Svensk författningssamling

Förordning om informationssäkerhet för samhällsviktiga och digitala tjänster

SFS 2018:1175
Publicerad
den 27 juni 2018

Utfärdad den 20 juni 2018

Regeringen föreskriver[1] följande.

Inledande bestämmelse

1 § Denna förordning kompletterar lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster och 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 nätverks- och informationssystem i hela unionen vad gäller närmare specificering av 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, här kallad kommissionens genomförandeförordning om leverantörer av digitala tjänster.

Uttryck i förordningen

2 § Uttryck som används i förordningen har samma innebörd som i lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster.

I denna förordning avses med

1. *standard*: en standard i den mening som avses i artikel 2.1 i Europaparlamentets och rådets förordning (EU) nr 1025/2012 av den 25 oktober 2012 om europeisk standardisering och om ändring av rådets direktiv 89/686/EEG och 93/15/EEG samt av Europaparlamentets och rådets direktiv 94/9/EG, 94/25/EG, 95/16/EG, 97/23/EG, 98/34/EG, 2004/22/EG, 2007/23/EG, 2009/23/EG och 2009/105/EG samt om upphävande av rådets beslut 87/95/EEG och Europaparlamentets och rådets beslut 1673/2006/EG,
2. *specifikation*: en teknisk specifikation i den mening som avses i artikel 2.4 i Europaparlamentets och rådets förordning (EU) nr 1025/2012, och
3. *CSIRT-enhet*: Sveriges enhet för hantering av incidenter som rapporteras enligt Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen (NIS-direktivet).

[1] Jfr Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen, i den ursprungliga lydelsen.

3 § Myndigheten för samhällsskydd och beredskap får, efter att ha gett tillsynsmyndigheterna och Socialstyrelsen tillfälle att yttra sig, meddela föreskrifter om vilka tjänster som är samhällsviktiga tjänster enligt lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster. Föreskrifterna ska uppdateras minst vartannat år.

Betydande störning i kontinuiteten i en samhällsviktig tjänst

4 § Vid bedömningen av vad som avses med en betydande störning enligt 3 § första stycket 1 lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster ska följande sektorsöverskridande faktorer beaktas:

1. antalet användare som är beroende av den tjänst som den berörda leverantören tillhandahåller,
2. hur beroende andra sektorer som omfattas av NIS-direktivet är av den tjänst som leverantören tillhandahåller,
3. vilken inverkan incidenter skulle kunna ha på ekonomisk och samhällelig verksamhet eller allmän säkerhet, uttryckt i grad och varaktighet,
4. leverantörens marknadsandel,
5. hur stort geografiskt område som skulle kunna påverkas av en incident, och
6. leverantörens betydelse för upprätthållandet av en tillräcklig tjänstenivå, med hänsyn tagen till alternativa sätt för att tillhandahålla tjänsten.

När det är lämpligt ska även sektorsspecifika faktorer beaktas.

Myndigheten för samhällsskydd och beredskap får, efter att ha gett tillsynsmyndigheterna och Socialstyrelsen tillfälle att yttra sig, meddela ytterligare föreskrifter om vad som avses med en betydande störning.

Säkerhetsåtgärder

Standarder och specifikationer

5 § Vid utformningen av säkerhetsåtgärder ska leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster beakta europeiska och internationellt accepterade standarder och specifikationer.

Tekniska och organisatoriska åtgärder

6 § Vid bedömningen av om säkerhetsåtgärder enligt 15 § lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster säkerställer en nivå på säkerheten i nätverk och informationssystem som är lämplig i förhållande till risken, ska följande beaktas:

1. säkerheten i system och anläggningar,
2. incidenthantering,
3. hantering av driftskontinuitet,
4. övervakning, revision och testning, och
5. efterlevnad av internationella standarder.

I artikel 2 i kommissionens genomförandeförordning om leverantörer av digitala tjänster finns bestämmelser som närmare anger vad som avses med första stycket punkt 1–5.

Ytterligare föreskrifter om säkerhetsåtgärder

7 § Myndigheten för samhällsskydd och beredskap får, efter att ha gett tillsynsmyndigheterna och Socialstyrelsen tillfälle att yttra sig, meddela föreskrifter om systematiskt och riskbaserat informationssäkerhetsarbete

enligt 11 § lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster.

8 § Statens energimyndighet, Transportstyrelsen, Finansinspektionen, Livsmedelsverket och Post- och telestyrelsen får meddela föreskrifter om säkerhetsåtgärder enligt 12–14 §§ lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster för sina respektive tillsynsområden. Socialstyrelsen får meddela sådana föreskrifter för Inspektionen för vård och omsorgs tillsynsområde. Innan föreskrifterna meddelas ska Myndigheten för samhällsskydd och beredskap ges tillfälle att yttra sig.

Myndigheten för samhällsskydd och beredskap ska lämna råd och stöd till tillsynsmyndigheterna och Socialstyrelsen när de tar fram föreskrifterna.

Incidentrapportering

Betydande inverkan på kontinuiteten i en samhällsviktig tjänst

9 § Vid bedömningen av om en incident har en betydande inverkan på kontinuiteten i en samhällsviktig tjänst enligt 18 § lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster ska följande särskilt beaktas:

1. det antal användare som påverkas av störningen i den samhällsviktiga tjänsten,
2. hur länge incidenten varar, och
3. hur stort geografiskt område som påverkas av incidenten.

Myndigheten för samhällsskydd och beredskap får, efter att ha gett tillsynsmyndigheterna och Socialstyrelsen tillfälle att yttra sig, meddela ytterligare föreskrifter om vad som avses med en betydande inverkan.

Avsevärd inverkan på tillhandahållandet av en digital tjänst

10 § Vid bedömningen av om en incident har en avsevärd inverkan på tillhandahållandet av en digital tjänst enligt 19 § lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster ska följande särskilt beaktas:

1. det antal användare som påverkas av incidenten, framför allt användare som är beroende av tjänsten för att kunna tillhandahålla sina egna tjänster,
2. hur länge incidenten varar,
3. hur stort geografiskt område som påverkas av incidenten,
4. i vilken utsträckning incidenten stör tjänstens funktion, och
5. i vilken utsträckning incidenten påverkar den ekonomiska och samhälleliga verksamheten.

I artiklarna 3 och 4 i kommissionens genomförandeförordning om leverantörer av digitala tjänster finns ytterligare bestämmelser om vad som anses utgöra en avsevärd inverkan.

Leverantörer av digitala tjänster är endast skyldiga att rapportera incidenter om de har tillgång till sådan information som behövs för att bedöma om en incident har en avsevärd inverkan.

Till vilken myndighet incidentrapportering ska göras

11 § Incidentrapportering enligt lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster ska göras till CSIRT-enheten.

12 § Myndigheten för samhällsskydd och beredskap är CSIRT-enhet.

CSIRT-enheten ska

1. ta emot incidentrapporter som lämnas enligt lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster eller enligt föreskrifter som har meddelats i anslutning till den lagen,
2. utan dröjsmål tillgängliggöra informationen i incidentrapporter för tillsynsmyndigheterna och Socialstyrelsen, och
3. skyndsamt uppmana leverantörer att till Polismyndigheten anmäla incidenter som kan antas ha sin grund i en brottslig gärning.

CSIRT-enheten ska även uppfylla de krav och fullgöra de uppgifter som framgår av bilaga 1 till NIS-direktivet samt i vissa fall informera rapporterande leverantörer, andra medlemsstater och allmänheten om incidenter enligt artiklarna 14.5, 14.6, 16.6 och 16.7 i NIS-direktivet.

Innehållet i en incidentrapport

13 § En incidentrapport ska innehålla information som gör det möjligt för CSIRT-enheten att fastställa omfattningen av incidentens gränsöverskridande verkningar.

Myndigheten för samhällsskydd och beredskap får, efter att ha gett tillsynsmyndigheterna och Socialstyrelsen tillfälle att yttra sig, meddela ytterligare föreskrifter om vilken information en incidentrapport ska innehålla.

Verkställighetsföreskrifter om incidentrapportering

14 § Myndigheten för samhällsskydd och beredskap får meddela närmare föreskrifter om inom vilken tid incidentrapportering ska göras och de närmare formerna för rapporteringen enligt 18 och 19 §§ lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster.

Frivillig rapportering av incidenter

15 § Myndigheten för samhällsskydd och beredskap får, efter att ha gett tillsynsmyndigheterna och Socialstyrelsen tillfälle att yttra sig, meddela föreskrifter om frivillig rapportering av incidenter enligt artikel 20 i NIS-direktivet för leverantörer som inte är leverantörer av samhällsviktiga tjänster eller leverantörer av digitala tjänster.

Anmälningsskyldighet för leverantörer av samhällsviktiga tjänster

16 § Myndigheten för samhällsskydd och beredskap får, efter att ha gett tillsynsmyndigheterna tillfälle att yttra sig, meddela närmare föreskrifter om anmälningsskyldigheten enligt 23 § lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster. Föreskrifterna får avse när i tiden en anmälan ska ske, vilken information en anmälan ska innehålla och de närmare formerna för fullgörandet av anmälningsskyldigheten.

Tillsyn

Tillsynsmyndigheter

17 § Följande myndigheter är, för angivna sektorer, tillsynsmyndigheter för leverantörer av samhällsviktiga tjänster enligt lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster:

Tillsynsmyndighet	*Sektor*
Statens energimyndighet	Energi
Transportstyrelsen	Transport
Finansinspektionen	Bankverksamhet
Finansinspektionen	Finansmarknadsinfrastruktur
Inspektionen för vård och omsorg	Hälso- och sjukvård
Livsmedelsverket	Leverans och distribution av dricksvatten
Post- och telestyrelsen	Digital infrastruktur

18 § Post- och telestyrelsen är tillsynsmyndighet för leverantörer av digitala tjänster enligt lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster.

Tillsynsmyndigheternas uppgifter

19 § Tillsynsmyndigheterna ska, för sina respektive tillsynsområden,

1. utan dröjsmål lämna uppgifter till Myndigheten för samhällsskydd och beredskap om innehållet i anmälningar som har gjorts enligt 23 § lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster,
2. senast den 20 september vartannat år med start 2020 ge Myndigheten för samhällsskydd och beredskap uppgifter om de leverantörer av samhällsviktiga tjänster som myndigheten har tillsyn över, fördelat på de sektorer och delsektorer som anges i bilaga 2 till NIS-direktivet, samt uppgifter om leverantörernas betydelse för dessa sektorer,
3. inom ramen för sin tillsyn ge allmän vägledning vid tillämpningen av lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster och av föreskrifter som har meddelats i anslutning till den lagen,
4. samarbeta med Datainspektionen vid hantering av incidenter som även utgör personuppgiftsincidenter,
5. lämna stöd till Sveriges representant i den samarbetsgrupp som har inrättats genom artikel 11 i NIS-direktivet, och
6. samarbeta med och bistå tillsynsmyndigheter i andra medlemsstater inom Europeiska unionen när det gäller juridiska personer som tillhandahåller digitala tjänster och som har sitt huvudsakliga etableringsställe eller har utsett företrädare i andra medlemsstater.

Begäran om information

20 § När en tillsynsmyndighet begär information enligt 24 § lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster ska tillsynsmyndigheten ange syftet med begäran och precisera vilken information som krävs.

Samarbetsforum för en effektiv och likvärdig tillsyn

21 § Myndigheten för samhällsskydd och beredskap ska leda ett samarbetsforum där tillsynsmyndigheterna och Socialstyrelsen ingår. Syftet med forumet ska vara att underlätta samordning och åstadkomma en effektiv och likvärdig tillsyn.

Nationell kontaktpunkt

22 § Myndigheten för samhällsskydd och beredskap är gemensam nationell kontaktpunkt enligt NIS-direktivet.

Den nationella kontaktpunkten ska fullgöra de uppgifter som framgår av artiklarna 8.4, 10.3 andra stycket och 14.5 tredje stycket i NIS-direktivet.

Den nationella kontaktpunkten ska även fullgöra Sveriges skyldighet enligt artikel 5.4 i NIS-direktivet att samråda med andra medlemsstater samt rapportera resultatet av samrådet till berörd tillsynsmyndighet.

Grupp för samarbete mellan medlemsstaterna

23 § Myndigheten för samhällsskydd och beredskap är Sveriges representant i den samarbetsgrupp som har inrättats genom artikel 11 i NIS-direktivet.

Information till kommissionen

24 § Myndigheten för samhällsskydd och beredskap ska fullgöra Sveriges skyldighet enligt artikel 5.7 i NIS-direktivet att tillhandahålla information om genomförandet av NIS-direktivet till kommissionen.

Denna förordning träder i kraft den 1 augusti 2018.

På regeringens vägnar

MORGAN JOHANSSON

Ida Wettervik
(Justitiedepartementet)