WeTeam AB
par.abelson@weteam.se | 0735-200025

Cybersäkerhetslagen (2025:1506)

En strategisk guide till efterlevnad av NIS2

LAGEN ÄR NU I KRAFT

Fullständigt uppdaterad med lagstiftning, SFS-nummer, tillsynsmyndigheter och regulatorisk kalender

Lagen ikraft	SFS-nummer	Proposition	Tillsynsmyndigheter
15 jan 2026	2025:1506	Prop. 2025/26:28	8 (+6 LST)

Inledning: Lagen gäller nu — vad innebär det?

Den svenska cybersäkerhetslagen (2025:1506) trädde i kraft den 15 januari 2026. Sverige är nu bundet av ett av Europas mest omfattande cybersäkerhetsramverk, implementerat med ett par månaders försening jämfört med EU:s deadline i oktober 2024. Lagen ersätter den tidigare NIS-lagen (2018:1174) och gäller utan övergångstid — efterlevnad krävdes från dag ett.

Sedan det ursprungliga whitepapert publicerades hösten 2025 har det regulatoriska läget förändrats avsevärt. Riksdagen antog lagen den 10 december 2025, MCF (f.d. MSB) öppnade sin registreringsportal den 2 februari 2026, och flertalet tillsynsmyndigheter har publicerat sektorspecifik vägledning. Centrala sekundärföreskrifter om säkerhetsåtgärder och incidentrapportering väntas i april 2026. Det innebär att organisationer befinner sig i ett läge där lagen gäller fullt ut, men delar av det detaljerade regelverket ännu inte fastställts formellt.

> **Viktig uppdatering: MSB byter namn till MCF**
> Den 1 januari 2026 bytte Myndigheten för samhällsskydd och beredskap (MSB) namn till Myndigheten för civilt försvar (MCF). MCF är nu CSIRT-enhet via CERT-SE, nationell samordningspunkt och ansvarig för registreringen av verksamhetsutövare. Alla hänvisningar till 'MSB' i äldre material avser numera MCF.

Det regulatoriska ekosystemet 2026

Cybersäkerhetslagen verkar inte isolerat. Den samspelar med ett antal parallella regelverk som är avgörande att känna till:

- **DORA:** DORA (EU) 2022/2554 — Finansiella entiteter lyder primärt under DORA som lex specialis. Finansinspektionen tillämpar DORA-kraven, inte cybersäkerhetslagens standardkrav.
- **CER:** CER-direktivet — Parallell lagstiftning om fysisk motståndskraft för kritiska entiteter. Många organisationer träffas av båda direktiven och tillsynen är samordnad.
- **Säkerhetsskyddslagen:** Säkerhetsskyddslagen (2018:585) — Verksamhet som regleras av säkerhetsskyddslagen är undantagen från cybersäkerhetslagens tillämpning, för att undvika överlappning vid nationella säkerhetsintressen.

- **EU Implementing Reg:** EU Genomförandeförordning (EU) 2024/2690 — Specificerar incidentrapporteringskriterierna för leverantörer av DNS-tjänster, TLD-register, molntjänster, datacenter m.fl. Gäller sedan november 2024.

Kapitel 1: Det nya lagstiftningsramverket — från förslag till lag

1.1 Lagstiftningens väg från SOU till SFS

Den svenska implementeringsprocessen följde en strukturerad men försenad bana:

1. Kommittédirektiv 2023:30 — Regeringen tillsätter utredningen ledd av Annette Norman i februari 2023.
2. SOU 2024:18 ("Nya regler om cybersäkerhet") — Presenteras mars 2024 och utgör grunden för lagförslaget.
3. Lagrådsremiss — Skickas till Lagrådet i juni 2025.
4. Proposition 2025/26:28 — "Ett starkt skydd för nätverks- och informationssystem – en ny cybersäkerhetslag" överlämnas till riksdagen oktober 2025.
5. Riksdagen antar lagen — 10 december 2025 utan ändringar, trots fem reservationer.
6. Kungörelse — SFS 2025:1506 (lagen) och SFS 2025:1507 (förordningen) utfärdas 11 december 2025 av Försvarsdepartementet.
7. Ikraftträdande — 15 januari 2026.

Sverige var den 19:e EU-medlemsstaten att genomföra NIS2 och mottog en motiverad åsikt från EU-kommissionen i maj 2025 för försenat genomförande. Trots förseningen gäller lagen nu fullt ut.

1.2 Viktiga förändringar jämfört med ursprungsförslaget (SOU 2024:18)

Propositionen innehöll ett antal materiella avvikelser från utredningens förslag som organisationer bör notera:

- **Smalare utbildningskrav:** Utbildningsskyldighet begränsad — Obligatorisk cybersäkerhetsutbildning gäller nu enbart ledningsorgan (styrelse/VD), inte bredare medarbetargrupper som SOU föreslog.
- **Statliga myndigheter:** Offentlig sektor avgränsad — Statliga myndigheter med gränsöverskridande beslutsmandat inkluderas, men inte alla statliga myndigheter.
- **Mjukare personansvar:** Personligt ledningsansvar — Centerpartiet kritiserade propositionen för att ha minskat kraven på ledningen jämfört med SOU. De direkta personliga sanktionerna mot enskilda chefer är kvar, men som en sista utväg.

- **Helhetsprincipen:** Hela-entitets-principen — Lagen gäller hela verksamheten när en organisation väl omfattas, inte bara den NIS2-relevanta affärsdelen.

Kapitel 2: Tillämpningsområde — vem berörs?

2.1 Tillämpningstestet: sektor och storlek

Lagen träffar verksamheter som uppfyller två kriterier: sektortillhörighet och storlek ('size-cap rule'). Lagen täcker 18 sektorer — en kraftig utökning från NIS1:s sju.

Storleksgränsen är uppfylld om organisationen:

- Sysselsätter 50 eller fler personer, eller
- Har en årsomsättning eller balansomslutning som överstiger 10 miljoner euro.

> **Koncernnivå är avgörande**
> Storleksbedömningen görs på koncernnivå. Ett litet svenskt dotterbolag till en global koncern som uppfyller storlekskriterierna omfattas av lagen — oavsett dotterbolagets egna storlek.

Undantag från storleksregeln gäller för verksamheter som är fundamentala för digital infrastruktur och därmed träffas oavsett storlek: leverantörer av allmänna elektroniska kommunikationsnät, betrodda tjänster, toppdomänregistratorer och DNS-tjänster.

2.2 Väsentliga vs. viktiga verksamhetsutövare

Klassificeringen avgör tillsynsregim och sanktionsnivå — inte de grundläggande skyldigheterna, som är desamma för båda kategorierna.

- **Väsentliga:** Väsentliga verksamhetsutövare — Verksamheter i högkritiska sektorer (Bilaga 1) plus de som är undantagna från storleksregeln. Proaktiv tillsyn (ex-ante).
- **Viktiga:** Viktiga verksamhetsutövare — Verksamheter i andra kritiska sektorer (Bilaga 2). Reaktiv tillsyn (ex-post) — tillsynsåtgärder initieras av incidentrapporter eller tips.

2.3 Sektorer, klassificering och tillsynsmyndigheter

Nedanstående tabell visar de 18 sektorerna med respektive klassificering och formellt utsedd tillsynsmyndighet enligt Cybersäkerhetsförordningen (SFS 2025:1507). Notera att 'MCF' i tabellen syftar på Myndigheten för civilt försvar (f.d. MSB). 'LST' avser de sex utsedda länsstyrelserna: Norrbotten, Stockholm, Skåne, Västra Götaland, Örebro och Östergötland.

Sektor	Exempel på verksamheter	Klassificering	Tillsynsmyndighet
HÖGKRITISKA SEKTORER (VÄSENTLIGA) — Bilaga 1			
Energi	El, fjärrvärme/-kyla, olja, gas, vätgas, laddinfrastruktur	**Väsentlig**	Statens energimyndighet
Transport	Luftfart, järnväg, sjöfart, vägtransport	**Väsentlig**	Transportstyrelsen
Bankverksamhet	Kreditinstitut	**Väsentlig**	Finansinspektionen
Finansmarknadsinfrastruktur	Handelsplatser, centrala motparter	**Väsentlig**	Finansinspektionen
Hälso- och sjukvård	Vårdgivare, läkemedelstillverkning	**Väsentlig**	IVO, Läkemedelsverket
Dricksvatten	Leverantörer och distributörer	**Väsentlig**	Livsmedelsverket
Avloppsvatten	Insamling, behandling och bortledning	**Väsentlig**	Livsmedelsverket
Digital infrastruktur	DNS, molntjänster, datacenter, IXP	**Väsentlig**	PTS
IKT-tjänster (B2B)	Managed service providers, MSSP	**Väsentlig**	PTS
Offentlig förvaltning	Statliga myndigheter, regioner, kommuner	**Väsentlig**	MCF
Rymden	Operatörer av markbaserad infrastruktur	**Väsentlig**	PTS
ANDRA KRITISKA SEKTORER (VIKTIGA) — Bilaga 2			
Post- och budtjänster	Leverantörer av post- och budtjänster	**Viktig**	PTS
Avfallshantering	Företag som bedriver avfallshantering	**Viktig**	Länsstyrelserna
Kemikalier	Tillverkning och distribution	**Viktig**	Länsstyrelserna
Livsmedel	Produktion, bearbetning, distribution	**Viktig**	Livsmedelsverket
Tillverkning	Medicintekniska produkter, datorer, fordon	**Viktig**	Läkemedelsverket, Transportstyrelsen, LST
Digitala leverantörer	Marknadsplatser online, sökmotorer, sociala medier	**Viktig**	PTS
Forskning	Forskningsorganisationer	**Viktig**	Länsstyrelserna

2.4 Anmälningsplikt: registreringen är stängd

MCF:s registreringsportal öppnade den 2 februari 2026 under MCFFS 2026:1 (MCF:s författningssamling) — den första föreskriften under den nya lagen. Alla verksamheter som

träffas av lagen, inklusive de som sedan tidigare var registrerade under gamla NIS-lagen, var skyldiga att anmäla sig inom 14 dagar — det vill säga senast runt den 16 februari 2026.

Har din organisation registrerat sig?
Om organisationen ännu inte har anmält sig till rätt tillsynsmyndighet är detta den mest akuta åtgärden. Kontakta er sektors tillsynsmyndighet (se tabell ovan) omedelbart. Utebliven registrering kan leda till sanktionsavgifter.

Kapitel 3: Säkerhetsåtgärder och styrning

3.1 De tio obligatoriska riskhanteringsåtgärderna

Cybersäkerhetslagen kräver 'lämpliga och proportionerliga tekniska, operativa och organisatoriska åtgärder' och specificerar tio obligatoriska åtgärdsområden enligt Artikel 21 i NIS2-direktivet. Detaljerade krav fastläggs i MCF:s föreskrifter (förväntat april 2026).

1. Riskanalys och policyer för informationssäkerhet
2. Incidenthantering (förebyggande, detektion, analys, hantering)
3. Verksamhetskontinuitet, säkerhetskopiering och katastrofåterställning
4. Säkerhet i leveranskedjan (direkta leverantörer och tjänsteleverantörer)
5. Säkerhet vid förvärv, utveckling och underhåll av system samt sårbarhetshantering
6. Löpande utvärdering av säkerhetsåtgärdernas effektivitet (penetrationstester, revisioner)
7. Grundläggande cyberhygien och obligatorisk utbildning för ledning
8. Kryptografipolicyer och kryptering av data i vila och under överföring
9. Personalsäkerhet, åtkomstkontroll och tillgångshantering
10. Multifaktorautentisering (MFA) och säkrade kommunikationssystem

Notera att utbildningskravet (punkt 7) i den antagna lagen gäller ledningsorgan — inte alla anställda som ursprungsförslaget SOU 2024:18 föreslog.

3.2 Leveranskedjans säkerhet — ansvar och gränsdragning

En av de mest långtgående nyheterna är det explicita ansvaret för säkerheten i den egna leveranskedjan. Sverige har valt att begränsa detta till direkta leverantörer (tier 1) — underleverantörer träffas inte direkt av lagen, men verksamhetsutövare måste ändå ställa adekvata avtalskrav på sina direkta leverantörer.

I praktiken innebär detta att organisationer måste:

- Kartlägga och riskbedöma direkta leverantörers säkerhetsnivå.
- Inkludera specifika cybersäkerhetskrav i leverantörsavtal.
- Implementera en robust process för tredjepartsriskhantering (Third-Party Risk Management).

Dominoeffekten fortfarande relevant

Stora verksamheter som träffas av lagen kommer i sin tur att ställa krav på sina leverantörer — även de som är för små för att direkt träffas av lagen. Cybersäkerhetslagen höjer därmed den allmänna säkerhetsnivån i hela det svenska näringslivet.

3.3 Ledningens ansvar — nu formaliserat i lag

Lagen gör ledningsorganen (styrelse och VD) direkt ansvariga för organisationens efterlevnad. Ledningen måste:

- Formellt godkänna och aktivt övervaka implementeringen av säkerhetsåtgärder.
- Genomgå obligatorisk cybersäkerhetsutbildning (kravet gäller ledningsnivå).
- Vara medveten om att bristande efterlevnad kan leda till personliga sanktioner — ytterst ett temporärt förbud att utöva ledningsfunktioner.

Kapitel 4: Incidentrapportering — 24-timmarsklockan

4.1 Definitionen av en 'betydande incident'

Rapporteringsskyldigheten gäller 'betydande incidenter'. En incident är betydande om den uppfyller något av följande kriterier:

- Den har orsakat eller kan orsaka allvarliga driftstörningar för tjänsten eller ekonomisk skada för verksamhetsutövaren.
- Den har påverkat eller kan påverka andra fysiska eller juridiska personer genom att vålla betydande materiell eller immateriell skada.

> **Notera: Detaljerade tröskelvärden saknas ännu**
> Exakta kvantitativa tröskelvärden för vad som utgör 'allvarlig störning' eller 'betydande skada' fastläggs i MCF:s kommande incidentrapporteringsföreskrifter (förväntat april 2026). För leverantörer av DNS-tjänster, molntjänster, datacenter m.fl. finns redan specifika kriterier i EU Genomförandeförordning (EU) 2024/2690, som gäller sedan november 2024.

4.2 Rapporteringsprocessen: strikta tidsfrister

Incidentrapportering sker till MCF via CERT-SE. Portalen heter IRON (iron.msb.se) och är tillgänglig dygnet runt. CERT-SE nås även via 010-240 40 40 och cert@cert.se. Rapporteringen följer en fasad process:

Steg	Tidsfrist	Innehåll
Tidig varning	**Inom 24 timmar**	Indikera att en betydande incident kan ha inträffat. Ange om det kan röra sig om ett brott eller ett gränsöverskridande angrepp.
Incidentanmälan	**Inom 72 timmar**	Uppdaterad bedömning av allvarlighetsgrad och konsekvenser. Indikatorer på kompromettering (IoC) om möjligt.
Slutrapport	**Inom 1 månad**	Detaljerad beskrivning, grundorsak (root cause), vidtagna åtgärder och långsiktiga konsekvenser. Om incident pågår: lägesrapport istället.

Utöver rapporteringen till MCF/CERT-SE gäller en separat skyldighet att informera egna tjänstemottagare (kunder, användare) inom 72 timmar om de kan påverkas av incidenten. MCF planerar en ny samlad portal för anmälan och incidentrapportering till våren 2026.

4.3 Att operationalisera incidentberedskapen

Att möta 24-timmarsfristen kräver förberedda och inövade processer. Organisationer bör proaktivt:

- Etablera ett dedikerat incidenthanteringsteam (IRT) med tydliga roller och mandat.
- Dokumentera en formell incidenthanteringsplan anpassad till lagens rapporteringskrav.
- Förbereda mallar för de tre rapportstadierna till MCF och för kommunikation med tjänstemottagare.
- Genomföra regelbundna tabletop-övningar för att träna teamet att agera under press.

Kapitel 5: Tillsyn och sanktioner

5.1 Den tvådelade tillsynsmodellen

Tillsynen utövas av de sektorsspecifika tillsynsmyndigheter som listas i tabell 1. Modellen skiljer sig åt mellan väsentliga och viktiga verksamhetsutövare:

- Väsentliga verksamhetsutövare: Proaktiv tillsyn (ex-ante). Tillsynsmyndigheten kan på eget initiativ genomföra granskningar, revisioner och inspektioner utan misstanke om brister. Organisationer måste vara ständigt redo att uppvisa dokumenterat säkerhetsarbete.
- Viktiga verksamhetsutövare: Reaktiv tillsyn (ex-post). Tillsyn initieras av incidentrapporter eller tips om brister.

5.2 Sanktionsavgifter

Sanktionsavgifterna är knutna till organisationens globala omsättning — en modell inspirerad av GDPR. Alla sanktioner har ett minimigolv på 5 000 SEK.

Kategori	Maxbelopp	Alternativt maxbelopp
Väsentliga verksamhetsutövare	**10 000 000 euro**	**2 % av global årsomsättning**
Viktiga verksamhetsutövare	**7 000 000 euro**	**1,4 % av global årsomsättning**
Offentliga verksamhetsutövare	**10 000 000 SEK**	**— (fast tak, ej omsättningsbaserat)**

5.3 Bortom böter: befogenheten att avsätta ledning

Som en sista utväg vid allvarliga och upprepade överträdelser kan tillsynsmyndigheten ansöka hos domstol om att temporärt förbjuda enskilda ledningspersoner (VD, styrelseledamöter) från att utöva sina uppdrag hos en väsentlig verksamhetsutövare. Detta gäller vid intentionell eller grovt oaktsam bristande efterlevnad.

Ingen organisation har ännu drabbats av sanktioner under den nya lagen — lagen trädde i kraft i januari 2026 och centrala sekundärföreskrifter väntas i april 2026. Aktiv tillsynsverksamhet och sanktioner förväntas ta fart under senare delen av 2026.

Erfarenheter från NIS1

Under gamla NIS-lagen varierade tillsynsaktiviteten kraftigt mellan myndigheter. Vissa var aktiva med att utfärda sanktioner, andra använde knappt sina befogenheter. Med NIS2:s skärpta krav och tydligare mandat förväntas en mer enhetlig och proaktiv tillsynskultur.

Kapitel 6: Regulatorisk kalender och nuläge

Lagen gäller från 15 januari 2026, men det regulatoriska ramverket byggs fortfarande ut. Nedan ges en samlad bild av vad som är på plats och vad som väntas.

Tidpunkt	Händelse	Status
Dec 2025	Riksdagen antar Cybersäkerhetslag (2025:1506) och Cybersäkerhetsförordning (2025:1507)	KLAR
15 jan 2026	Lagen träder i kraft. Äldre NIS-lagen upphör.	KLAR
1 jan 2026	MSB byter namn till MCF – Myndigheten för civilt försvar	KLAR
2 feb 2026	MCF:s registreringsportal öppnar (MCFFS 2026:1)	KLAR
~16 feb 2026	Sista dag för registrering (14 dagars frist)	KLAR
Apr 2026	MCF:s föreskrifter om säkerhetsåtgärder och utbildning (förväntat)	KOMMANDE
Apr 2026	MCF:s föreskrifter om incidentrapportering (förväntat)	KOMMANDE
Vår 2026	Ny samlad portal för anmälan och incidentrapportering (planerat)	KOMMANDE
Höst 2026	MCF:s föreskrifter om säkerhetsrevisioner (planerat)	KOMMANDE
Löpande 2026	PTS sektorspecifika föreskrifter (datum ej fastlagt)	KOMMANDE

Regulatoriskt gap — viktigt att bevaka

Fram till april 2026 saknas bindande föreskrifter om exakta säkerhetsåtgärder, incidentrapporteringströskelvärden och detaljerade utbildningskrav. PTS har väglett att 'vad som utgör lämpliga åtgärder är åtminstone detsamma som krävdes av de nu upphävda säkerhetsföreskrifterna'. Organisationer bör bevaka MCF:s och PTS:s hemsidor löpande.

Kapitel 7: Handlingsplan — vad ska din organisation göra nu?

Lagen gäller fullt ut. Det finns ingen övergångstid. Nedan presenteras en prioriterad handlingsplan baserad på det faktiska nuläget i mars 2026.

Omedelbart (om inte redan gjort)

1. Registrering — Kontakta er tillsynsmyndighet omedelbart om ni inte redan registrerat er. Deadline var ca 16 februari 2026.
2. Tillämpningsanalys — Genomför och dokumentera en formell bedömning av om och hur lagen gäller er verksamhet. Inkludera koncernnivå-analys.
3. Ledningsbriefing — Presentera juridiska skyldigheter och personligt ansvar för styrelse och VD. Säkra formellt mandat och budget.

Kortfristigt (Q1–Q2 2026)

4. Gapanalys — Granska er nuvarande cybersäkerhetsförmåga mot de tio obligatoriska åtgärdsområdena. Identifiera specifika brister i policyer, processer och tekniska kontroller.
5. Incidentberedskap — Etablera eller uppdatera incidenthanteringsplan för att möta 24/72-timmarsfristen. Registrera er i IRON-portalen (iron.msb.se).
6. Leverantörsgranskning — Genomför riskbedömning av direkta leverantörer. Uppdatera avtal med cybersäkerhetskrav.
7. Ledningsutbildning — Genomför obligatorisk cybersäkerhetsutbildning för styrelseledamöter och VD.

Medelfristigt (Q2–Q4 2026)

8. Bevaka sekundärföreskrifter — Följ MCF:s föreskrifter om säkerhetsåtgärder och incidentrapportering (förväntat april 2026). Uppdatera ert program utifrån nya krav.
9. Implementera tekniska kontroller — MFA, kryptering, åtkomstkontroll, loggning och sårbarhetshantering utifrån gapanalysens prioriteringar.
10. Efterlevnadsrevision — Genomför intern eller extern revision för att verifiera att alla krav är uppfyllda. Förbered för proaktiv tillsyn (om ni är väsentlig verksamhetsutövare).
11. Övningar och simuleringar — Genomför tabletop-övningar för incidenthanteringsteamet minst en gång per halvår.

Slutsats: Från regulatorisk börda till strategisk motståndskraft

Cybersäkerhetslagen (2025:1506) är nu verklighet. Den markerar ett paradigmskifte i hur cybersäkerhet regleras i Sverige — med personligt ledningsansvar, kraftiga sanktioner och en utökad räckvidd som träffar tusentals organisationer som tidigare stod utanför NIS-regelverket.

Det återstående regulatoriska gapet — att centrala föreskrifter väntas i april 2026 — skapar en möjlighet att använda den närmaste tiden väl: genomföra gapanalyser, träna ledning, stärka leveranskedjesäkerheten och etablera incidentberedskap. Organisationer som investerat i ISO 27001 och systematiskt informationssäkerhetsarbete under NIS1 är bäst positionerade; de som börjar från noll har en brant inlärningskurva framför sig.

Efterlevnad av cybersäkerhetslagen är inte ett projekt med ett slutdatum — det är en löpande affärsfunktion. Organisationer som anammar detta perspektiv och integrerar cybersäkerhet i sin kärnstyrning kommer inte bara att undvika sanktioner. De bygger motståndskraft, stärker förtroendet hos kunder och partners och skapar en konkurrensfördel i en marknad som ställer allt högre krav på digital trygghet.

Nyckelreferenser

Nedan listas de viktigaste officiella källorna för löpande uppföljning:

- **Lagtext:** Cybersäkerhetslag (2025:1506) — riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/cybersakerhetslag-20251506_sfs-2025-1506/
- **Förordning:** Cybersäkerhetsförordning (2025:1507) — riksdagen.se
- **Prop:** Proposition 2025/26:28 — regeringen.se
- **MCF/CERT-SE:** MCF (f.d. MSB) — mcf.se | Incidentrapportering: iron.msb.se | CERT-SE: cert.se
- **PTS:** PTS — pts.se/sakerhet-och-integritet/cybersakerhetslagen/
- **Energimyndigheten:** Statens energimyndighet — energimyndigheten.se (NIS2-vägledning för energisektorn)

- **FI:** Finansinspektionen — fi.se/sv/bank/sok-tillstand/nis/
- **Livsmedelsverket:** Livsmedelsverket — livsmedelsverket.se (NIS2 och cybersäkerhetslagen)
- **Transportstyrelsen:** Transportstyrelsen — transportstyrelsen.se/nis
- **NIS2-direktivet:** EU NIS2-direktivet (EU) 2022/2555 — EUR-Lex
- **EU 2024/2690:** EU Genomförandeförordning (EU) 2024/2690 — EUR-Lex (incidentrapporteringskriterier)

WeTeam AB

Pär Abelson | par.abelson@weteam.se | 0735-200025

Uppdaterad mars 2026 | Baserat på officiella källor och gällande lagstiftning