Svensk författningssamling

Lag om informationssäkerhet för samhällsviktiga och digitala tjänster

SFS 2018:1174
Publicerad
den 27 juni 2018

Utfärdad den 20 juni 2018

Enligt riksdagens beslut[1] föreskrivs[2] följande.

Syftet med lagen

1 § Syftet med denna lag är att uppnå en hög nivå på säkerheten i nätverk och informationssystem för

1. samhällsviktiga tjänster inom sektorerna
– energi,
– transport,
– bankverksamhet,
– finansmarknadsinfrastruktur,
– hälso- och sjukvård,
– leverans och distribution av dricksvatten,
– digital infrastruktur, och
2. digitala tjänster.

Uttryck i lagen

2 § I lagen avses med

1. *nätverk och informationssystem*:

a) ett elektroniskt kommunikationsnät enligt 1 kap. 7 § lagen (2003:389) om elektronisk kommunikation,

b) en enhet eller en grupp enheter som är sammankopplade eller hör samman med varandra, av vilka en eller flera genom ett program utför automatisk behandling av digitala uppgifter, eller

c) digitala uppgifter som lagras, behandlas, hämtas eller överförs med sådana hjälpmedel som omfattas av a och b för att de ska kunna driftas, användas, skyddas och underhållas,

2. *säkerhet i nätverk och informationssystem*: nätverks och informationssystems förmåga att vid en viss tillförlitlighetsnivå motstå åtgärder som undergräver tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten hos lagrade, överförda eller behandlade uppgifter eller hos de besläktade tjänster som erbjuds genom eller är tillgängliga via dessa nätverk och informationssystem,

3. *samhällsviktig tjänst*: en tjänst som är viktig för att upprätthålla kritisk samhällelig eller ekonomisk verksamhet,

[1] Prop. 2017/18:205, bet. 2017/18:FöU14, rskr. 2017/18:375.
[2] 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.

4. *digital tjänst*: en tjänst i den mening som avses i artikel 1.1 b i Europaparlamentets och rådets direktiv (EU) 2015/1535 av den 9 september 2015 om ett informationsförfarande beträffande tekniska föreskrifter och beträffande föreskrifter för informationssamhällets tjänster, och som utgör en internetbaserad marknadsplats, internetbaserad sökmotor eller molntjänst,

5. *internetbaserad marknadsplats*: en tjänst som gör det möjligt för konsumenter eller näringsidkare enligt definitionen i artikel 4.1 a respektive 4.1 b i Europaparlamentets och rådets direktiv 2013/11/EU av den 21 maj 2013 om alternativ tvistlösning vid konsumenttvister och om ändring av förordning (EG) nr 2006/2004 och direktiv 2009/22/EG (direktivet om alternativ tvistlösning) att ingå internetbaserade köpeavtal eller tjänsteavtal med näringsidkare, antingen på webbplatsen för den internetbaserade marknadsplatsen eller på en webbplats som tillhör en näringsidkare och där datatjänster som tillhandahålls av en internetbaserad marknadsplats används,

6. *internetbaserad sökmotor*: en tjänst som gör det möjligt för användare att göra sökningar på i princip alla webbplatser eller webbplatser på ett visst språk genom en förfrågan om vilket ämne som helst i form av ett nyckelord, en fras eller någon annan inmatning, och som returnerar länkar som innehåller information om det begärda innehållet,

7. *molntjänst*: en tjänst som möjliggör tillgång till en skalbar och elastisk pool av delbara dataresurser,

8. *NIS-direktivet*: 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,

9. *företrädare*: en fysisk eller juridisk person som uttryckligen har utsetts att agera för en leverantör och till vilken myndigheter kan vända sig, i stället för till leverantören, i frågor som gäller de skyldigheter som leverantören har enligt NIS-direktivet,

10. *incident*: en händelse med en faktisk negativ inverkan på säkerheten i nätverk och informationssystem, och

11. *risk*: en rimligen identifierbar omständighet eller händelse med en potentiell negativ inverkan på säkerheten i nätverk och informationssystem.

Lagens tillämpningsområde

3 § Lagen gäller för

1. leverantörer av det slag som anges i bilaga 2 till NIS-direktivet och som tillhandahåller en samhällsviktig tjänst, under förutsättning att leverantören är etablerad i Sverige, att tillhandahållandet av tjänsten är beroende av nätverk och informationssystem och att en incident skulle medföra en betydande störning vid tillhandahållandet av tjänsten (leverantörer av samhällsviktiga tjänster), och

2. juridiska personer som tillhandahåller en digital tjänst och som har sitt huvudsakliga etableringsställe i Sverige eller har utsett en företrädare som är etablerad här (leverantörer av digitala tjänster).

I 10 § finns en bestämmelse som gäller för andra leverantörer.

4 § Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om vilka tjänster som är samhällsviktiga tjänster och vad som avses med en betydande störning enligt 3 § första stycket 1.

Leverantörer av elektroniska kommunikationstjänster

5 § Lagen gäller inte för företag som tillhandahåller allmänna kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster och därför omfattas av kraven i 5 kap. 6 b och c §§ lagen (2003:389) om elektronisk kommunikation.

Leverantörer av betrodda tjänster

6 § Lagen gäller inte för leverantörer av betrodda tjänster som omfattas av kraven i artikel 19 i Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG.

Leverantörer av digitala tjänster som är mikroföretag eller små företag

7 § Lagen gäller inte för leverantörer av digitala tjänster som är mikroföretag eller små företag enligt definitionen i kommissionens rekommendation 2003/361/EG av den 6 maj 2003 om definitionen av mikroföretag samt små och medelstora företag.

Säkerhetskänslig verksamhet

8 § Lagen gäller inte för verksamhet som omfattas av krav på säkerhetsskydd enligt säkerhetsskyddslagen (1996:627).

Leverantörer som omfattas av krav på informationssäkerhet i andra författningar

9 § Om det i lag eller annan författning finns bestämmelser som innehåller krav på säkerhetsåtgärder och incidentrapportering ska de bestämmelserna gälla om verkan av kraven minst motsvarar verkan av skyldigheterna enligt denna lag, med beaktande av bestämmelsernas omfattning samt vilken tillsyn och vilka sanktioner som är kopplade till kraven i bestämmelserna.

Utseende av företrädare

10 § En juridisk person som erbjuder digitala tjänster i Sverige men som inte har sitt huvudsakliga etableringsställe inom Europeiska unionen och inte heller har utsett en företrädare som är etablerad i en medlemsstat där tjänsterna erbjuds, ska, om inte något undantag från lagens tillämpningsområde enligt 5–9 §§ är tillämpligt, utse en sådan företrädare.

Säkerhetsåtgärder

Skyldigheter för leverantörer av samhällsviktiga tjänster

11 § Leverantörer av samhällsviktiga tjänster ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete avseende nätverk och informationssystem som de använder för att tillhandahålla samhällsviktiga tjänster.

12 § Leverantörer av samhällsviktiga tjänster ska göra en riskanalys som ska ligga till grund för val av säkerhetsåtgärder enligt 13 och 14 §§. I analysen ska det ingå en åtgärdsplan. Analysen ska dokumenteras och uppdateras årligen.

13 § Leverantörer av samhällsviktiga tjänster ska vidta ändamålsenliga och proportionella tekniska och organisatoriska åtgärder för att hantera risker som hotar säkerheten i nätverk och informationssystem som de använder för att tillhandahålla samhällsviktiga tjänster. Åtgärderna ska säkerställa en nivå på säkerheten i nätverken och informationssystemen som är lämplig i förhållande till risken.

14 § Leverantörer av samhällsviktiga tjänster ska vidta lämpliga åtgärder för att förebygga och minimera verkningar av incidenter som påverkar nätverk och informationssystem som de använder för att tillhandahålla samhällsviktiga tjänster. Åtgärderna ska syfta till att säkerställa kontinuiteten i tjänsterna.

Skyldigheter för leverantörer av digitala tjänster

15 § Leverantörer av digitala tjänster ska vidta de tekniska och organisatoriska åtgärder som de anser ändamålsenliga och proportionella och som hanterar risker som hotar säkerheten i nätverk och informationssystem som de använder när de tillhandahåller digitala tjänster inom Europeiska unionen. Åtgärderna ska säkerställa en nivå på säkerheten i nätverken och informationssystemen som är lämplig i förhållande till risken.

16 § Leverantörer av digitala tjänster ska vidta åtgärder för att förebygga och minimera verkningar av incidenter som påverkar nätverk och informationssystem som de använder. Skyldigheten gäller endast i förhållande till verkningar som sådana incidenter har på digitala tjänster som leverantören erbjuder inom Europeiska unionen. Åtgärderna ska syfta till att säkerställa kontinuiteten i tjänsterna.

Bemyndigande

17 § Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om säkerhetsåtgärder enligt 11–16 §§.

Incidentrapportering

Rapporteringsskyldighet för leverantörer av samhällsviktiga tjänster

18 § Leverantörer av samhällsviktiga tjänster ska utan onödigt dröjsmål rapportera incidenter som har en betydande inverkan på kontinuiteten i den samhällsviktiga tjänst som de tillhandahåller. Rapporteringen ska göras till den myndighet som regeringen bestämmer.

Rapporteringsskyldighet för leverantörer av digitala tjänster

19 § Leverantörer av digitala tjänster ska utan onödigt dröjsmål rapportera incidenter som har en avsevärd inverkan på tillhandahållandet av en digital tjänst som de erbjuder inom Europeiska unionen. Rapporteringen ska göras till den myndighet som regeringen bestämmer.

Bemyndigande

20 § Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om incidentrapportering enligt 18 och 19 §§.

Tillsynsmyndighetens uppdrag

21 § Den myndighet som regeringen bestämmer ska vara tillsynsmyndighet. Tillsynsmyndigheten ska utöva tillsyn över att denna lag och föreskrifter som har meddelats i anslutning till lagen följs.

22 § Tillsynsåtgärder när det gäller leverantörer av digitala tjänster får vidtas endast när tillsynsmyndigheten har befogad anledning att anta att en leverantör inte uppfyller kraven i 15, 16 eller 19 §.

Anmälningsskyldighet för leverantörer av samhällsviktiga tjänster

23 § Leverantörer av samhällsviktiga tjänster ska utan dröjsmål anmäla sig till tillsynsmyndigheten. Av en anmälan ska det framgå om leverantören tillhandahåller en samhällsviktig tjänst i två eller flera medlemsstater inom Europeiska unionen.

Tillsynsmyndighetens undersökningsbefogenheter

24 § Den som står under tillsyn ska på begäran tillhandahålla tillsynsmyndigheten den information som behövs för tillsynen.

25 § Tillsynsmyndigheten har i den omfattning det behövs för tillsynen rätt att få tillträde till områden, lokaler och andra utrymmen, dock inte bostäder, som används i verksamhet som omfattas av lagen.

26 § Tillsynsmyndigheten får förelägga den som står under tillsyn att tillhandahålla information och ge tillträde enligt 24 och 25 §§.

Ett sådant föreläggande får förenas med vite.

27 § Tillsynsmyndigheten får begära handräckning av Kronofogdemyndigheten för att genomföra de åtgärder som avses i 24 och 25 §§. Vid handräckning gäller bestämmelserna i utsökningsbalken om verkställighet av förpliktelser som inte avser betalningsskyldighet, avhysning eller avlägsnande.

Ingripanden och sanktioner

Åtgärdsförelägganden

28 § Tillsynsmyndigheten får meddela de förelägganden som behövs för att leverantörer ska uppfylla kraven på utseende av företrädare, säkerhetsåtgärder och incidentrapportering enligt 10, 12–16, 18 och 19 §§ och enligt föreskrifter som har meddelats i anslutning till de paragraferna.

Ett sådant föreläggande får förenas med vite.

Sanktionsavgift

29 § Tillsynsmyndigheten ska ta ut en sanktionsavgift av den som underlåter att

1. göra en anmälan till tillsynsmyndigheten enligt 23 § eller enligt föreskrifter som har meddelats i anslutning till den paragrafen,
2. vidta säkerhetsåtgärder enligt någon av 12–16 §§ eller enligt föreskrifter som har meddelats i anslutning till de paragraferna, eller
3. rapportera incidenter enligt 18 eller 19 § eller enligt föreskrifter som har meddelats i anslutning till de paragraferna.

30 § En sanktionsavgift ska bestämmas till lägst 5 000 kronor och högst 10 000 000 kronor.

31 § När sanktionsavgiftens storlek bestäms ska särskild hänsyn tas till den skada eller risk för skada som uppstått till följd av överträdelsen, om leverantören tidigare har begått en överträdelse och de kostnader som leverantören har undvikit till följd av överträdelsen.

32 § En sanktionsavgift får efterges helt eller delvis om överträdelsen är ringa eller ursäktlig eller om det annars med hänsyn till omständigheterna skulle vara oskäligt att ta ut avgiften.

33 § En sanktionsavgift får inte beslutas om överträdelsen omfattas av ett föreläggande om vite och överträdelsen ligger till grund för en ansökan om utdömande av vitet.

34 § En sanktionsavgift får endast beslutas om den som avgiften ska tas ut av har fått tillfälle att yttra sig inom två år från det att överträdelsen ägde rum.

Ett beslut om sanktionsavgift ska delges.

35 § En sanktionsavgift ska betalas till tillsynsmyndigheten inom 30 dagar från det att beslutet om att ta ut avgiften har fått laga kraft eller inom den längre tid som anges i beslutet.

Om sanktionsavgiften inte betalas inom den tid som anges i första stycket, ska myndigheten lämna den obetalda avgiften för indrivning. Bestämmelser om indrivning finns i lagen (1993:891) om indrivning av statliga fordringar m.m. Vid indrivning får verkställighet ske enligt utsökningsbalken.

En sanktionsavgift tillfaller staten.

36 § En beslutad sanktionsavgift faller bort till den del beslutet om avgiften inte har verkställts inom fem år från det att beslutet fick laga kraft.

Föreskrifter om verkställighet

37 § Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om verkställighet av denna lag.

Förordnande om att beslut ska gälla omedelbart

38 § Tillsynsmyndigheten får bestämma att ett beslut om föreläggande enligt denna lag ska gälla omedelbart.

Överklagande

39 § Tillsynsmyndighetens beslut enligt denna lag får överklagas till allmän förvaltningsdomstol. När ett sådant beslut överklagas är tillsynsmyndigheten motpart i domstolen.

Prövningstillstånd krävs vid överklagande till kammarrätten.

Denna lag träder i kraft den 1 augusti 2018.

YLVA JOHANSSON

MORGAN JOHANSSON
(Justitiedepartementet)