# Myndigheten för samhällsskydd och beredskaps föreskrifter om rapportering av incidenter för leverantörer av digitala tjänster

## A. Allmänt

### Beskrivning av problemet och vad man vill uppnå

Centrala samhällstjänster är i hög utsträckning digitaliserade. Nya sätt att hantera, lagra och kommunicera information medför nya möjligheter men också nya risker. Förekomsten av sårbarheter i nätverk och informationssystem, ökad it-relaterad brottslighet och det förändrade samhällsläget skapar ett stort behov av att arbeta systematiskt med informationssäkerhet samt skapa en samlad bild av inträffade incidenter. Incidenter kan hindra genomförandet av ekonomisk verksamhet, generera omfattande ekonomiska förluster och undergräva användarnas förtroende för tjänsterna. Samhället behöver bli bättre i arbetet med informations- och cybersäkerhet.

I syfte att skapa tillit till digital hantering av information och på det sättet förbättra den inre marknadens funktion antog Europaparlamentet och rådet NIS-direktivet, Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverk och informationssystem i hela unionen.

Genom NIS-direktivet ska en hög gemensam nivå av säkerhet i nätverk och informationssystem inom unionen uppnås. Direktivet innebär att leverantörer av samhällsviktiga och digitala tjänster ska vidta säkerhetsåtgärder i nätverk och informationssystem samt rapportera incidenter. Med digitala tjänster avses internetbaserade marknadsplatser, internetbaserade sökmotorer och molntjänster. Säkerhetskrav och krav på vilka incidenter som ska rapporteras regleras gemensamt på EU-nivå i Kommissionens genomförandeförordning (EU) 2018/151 av den 30 januari 2018 om tillämpningsföreskrifter för Europaparlamentets och rådets direktiv (EU) 2016/1148 om åtgärder för en hög gemensam nivå på säkerhet i nätverk och informationssystem i hela unionen. I förordningen specificeras de aspekter som ska beaktas av leverantörer av digitala tjänster när de hanterar risker som hotar säkerheten i deras nät- och informationssystem samt parametrarna för fastställande av om

en incident har avsevärd inverkan och därmed är rapporteringspliktig. EU:s medlemsländer får inte införa ytterligare säkerhets- eller rapporteringskrav för leverantörer av digitala tjänster.

I Sverige implementeras NIS-direktivet genom en ny lag, lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster, förordning (2018: 1175) om informationssäkerhet för samhällsviktiga och digitala tjänster, myndighetsföreskrifter utfärdade av Myndigheten för samhällsskydd och beredskap samt där så behövs sektorsspecifika föreskrifter utfärdade av respektive tillsynsmyndighet avseende säkerhetsåtgärder

Myndigheten för samhällsskydd och beredskap (MSB) utfärdar närmare föreskrifter och allmänna råd om anmälan och identifiering av leverantörer av samhällsviktiga tjänster, systematiskt och riskbaserat informationssäkerhetsarbete och incidentrapportering för leverantörer av samhällsviktiga tjänster respektive digitala tjänster samt frivillig rapportering av incidenter i tjänster som är viktiga för samhällets funktionalitet.

I denna författning, Myndigheten för samhällsskydd och beredskaps föreskrifter om rapportering av incidenter för leverantörer av digitala tjänster, tydliggörs kraven avseende vad, när och hur incidentrapportering till MSB ska ske.

## Beskrivning av alternativa lösningar för det man vill uppnå och vilka effekterna blir om någon reglering inte kommer till stånd

NIS-direktivet ska implementeras i Sverige. Sverige har valt att införa NIS-direktivet genom en ny lag (2018:1174) och en ny förordning (2018:1175) som omfattar alla berörda sektorer. Kraven i lag och förordning kan förtydligas genom myndighetsföreskrifter. Kommissionen har antagit en genomförandeförordning som ytterligare specificera vilka hänsyn som ska tas när leverantörer av digitala tjänster vidtar tekniska och organisatoriska åtgärder för att hantera risker som hotar säkerheten i nätverk och informationssystem samt vad avsevärd inverkan innebär och därmed vilka incidenter som ska rapporteras. Genomförandeförordningen gäller direkt i Sverige.

I betänkandet SOU 2017:36 förs ett resonemang rörande möjligheten att implementera NIS-direktivet genom att göra tillägg i respektive sektors reglering. Utredningen konstaterade dock att detta förutsätter ett omfattande kartläggningsarbete samt att regleringen riskerar att bli oöverskådlig och rörig. Utredningen ansåg att fördelarna med ett samlat regelverk bland annat är att det blir tydligt för samtliga berörda vilken reglering som finns avseende samhällsviktiga tjänster och digitala tjänster, lagstiftningen blir heltäckande

och ingen tjänst riskerar att bli utan reglering. Beslutad lag och förordning inklusive kommande myndighetsföreskrifter utgör ett sådant samlat regelverk.

Enligt förordning (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster ska MSB årligen till EU:s samarbetsgrupp lämna en sammanfattande rapport om de rapporter som mottagits i enlighet med lag (2018:1174). Samarbetsgruppen består av företrädare för medlemsstaterna, kommissionen och Europeiska unionens byrå för nät- och informationssäkerhet (Enisa). Den sammanfattande rapporten ska innehålla antalet rapporter, rapporterade incidenters art samt vilka åtgärder som vidtagits.

Ett system för it-incidentrapportering ska enligt NIS-regleringen kunna användas för att varna andra och därigenom minska konsekvenser av inträffade incidenter. Det ska även utgöra underlag för analyser och bidra till en samlad lägesbild över tid när det gäller informationssäkerhet. Detta ger ökad möjlighet att återkoppla relevant information och stöd till berörda aktörer och inrikta förebyggande insatser. För att systemet ska kunna användas på avsett sätt och för att Sverige ska kunna uppfylla sina skyldigheter gentemot EU behövs en tydlig struktur som klargör vad som ska rapporteras, när och hur. Det är således centralt att kraven blir bindande och tydliggörs i form av myndighetsföreskrifter. Avsaknad av sådana bindande krav bedöms resultera i allt för stor otydlighet om hur en leverantör ska uppfylla rapporteringsplikten, vilket kan leda till en ojämn och sporadisk rapportering där inlämnad information inte kan ligga till grund för utformning av nödvändigt stöd och analyser. Det blir även svårare att säkerställa att skyldigheten att tillhanda information till EU och andra medlemsstater kan uppfyllas. Otydligheten försvårar även tillsynen.

### Uppgifter om vilka som berörs av regleringen

Föreskrifterna berör juridiska personer som tillhandahåller en digital tjänst och som har sitt huvudsakliga etableringsställe i Sverige eller har utsett en företrädare som är etablerad här. Totalt rör det sig om ca 90 leverantörer fördelat på internetbaserade marknadsplatser, internetbaserade sökmotorer samt molntjänster.

I rapporten "Digitala tjänster i Sverige" med dnr MSB 2017-07148, som är en delleverans till regeringsuppdrag Ju2017/05786/L4, redovisas en kartläggning av vilka digitala tjänster enligt bilaga 3 i direktivet 2016/1148/EU som finns i Sverige. NIS-direktivets indelning och beskrivning av digitala tjänster motsvarar inte någon etablerad indelning på den svenska digitala marknaden idag. Det är sannolikt att det finns digitala tjänster på den svenska marknaden som berörs av regleringen, men som inte kunde identifieras i den initiala kartläggningen. Dessutom förändras marknaden för digitala tjänster, och de branscher som verkar på den, fort. Det kan innebära att resultaten i MSB:s

rapport har en begränsad livslängd, och att undersökningen därför kan komma att behöva genomföras igen.

### Uppgifter om de bemyndiganden som myndighetens beslutanderätt grundar sig på

Bemyndigandet grundar sig på 13 och 14 §§ i förordning (2018:1175) om informationssäkerhet för vissa tillhandahållare av samhällsviktiga och digitala tjänster.

### Uppgifter om vilka kostnadsmässiga och andra konsekvenser regleringen medför och en jämförelse av konsekvenserna för de övervägda regleringsalternativen

Kostnader för leverantörer av digitala tjänster bör bedömas i ett helhetsperspektiv tillsammans Kommissionens genomförandeförordning (EU) 2018/151, särskilt vad gäller krav på säkerhetsaspekter avseende incidenthantering. Tillsammans med förordningen kommer leverantörer på längre sikt att minska sin risk för störningar och därmed kunna erbjuda mer stabila leveranser och höja sin konkurrenskraft.

För de leverantörer som inte bedriver ett systematiskt och riskbaserat arbete idag kan krav i föreskrifterna initialt ge obetydligt ökade kostnader. De flesta leverantörer torde dock redan i dag arbeta med informationssäkerhet på något sätt. Kravet på incidentrapportering kan för flertalet leverantörer vara en ny uppgift och därmed ge upphov till nya kostnader. Dessa bedöms infalla främst i det initiala uppbyggnadsskedet i form av administrativa kostnader då anpassning av processer och rutiner kan behöva ske. MSB arbetar med att ta fram ett tekniskt gränssnitt för incidentrapportering. Detta kommer att underlätta för leverantörer att rapportera incidenter.

Föreskriftskravet att initial notifiering ska ske inom sex timmar efter att leverantören har identifierat en incident som rapporteringspliktig och uppföljande rapportering inom 24 timmar ska inte tolkas som krav på ökad bemanning. Tidsfristen räknas från den tidpunkt då leverantören med stöd av sina interna processer och rutiner upptäcker incidenten. Bedömningen är att incidentrapportering bör ske efter att de första kritiska åtgärderna för att avhjälpa incidenten har vidtagits. Vidare är den mängd information som ska lämnas inom sex timmar och även anvisade kontaktvägar anpassade efter skyndsamhetskravet.

Tidsfristen på sex timmar är framtagen med anledning av möjligheten för CERT-SE (Sveriges Computer Emergency Response Team) att vid behov och när så är möjligt hjälpa leverantören med incidenten. I och med kravet på initial notifiering på sex timmar och sedan uppföljande rapportering inom 24 timmar kan CERT-SE och MSB skapa en samlad lägesbild. Vid inrapporterad incident bedömer CERT-SE om det finns behov av att agera på incidenten.

Därefter inleds eventuellt incidenthantering som bland annat kan innebära kontakt med rapporterande leverantör och andra drabbade, sökning bland tillgänglig information och hos CERT-SE:s kontaktnät, informera allmänheten eller samordna åtgärder, informera andra aktörer, såväl nationellt som internationellt. MSB ska, för Sveriges räkning, informera övriga medlemsstater om gränsöverskridande incidenter. Inkomna rapporter vidarebefordras skyndsamt till berörd tillsynsmyndighet. Enligt MSB:s bedömning kommer inte tidskraven att föranleda att leverantörerna drabbas av ökade kostnader i någon större utsträckning annat än i det initiala uppbyggnadsskedet.

För samhällsekonomin kommer den ökade tillförlitligheten som ett systematiskt arbete med informationssäkerhet ger vara viktig. Sveriges stora beroende av nätverk och informationssystem gör att brister får större inverkan på samhället och samhällsekonomin. Brister i informationshanteringen, oavsett orsak, kan ge omfattande ekonomisk skada, undergräva användarnas förtroende för tjänsterna och medföra stor samhällspåverkan. Incidentrapporteringen är en åtgärd för att förebygga och minimera verkningar av incidenter för att säkerställa kontinuiteten i de digitala tjänsterna.

### Bedömning av om regleringen överensstämmer med eller går utöver de skyldigheter som följer av Sveriges anslutning till Europeiska unionen

Bedömningen är att föreskrifterna överensstämmer med de skyldigheter som följer av Sveriges medlemskap i Europeiska unionen.

### Bedömning av om särskilda hänsyn behöver tas när det gäller tidpunkten för ikraftträdande och om det finns behov av speciella informationsinsatser

Direktivet börjar gälla från den 10 maj 2018, lag och förordning träder i kraft 1 augusti samma år. Från och med 1 augusti ska leverantörer av digitala tjänster rapportera sådana incidenter som specificeras i Kommissionens genomförandeförordning (EU) 2018/151. Dessa föreskrifter som specificeras hur och när incidenter ska rapporteras behöver därför träda ikraft så snart som möjligt efter detta datum. Med hänsyn till remiss och beredningsprocess bedöms ikraftträdande kunna ske under sista kvartalet 2018.

De leverantörer som berörs av föreskrifterna kommer att behöva informeras genom speciella informationsinsatser som koordineras med respektive tillsynsmyndighet.

# B. Kommuner och landsting

*Markera med x*

(X) Regleringen bedöms inte få effekter för kommuner eller landsting.

( ) Regleringen bedöms få effekter för kommuner eller landsting.

### Beskrivning av effekter för kommuner eller landsting

# C. Företag

Med företag avses här en juridisk eller en fysisk person som bedriver näringsverksamhet, det vill säga försäljning av varor och/eller tjänster yrkesmässigt och självständigt. Att yrkesmässigt bedriva näringsverksamhet bör tolkas brett.

*Markera med x*

( ) Regleringen bedöms inte få effekter av betydelse för företags arbetsförutsättningar, konkurrensförmåga eller villkor i övrigt. Konsekvensutredningen innehåller därför inte någon beskrivning av punkterna i avsnitt C.

( X ) Regleringen bedöms få effekter av betydelse för företags arbetsförutsättningar, konkurrensförmåga eller villkor i övrigt. Konsekvensutredningen innehåller därför en beskrivning av punkterna i avsnitt C.

### Beskrivning av antalet företag som berörs, vilka branscher företagen är verksamma i samt storleken på företagen

Se avsnitt "Uppgifter om vilka som berörs av regleringen" samt rapporten "Digitala tjänster i Sverige" med dnr MSB 2017-07148.

### Beskrivning av vilken tidsåtgång regleringen kan föra med sig för företagen och vad regleringen innebär för företagens administrativa kostnader.

Förmåga att identifiera och rapportera incidenter till MSB i enlighet med regleringen på området förutsätter att leverantören av digitala tjänster har rutiner för intern incidenthantering. Befintliga arbetsprocesser och rutiner behöver sannolikt anpassas för att stämma överens med föreskrifterna och för att underlätta användning av MSB:s tekniska gränssnitt för rapportering. Tillkommande administrativa kostnader för extern rapportering bedöms inte tillföra några omfattande kostnader. Särskilt då det inte är alla incidenter som ska rapporteras, utan endast de som bedöms ha en avsevärd inverkan på

tillhandahållandet av en digital tjänst som leverantören erbjuder inom EU. De företag som behöver bygga upp sin interna incidenthantering från grunden kommer att behöva tillföra resurser för detta.

### Beskrivning av vilka andra kostnader den föreslagna regleringen medför för företagen och vilka förändringar i verksamheten som företagen kan behöva vidta till följd av den föreslagna regleringen

För de leverantörer som inte bedriver ett systematiskt och riskbaserat arbete idag som möjliggör extern rapportering av incidenter kan kraven i föreskrifterna initialt ge obetydligt ökade kostnader då befintliga arbetsprocesser och rutiner behöver sannolikt anpassas för att stämma överens med föreskrifterna och underlätta användning av MSB:s tekniska gränssnitt för rapportering. De flesta leverantörer torde redan i dag arbeta med informationssäkerhet på något sätt.

### Beskrivning av i vilken utsträckning regleringen kan komma att påverka konkurrensförhållandena för företagen

Ett av syftena med regleringen är att säkerställa att leverantörer får förutsättningar för att konkurrera på lika villkor genom att leverantörer av digitala tjänster arbetar utifrån samma krav avseende säkerhet (regleras i artikel 2 Kommissionens genomförandeförordning (EU) 2018/151,) och incidentrapportering Detta motverkar att en leverantör erbjuder en tjänst till lägre pris för att därefter ta ut extra kostnader från sina kunder när leveransen på grund av bristande informationssäkerhet inte fungerar. De leverantörer av digitala tjänster som idag arbetar systematiskt och riskbaserat få därmed en mer rättvis konkurrenssituation. Kravet på incidentrapportering är lika för leverantörerna. Leverantörer som drabbas av många incidenter måste naturligtvis i högre grad rapportera till myndigheterna.

### Beskrivning av hur regleringen i andra avseenden kan komma att påverka företagen

Rapportering medför att CERT-SE vid behov och när så är möjligt kan hjälpa leverantören med incidenten. Leverantören kan även få hjälp av MSB att vid behov hantera de störningar som incidenten medför i den samhällsviktiga tjänsten. Leverantörer kan också få varningar när andra leverantörer rapporterar om incidenter, som kan få påverkan på andra leverantörer och på så sätt kunna vidta åtgärder i tid.
Den kunskapsbank som MSB kan bygga upp tack vare incidentrapporteringen och analyser som genomförs av informationen ger underlag till utvecklingen av råd och stöd som kan förmedlas till leverantörerna

### Beskrivning av om särskilda hänsyn behöver tas till små företag vid reglernas utformning

Ingen särskild hänsyn har tagits till små företag i föreskrifterna. Dessa bedöms endast i undantagsfall beröras av regleringen.

## D. Samråd

### Beskrivning av ett eventuellt tidigt samråd

I syfte att få underlag till utformningen av regleringen har tillsynsmyndigheten vid ett flertal tillfällen fått lämna synpunkter på tidiga utkast på föreskrifter och allmänna råd. Tillsynsmyndigheten har stor kunskap inom sin sektor och har kunnat bidra med värdefulla synpunkter.

Något formellt samråd med direkt berörda leverantörer av digitala tjänster har inte genomförts.

## E. Kontaktpersoner

### Ange vem som kan kontaktas vid eventuella frågor

Kontaktperson för konsekvensutredningen gällande föreskrifter om rapportering av incidenter för leverantörer av samhällsviktiga tjänster är Carina Wetzel som lämpligas nås på carina.wetzel@msb.se
eller 010-240 42 62.