hendelser, det vil si å begrense skade, sikre gjenoppretting og hindre gjentagelse, og ikke benyttes for andre formål

- *dataminimering* – ved at det ikke behandles andre personopplysninger enn de som er nødvendig for å oppfylle formålene angitt over, og som ikke er mer inngripende enn nødvendig. Dette forutsetter en avveining mellom et mulig resultat av en konkret håndtering av uønsket hendelse og inngrepet i den enkeltes personvern som må til for å oppnå dette resultatet
- *riktighet* – gjennom etablering av prosedyrer for retting eller sletting av personopplysninger som ikke er riktige, slik at ikke håndteringen av en uønsket hendelser baseres på feilaktige eller foreldete personopplysninger
- *lagringsbegrensing* – ved at personopplysninger ikke oppbevares lenger enn nødvendig. Dette innebærer blant annet at det må vurderes hvor lenge personopplysninger må inngå i dokumentasjon fra håndtering av uønskede hendelser
- *integritet og fortrolighet* – ved at personopplysningene sikres konfidensialitet, tilgjengelighet og integritet av hensyn til den enkeltes personvern, så vel som av de hensyn som følger av sikkerhetslovens formål. Dette innebærer at virksomhetens risikovurderinger også må dekke risiko ovenfor den enkeltes personvern, så vel som risiko for sikkerhetstruende virksomhet

Virksomheten må utarbeide rutiner for behandling av personopplysninger ved håndtering av uønskede hendelser, slik at det gjennomføres konkrete nødvendighetsvurderinger og avveininger i alle håndteringer hvor personopplysninger behandles.

3.2. Undersøkelser knyttet til enkeltindivider

Uønskede hendelser håndteres for å begrense skade, sikre gjenoppretting og hindre gjentagelse, med andre ord for å forbedre sikkerhetsnivået og sikkerhetsstyringen. I dette ligger at håndteringen også kan medføre undersøkelser knyttet til enkeltindivider. Virksomhetens undersøkelser av et alvorlig sikkerhetsbrudd kan for eksempel avdekke at en ansatt ikke har etterlevd sine sikkerhetsmessige plikter i arbeidsforholdet, og gi grunnlag for endring av eller tilbakekall av autorisasjon.

Undersøkelser og tiltak ved håndtering av uønskede hendelser skal ikke være mer inngripende overfor den enkelte enn nødvendig, jf. virksomhetsikkerhetsforskriften § 15, tredje ledd. Undersøkelser og tiltak skal velges i samsvar med håndteringens formål og det må i det enkelte tilfelle gjøres konkrete nødvendighetsvurderinger og avveininger. Når virksomheten benytter undersøkelser eller tiltak som kan være inngripende overfor den enkelte skal vurderingene til grunn for undersøkelsene dokumenteres.

4. Referanser

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

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

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

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

Vedlegg A – Varsel om uønsket hendelse

Fylles ut for hånd eller på godkjent informasjonssystem **Husk graderingsmerke**

Type hendelse		
☐ Sikkerhetstruende virksomhet	☐ Sikkerhetsbrudd	☐ Avvik

Berørte verdier			
☐ Skjermingsverdig informasjon	☐ Skjermingsverdig informasjonssystem	☐ Skjermingsverdig objekt	☐ Skjermingsverdig infrastruktur
☐ Nasjonale sikkerhetsinteresser		☐ Annet (utdyp):	

Høyeste graderings- / godkjennings- / klassifiseringsnivå på berørte verdier			
☐ BEGRENSET	☐ KONFIDENSIELT ☐ VIKTIG	☐ HEMMELIG ☐ KRITISK	☐ STRENGT HEMMELIG ☐ MEGET KRITISK
☐ Ugradert / Annet (utdyp):			

Hendelsen inntraff hos (virksomhet):			
Hendelse varsles av (virksomhet):			
Dato for hendelse:		Tid:	
Hvor inntraff hendelsen?			
Hva har skjedd?			
Hvem var involvert? Antatt aktør?			
Hvilke konsekvenser har hendelsen?			
Hvilke tiltak er iverksatt?			
Hvem er informert?			
Signatur:		**Sted, dato:**	
Blokkbokstaver:			

Se https://www.nsm.stat.no/ for oppdaterte varslingspunkter til NSM **Husk graderingsmerke**

Nasjonal sikkerhetsmyndighet

Postboks 814
1306 Sandvika

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