NIS2 & cybersäkerhetslagen – Krav, ansvar & åtgärder

Johan Sundberg & Fredrik Eråker, 12 november 2026
edpLaw Advokatbyrå

Institute
EN DEL AV BLENDOW GROUP



Agenda

- Bakgrund och regelverk
- Tillämpningsområde
- Centrala skyldigheter
- Incidentrapportering
- Tillsyn och sanktioner

BG Institute
EN DEL AV BLENDOW GROUP

Bakgrund och syfte

💡 CER-direktivet – omfattar samhällsviktig verksamhet

➡️ Syftet med NIS2-direktivet är uppnå en hög gemensam cybersäkerhetsnivå inom EU och *stärkt motståndskraft*

➡️ Lagen, inkl. regeringsförordningen, trädde i kraft den 15 januari 2026 och ersatte då NIS-lagen

BG Institute
EN DEL AV BLENDOW GROUP

Tidsplan för implementering

15 januari 2026

Lag och förordning träder i kraft

2 februari 2026

Anmälningstjänsten öppnar

1 juli 2026

Föreskrifter om incidentrapportering och informationsskyldighet träder i kraft

1 oktober 2026

Föreskrifter om säkerhetsåtgärder och ledningens utbildning träder i kraft

Föreskrifter om säkerhetsrevisioner och säkerhetsskanningar träder i kraft

BG Institute
EN DEL AV BLENDOW GROUP

Antagna och kommande föreskrifter från PTS

Ansvar:

- Digital infrastruktur
- Digitala leverantörer
- Förvaltning av IKT-tjänster (mellan företag)
- Post- och budtjänster
- Rymden
- Länsstyrelserna
- Verksamhetsutövare som erbjuder domännamnsregistreringstjänster

Föreskrifter om säkerhetsåtgärder → början av 2027.

Föreskrifter för telekomområdet om betydande incidenter → trädde i kraft 15 oktober 2026.

Föreskrifter om säkerhetsåtgärder och incidentrapportering för sektorerna rymden och post- och budtjänster → prel. hösten 2027.

Föreskrifter avseende skyldigheten att föra register om domännamn → prel. Hösten 2027.

Föreskrifter om informationsskyldighet vid betydande incidenter och cyberhot → ingen fastställd tidsplan.

BG Institute
EN DEL AV BLENDOW GROUP

Vilka verksamheter omfattas?

!! Om verksamheten omfattas så omfattas den i *sin helhet*

➡️ Vissa offentliga aktörer

➡️ Verksamhetsutövare som omfattas av bilaga 1 eller 2 till NIS2-direktivet, är etablerad i Sverige och är åtminstone ett medelstort företag

➡️ Vissa andra aktörer som är undantagna från etablerings- eller storlekskravet, till exempel leverantörer av allmänt tillgängliga elektroniska kommunikationstjänster

➡️ *Väsentliga* och *viktiga* verksamhetsutövare

➡️ Bilaga 1 till NIS2-direktivet: *Högkritiska sektorer*

➡️ Bilaga 2 till NIS-2-direktivet: *Andra kritiska sektorer*

➡️ Kommissionens rekommendation 2003/361/EG med definition av små och medelstora företag och bestämmande av beräkningsunderlag (50 sysselsatta eller 10 miljoner EUR i omsättning)

BG Institute
EN DEL AV BLENDOW GROUP

NIS2-sektorer

- Energi
- Transporter
- Bankverksamhet
- Finansmarknads-infrastruktur
- Hälso- och sjukvårdssektorn
- Dricksvatten
- Avloppsvatten
- Digital infrastruktur
- Förvaltning av IKT-tjänster
- Offentlig förvaltning
- Rymden
- Post- och budtjänster
- Avfallshantering
- Tillverkning, produktion och distribution av kemikalier
- Produktion, bearbetning och distribution av livsmedel
- Tillverkning
- Digitala leverantörer
- Forskning

BG Institute
EN DEL AV BLENDOW GROUP

Vilka verksamheter omfattas – Kommissionens rekommendation 6 maj 2003

➡️ Medelstora företag – färre än 250 anställda, omsättning mindre än 50 MEURO och/eller balansomslutning mindre än 43 MEURO

➡️ Små företag – Färre än 50 anställda, omsättning mindre än 10 MEURO och/eller balansomslutning mindre än 10 MEURO

➡️ Microföretag – Färre än 10 anställda, omsättning mindre än 2 MEURO och/eller balansomslutning mindre än 2 MEURO

BG Institute
EN DEL AV BLENDOW GROUP

Vilka krav innebär den nya cybersäkerhetslagen?

📄 Anmälningsskyldighet (2 kap. 2. §)

🔐 Skyldighet att vidta säkerhetsåtgärder (2 kap. 3 §)

📚 Ledningen ska genomgå utbildning (2 kap. 4 §)

📢 Incidentrapportering och informationsskyldighet (2 kap. 5–10 §§)

🔀 EU-kommissionens genomförandeförordning 2024/2690

🌟 ENISA:s implementeringsvägledning från juni 2025

BG Institute
EN DEL AV BLENDOW GROUP

Hur går anmälan till?

Alla verksamhetsutövare som omfattas av CSL ska anmäla sig, inkl. kommuner och regioner.

Anmälan öppnade 2 feb 2026 och ska ske till MCF: https://www.ncsc.se/sv/radgivning-och-stod/cybersakerhetslagen-nis2/att-anmala-en-verksamhet/

Anmälan ska göras “så snart det kan ske”. Detta kan skilja sig åt beroende på verksamhet och hur komplicerade bedömningarna är.

MCF “kan komma att vidta åtgärder” för anmälningar som är mer än 14 dagar sena.

PTS har en vägledande e-tjänst: https://csl-omfattning.pts.se

BG Institute
EN DEL AV BLENDOW GROUP

Kravet på säkerhetsåtgärder

Verksamhetsutövare ska vidta **lämpliga** och **proportionella** tekniska, driftsrelaterade och organisatoriska åtgärder för att skydda nätverks- och informationssystem som de använder för sin verksamhet eller för att tillhandahålla sina tjänster och systemens fysiska miljö mot incidenter (säkerhetsåtgärder).

Säkerhetsåtgärderna ska utgå från ett **allriskperspektiv** och säkerställa en nivå på säkerheten i nätverks- och informationssystemen som är **lämplig** i förhållande till **risken**.

BG Institute
EN DEL AV BLENDOW GROUP

Kravet på säkerhetsåtgärder

Riskanalys	Incidenthantering	Kontinuitetshantering och krishantering	Säkerhets i leveranskedjan	Förvärv, utveckling och underhåll av system
Bedöma effektiviteten i åtgärderna	Cyberhygien och utbildning	Kryptografi	Personalsäkerhet och åtkomstkontroll	Autentisering

BG Institute
EN DEL AV BLENDOW GROUP

EU:s genomförandeförordning 2024/2690

Direkt tillämplig på vissa digitala verksamheter, bland annat:

- Molntjänster, datacenter och DNS-tjänster
- Leverantörer av förvaltade IKT-tjänster och säkerhetstjänster
- Digitala marknadsplatser, sökmotorer och sociala nätverksplattformar
- Betrodda tjänster

Innehåller detaljerade krav på:

- Cybersäkerhetsåtgärder, policyer och dokumentation
- Incidenthantering och leverantörssäkerhet
- När incidenter ska anses betydande

BG Institute
EN DEL AV BLENDOW GROUP

Säkerhet i leveranskedjan

Lämpliga tekniska, driftsrelaterade och organisatoriska åtgärder ska vidtas för att skydda nätverks- och informationssystem, bl.a. i förhållande till säkerhet i leveranskedjan (2 kap. 3 § pt 4 CSL).

Krav på att bedöma och hantera cybersäkerhetsrisker inför utkontraktering samt säkerställa att lämpliga säkerhetsåtgärder regeras i avtal med leverantören (4 kap. 1 och 4 §§ MCFFS 2026:11). Se särskilt de allmänna råden till 4. kap 4 §.

Särskilda krav i balagan (pt 5) till genomförandeförordningen kring strategi och avtalsinnehåll för säkerhet i leveranskedjan.

BG Institute
EN DEL AV BLENDOW GROUP

Incidentrapportering – vilka incidenter omfattas?

Incident

En händelse som undergräver tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten hos lagrade, överförda eller behandlade uppgifter eller hos de tjänster som erbjuds genom eller är tillgängliga via nätverks- och informationssystem

Betydande incidenter

En incident som orsakat eller kan orsaka allvarlig driftsstörning för den erbjudna tjänsten eller ekonomisk skada för den berörda verksamhetsutövaren, eller om den har påverkat eller kan påverka andra fysiska eller juridiska personer genom att vålla betydande skada.

Se även särskilda regler i genomförande-förordningen

BG Institute
EN DEL AV BLENDOW GROUP

När är en incident betydande – driftsstörningar och ekonomisk skada

Allvarlig driftstörning (1 §)

- Sektorsverksamheten kraftigt begränsad i mer än 12 timmar.
- Alternativa arbetssätt krävs i mer än 48 timmar.
- Skyddsvärd information i sektorskritiska system röjs, förvanskas eller förstörs.

Ekonomisk skada (3 och 5 §§)

- Kostnader som överstiger 5 % av årsomsättningen.
- Både direkta och indirekta kostnader beaktas, inklusive återställning, rådgivning och intäktsbortfall.

BG Institute
EN DEL AV BLENDOW GROUP

När är en incident betydande – övriga kriterier

Betydande skada för andra (6 §)

- Skyddsvärd information som rör annan juridisk person eller minst 500 individer röjs, förvanskas eller förstörs.
- Föroreningsskada, allvarlig personskada, dödsfall eller allvarlig påverkan på samhällsviktig verksamhet.

Risk för betydande konsekvenser (2, 4 och 7 §§)

- Även betydande cyberhot och sårbarheter som kan leda till ovanstående konsekvenser omfattas.

Återkommande incidenter (8 §)

- Minst två incidenter inom sex månader med samma grundorsak och sammantagen ekonomisk skada över 5 %-gränsen.

BG Institute
EN DEL AV BLENDOW GROUP

Incidentrapportering – tidskrav

24 timmar

Upplysning

Om betydande incident, efter att den identifierats som betydande

24 timmar

Betrodda tjänster

Även incidentanmälan ska lämnas inom 24 timmar

72 timmar

Incidentanmälan

För övriga verksamhetsutövare, efter att incidenten identifierats som betydande

1 månad

Slutrapport

Alternativ lägesrapport om incidenten fortfarande pågår. Delrapport på begäran

BG Institute
EN DEL AV BLENDOW GROUP

Policyer och grundläggande dokumentation

- Policy för säkerhet i nätverks- och informationssystem
- Riskhanteringspolicy
- Incidenthanteringspolicy
- Policy för säkerhet i leveranskedjan
- Policy för säkerhetstestning
- Policy för att utvärdera effektiviteten hos vidtagna riskhanteringsåtgärder
- Policy för kryptografi
- Åtkomstkontrollpolicy
- Policy för hantering av privilegierade konton och systemadministrationskonton
- Policy för hantering av tillgångar
- Policy för hantering av flyttbar media

- Riskhanteringsplan
- Tillgångsregister
- Plan för driftkontinuitet
- Krishanteringsplan
- Leverantörsregister

BG Institute
EN DEL AV BLENDOW GROUP

Något om krav på bakgrundskontroller

- **Cybersäkerhetslagen 3 §** – personalsäkerhet, strategier för åtkomstkontroll och tillgångsförvaltning.

- **Genomförandeförordningen – artikel 10** – säkerställa att bakgrunden kontrolleras för sina anställda och, i förekommande fall, för direkta leverantörer och tjänsteleverantörer, om (i) detta är genomförbart och (ii) detta krävs för deras roller, ansvarsområden och befogenheter.

- **Vägledning från ENISA** – överväga att kontrollera brottshistorik.
- Rättslig grund för behandling av personuppgifter enligt artikel 6 i GDPR?
- Grund för att hantera brottsuppgifter?

BG Institute
EN DEL AV BLENDOW GROUP

Sanktioner (4 kap) och tillsyn (3 kap)

➡️ **4 kap 10 § - Lägst 5.000 kr**

➡️ **Upp till det högsta av 2 % av årsomsättningen eller 10 MEURO (väsentliga verksamhetsutövare)**

➡️ **Upp till det högsta av 1,4 % av årsomsättningen eller 7 MEURO (viktiga verksamhetsutövare)**

➡️ **4 kap 12 § - Preskription - 2 år**

BG Institute
EN DEL AV BLENDOW GROUP

Sanktioner och tillsyn

➡️ **4 kap 6 § - Förbud att inneha ledningsfunktion (personlig)**

➡️ **3 kap 2 § - reaktiv tillsyn (viktiga verksamhetsutövare)**

➡️ **3 kap 5 § Proaktiv tillsyn – bl.a. säkerhetsrevisioner av väsentliga verksamhetsutövare**

➡️ **Får agera utan att något inträffat**

BG Institute
EN DEL AV BLENDOW GROUP

Kort checklista

1. Omfattas verksamheten?
2. Om ja, uppfyll anmälningsskyldigheten.
3. Genomför gap-analys, bedöm risker och vidta säkerhetsåtgärder
4. Implementera rutiner för rapportering av betydande incidenter – använd befintliga incidentprocesser
5. Utbilda ledning och anställda

BG Institute
EN DEL AV BLENDOW GROUP

NIS2 och cybersäkerhetslagen i praktiken

Heldagskurs 9 februari

Som kursdeltagare får du kunskap om:

- Hur du bedömer om en verksamhet omfattas av NIS2 och cybersäkerhetslagen
- Grundläggande krav enligt det nya regelverket
- Incidenthantering och incidentrapportering
- Säkerhet i leveranskedjan och krav på leverantörer
- Regler om bakgrundskontroller
- Risker vid bristande efterlevnad, inklusive sanktions- och tillsynsaspekter
- Förhållandet mellan NIS2, cybersäkerhetslagen och GDPR
- Ledningens ansvar och utbildningskrav kopplade till säkerhetsåtgärder

BG Institute
EN DEL AV BLENDOW GROUP

Frågor?

Institute

EN DEL AV BLENDOW GROUP

Tack!

För frågor om BG Institute och våra kurser,
mejla oss på **kursinformation@bginstitute.se**

BG Institute
EN DEL AV BLENDOW GROUP