Datum
2024-12-13

Energisystem
Emma Johansson, 08-677 25 05
emma.johansson@energiforetagen.se

Säkerhet för energisektorn – en översikt över nuvarande och kommande regleringar

Energiföretagens medlemsföretag berörs av många lagstiftningar inom säkerhetsområdet. Dokumentet ger en omfattande översikt över nuvarande och kommande regleringar inom säkerhetsområdet för energisektorn, inklusive direktiv och förordningar. Utöver de lagstiftningar som sammanfattas här finns det flera andra relevanta lagstiftningar som inte riktar sig specifikt mot energisektorn, exempelvis dataskyddsförordningen (GDPR) som regler hantering av personuppgifter.

Innehåll

Säkerhetsarbete bidrar till en resilient energiförsörjning

Energiförsörjningen är helt avgörande för försörjningstryggheten i samhället. Ett omfattande och långvarigt avbrott påverkar många samhällsviktiga verksamheter samt totalförsvaret. Därför är det nödvändigt att de mest kritiska funktionerna inom energiförsörjningen kan upprätthållas både vid kriser i fredstid och under höjd beredskap samt krig.

Säkerhets- och beredskapsfrågor är centrala för att skydda vårt energisystem och samhället i stort. I takt med ökad omvärldsutveckling, inkluderande hot, risker samt ett potentiellt militärt angreppshot, blir kontinuerligt och långsiktigt säkerhetsarbete allt viktigare. Kombinationen av energisektorns roll som kritisk för samhällets trygghet och den ökande elektrifieringen samt klimatomställningen förstärker behovet av robusta säkerhetsåtgärder ytterligare.

Med förändrade hotbilder följer även ökade krav på effektiv cybersäkerhet, resiliens och beredskap från lagstiftare och tillsynsmyndigheter. Resiliens innebär att kunna återgå till normaldrift så snabbt som möjligt efter en störning och lära sig av händelsen. Riskanalyser har utvecklats från att enbart omfatta kriser till att täcka hela hotskalan, inklusive cyberattacker, sabotage, spionage och spridning av desinformation, samt införlivar även perspektiv från totalförsvaret i verksamhetsplanering och beslut.

Exempel på nuvarande och kommande regleringar för energisektorn presenteras nedan. Genom att införa nya krav och kontinuerligt följa upp åtgärder samt efterlevnad kan energibranschen gemensamt bättre hantera dagens och framtidens hot och risker, säkerställa en resilient energiförsörjning och minimera avbrott.

Checklista för företag inom energisektorn

Denna checklista är avsedd att ge en översikt över aktiviteter som företag inom energisektorn behöver beakta för att säkerställa regelefterlevnad i sitt säkerhetsarbete. Det är viktigt att kontinuerligt följa upp både den digitala och fysiska miljön samt personalsäkerhet inklusive leverantörer och konsulter med åtkomst till system och anläggningar. En grundlig planering för implementering av åtgärder, uppföljning och översyn rekommenderas starkt.

För att implementera nya regleringar bör ni följa en strukturerad och systematisk process. Här är en steg-för-steg-guide för att hjälpa er att komma i gång:

1. Skapa en projektplan:
    - Utveckla en detaljerad projektplan som beskriver alla åtgärder som behöver vidtas, tidsramar, ansvariga personer och resurser som krävs. Använd projektledningsverktyg för att hålla koll på framstegen.
2. Utse en projektledare och ett team:
    - Utse en projektledare som ansvarar för att driva implementeringen framåt. Sätt samman ett tvärfunktionellt team med representanter från olika avdelningar, såsom IT, säkerhet, HR och juridik.
3. Genomför en riskbedömning:
    - Utför en omfattande riskbedömning för att identifiera och prioritera de mest kritiska riskerna. Använd resultaten för att utveckla specifika åtgärder och säkerhetsåtgärder.
4. Utveckla och implementera säkerhetspolicyer:
    - Skapa tydliga säkerhetspolicyer och riktlinjer som beskriver hur olika säkerhetsåtgärder ska genomföras och följas. Kommunicera dessa policyer till all personal och säkerställ att de är lättillgängliga.
5. Utbilda och träna personalen:
    - Planera och genomför regelbundna utbildningar och övningar för att säkerställa att all personal är medveten om säkerhetsrutiner och vet hur de ska agera vid en incident. Använd både teoretiska och praktiska övningar.
6. Implementera tekniska lösningar:
    - Installera och konfigurera nödvändiga tekniska lösningar, såsom brandväggar, antivirusprogram, övervakningssystem och multifaktorautentisering (MFA). Se till att dessa system regelbundet uppdateras och underhålls.
7. Utveckla en incidenthanteringsplan:
    - Skapa en detaljerad incidenthanteringsplan som beskriver hur olika typer av incidenter ska hanteras. Planen bör inkludera roller och ansvar, kommunikationsstrategier och återställningsåtgärder.

8. Övervaka och utvärdera framstegen:
    - Använd övervakningsverktyg för att kontinuerligt övervaka säkerhetsläget och identifiera potentiella hot i realtid. Genomför regelbundna revisioner och uppdateringar av säkerhetsskyddsplanen.
9. Samarbeta med externa experter:
    - Anlita säkerhetskonsulter eller samarbeta med säkerhetsföretag för att få expertis och råd om hur ni bäst kan skydda er verksamhet. Detta kan inkludera genomförande av penetrationstester och säkerhetsrevisioner.
10. Dokumentera och rapportera framstegen:
    - Dokumentera alla åtgärder som vidtas och rapportera regelbundet framstegen till ledningen och relevanta myndigheter. Detta hjälper till att säkerställa att ni följer lagkraven och kan visa på efterlevnad.

Genom att följa dessa steg ovan kan ni effektivt implementera de föreslagna åtgärderna och stärka säkerheten och motståndskraften inom er organisation.

Urval av säkerhets- och beredskapsregleringar för energibranschen

Lagarna reglerar informations- och cybersäkerhet, personalsäkerhet, fysiskt skydd samt beredskap under fredstida kriser, höjd beredskap samt ytterst krig. Till lagarna tillkommer allmänna förordningar, föreskrifter samt sektorspecifika föreskrifter.

Gällande och kommande regleringar

1. Direktivet om nät- och informationssäkerhet (NIS)

Kort om 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, eller NIS-direktivet, som trädde i kraft 2016 var den första EU-omfattande cybersäkerhetslagstiftningen. NIS-direktivet är uppbyggt kring fyra huvuddelar:

1 Stärkande av den nationella cybersäkerhetskapaciteten, särskilt genom antagande av en nationell strategi för cybersäkerhet, inrättande av en eller flera nationella behöriga myndigheter för cybersäkerhet och inrättande av minst en enhet för hantering av cybersäkerhetsincidenter (CSIRT-enhet).
2 Inrättande av en ram för samarbete mellan medlemsstaterna, och i synnerhet inrättandet av samarbetsnätverket som består av företrädare för medlemsstaterna, kommissionen och Enisa och CSIRT-nätverket (som består av företrädare för nationella CSIRT-enheter och CERT-EU) i syfte att underlätta informationsutbyte om potentiella risker och sårbarheter.
3 Förstärkning av säkerheten för leverantörer av samhällsviktiga tjänster genom minimikrav på säkerhet och rapportering av incidenter som kan ha en betydande inverkan på relevanta nationella myndigheter.
4 Införande av gemensamma europeiska cybersäkerhetsregler för leverantörer av digitala tjänster på områdena molntjänster, sökmotorer och internetbaserade marknadsplatser.

Syftet med NIS-lagstiftningen är att uppnå en hög nivå av säkerhet i nätverk och informationssystem för samhällsviktiga tjänster. Detta ska uppnås genom krav på införande av systematiskt och riskbaserat informationssäkerhetsarbete och incidentrapportering. Organisationen ska också vidta säkerhetsåtgärder för att hantera risker och säkerställa kontinuitet. Nuvarande NIS-direktivet genomfördes i svensk rätt 2018 genom lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster (NISL) och Förordning (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster (NISF). NIS-lagen gäller inte om säkerhetsskyddslagen är tillämplig enligt 8 § NISL. Myndigheten för samhällsskydd och beredskap (MSB) har föreskriftsrätt.

Medlemsstaterna ska fastställa regler om sanktioner för överträdelse av nationella bestämmelser som har antagits enligt NIS-direktiv och vidta alla nödvändiga åtgärder för att se till att de tillämpas. Sanktionerna ska vara effektiva, proportionella och avskräckande.

Betydelse/konsekvenser för energisektorn

Energisektorn omfattades redan av NIS-direktivet, med el, gas och olja som delsektorer. Anmälningsplikt råder för de som identifierat sig som NIS-leverantör enligt MSBFS 2024:4 föreskrifter om anmälan och identifiering av leverantörer av samhällsviktiga tjänster. Energimyndigheten har tagit fram sektorsspecifik föreskrift Statens Energimyndighets föreskrifter och allmänna råd om riskanalys och säkerhetsåtgärder för nätverk och informationssystem inom energisektorn (STEMFS 2021:3). Samt vägledning på föreskriften: Vägledning till Statens Energimyndighets föreskrifter och allmänna råd om riskanalys och säkerhetsåtgärder för nätverk och informationssystem inom energisektorn (ER 2022:17). Efterlevnad av regelverket följs upp genom tillsyn. För energiförsörjningen är det Energimyndigheten som är tillsynsmyndighet för hela NIS-lagstiftningen.

2. Direktivet om nät- och informationssäkerhet (NIS2)

Kort om direktivet

Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, eller NIS2-direktivet, som tillhandahåller en rättslig ram för att hålla jämna steg med den ökade digitaliseringen och en föränderlig hotbild mot cybersäkerheten.

I kommissionens översyn av NIS-direktivet drogs slutsatsen att genomförandet av direktivet visade sig vara en utmaning på grund av dess begränsade tillämpningsområde, dess brist på tydlighet när det gäller tillämpningsområde och befogenheter, men också på grund av den ineffektiva kontrollen av efterlevnaden på medlemsstatsnivå och alltför stora skillnader mellan de nationella strategierna. NIS2-direktivet antogs i syfte att bredda dess tillämpningsområde. Kommissionen kan lämna delegerade akter kopplat till genomförandet av kraven i NIS2-direktivet för att anpassa och harmonisera reglerna på EU-nivå.

Enligt NIS2-direktivet är medlemsstaterna skyldiga att ytterligare stärka sin cybersäkerhetskapacitet genom att utvidga tillämpningsområdet för sina nationella cybersäkerhetsstrategier och genom att öka sitt samarbete. Dessutom måste de inrätta ramar för hantering av cybersäkerhetskriser och en samordnad sårbarhetsrapportering. Det europeiska samarbetet utvidgas också, både på strategisk och teknisk nivå, men också på krishanteringsnivå genom inrättandet av ett nytt nätverk, Cyber Crisis Liaison Organisation Network (CyCLONe).

En av de största förändringarna är den enorma utvidgningen av tillämpningsområdet för NIS2 jämfört med NIS-direktivet. NIS2 omfattar 18 sektorer, däribland energisektorn. Förutom nya sektorer har också nya typer av enheter inom befintliga sektorer lagts till i direktivets tillämpningsområde. Distinktionen mellan "väsentliga" och "viktiga" enheter görs nu på grundval av enhetens storlek, dess omsättning och vilken typ av enhet det rör sig om. "Väsentliga" och "viktiga" entiteter som omfattas av direktivet måste vidta lämpliga åtgärder för att hantera riskerna för säkerheten i sina nätverks- och informationssystem och för att förebygga incidenter eller mildra effekterna av incidenter. I NIS2-direktivet fastställs också mer omfattande regler kring incidentrapportering till nationella behöriga myndigheter.

Överträdelser kan resultera i betydande ekonomiska sanktioner. Väsentliga entiteter som överträder artikel 21 eller 23, kan få sanktionsavgifter på högst 10 000 000 EUR eller högst 2 procent av den totala globala årsomsättningen under det föregående räkenskapsåret för det företag som den väsentliga entiteten tillhör, beroende på vilken siffra som är högst. Som lägst kan sanktionsavgifter för väsentliga verksamheter uppgå till 5 000 kronor.

Betydelse/konsekvenser för energisektorn

NIS2-direktivet implementeras i svensk lagstiftning genom cybersäkerhetslagen (CSL). Lagen föreslås att träda i kraft 1 augusti 2025. Energisektorn är en sektor som klassificeras som väsentlig (högkritisk). Den omfattar delsektorerna elektricitet, fjärrvärme eller fjärrkyla, olja, gas och vätgas.

I Sverige kommer NIS2-direktivet att implementeras genom en ny lag, cybersäkerhetslagen och en ny förordning, cybersäkerhetsförordningen (ej fastställda

ännu). Den nu gällande NIS-lagen och förordningen om informationssäkerhet för samhällsviktiga och digitala tjänster ska då upphävas.

Enligt NIS2 måste verksamheterna utföra självutvärdering och självregistrering genom anmälningsplikt för att informera myndigheterna om de kriterier som fastställs i lagstiftningen. Anvisningar för anmälan kommer under 2025 att publiceras på Energimyndighetens webb. Även verksamheter som inte räknas som ett medelstort företag enligt definitionen i NIS2 kan komma att omfattas via föreskrifter för cybersäkerhetslagen eller via identifiering enligt CER-lagstiftningen. Vi återkommer med mer information när föreskrifterna tagits fram.

Energimyndigheten föreslås bli tillsynsmyndighet för energisektorn. Energimyndigheten har rätt att inleda tillsyn om vi får bevis på, indikationer på, eller information om att ni underlåtit att fullgöra era skyldigheter enligt cybersäkerhetslagen. Ni är skyldiga att bland annat vidta riskhanteringsåtgärder för cybersäkerhet och rapportera incidenter.

Det här gäller säkerhetskänslig verksamhet

Enskilda verksamhetsutövare som bedriver säkerhetskänslig verksamhet omfattas av NIS2 i den delen av verksamheten som inte är säkerhetskänslig. Är ni en verksamhetsutövare som har säkerhetskänslig verksamhet kan ni alltså behöva anmäla er till Energimyndigheten. Bedriver ni däremot enbart säkerhetskänslig verksamhet så kan ni falla utanför NIS2. I sådana fall ska ni inte anmäla er enligt NIS2.

3. Kritiska entiteters motståndskraft (CER)

Kort om direktivet

Europaparlamentets och rådets direktiv (EU) 2022/2557 av den 14 december 2022 om kritiska entiteters motståndskraft, eller CER-direktivet, som syftar till att stärka kritiska entiteters motståndskraft mot en rad hot och risker. Direktivet trädde i kraft den 16 januari 2023. EU-länderna har haft fram till den 17 oktober 2024 på sig att anta nationell lagstiftning för att införliva direktivet. Preliminärt sker den svenska implementeringen genom den nya lag som träder i kraft först under 2025. De behöriga myndigheterna ska sedan använda förteckningen i bilagan till CER-direktivet för att göra en riskbedömning senast den 17 januari 2026.

I CER-direktivet konstateras att kritiska verksamhetsutövare spelar en avgörande roll för att upprätthålla viktiga samhällsfunktioner eller central ekonomisk verksamhet på den inre marknaden. Det är därför enligt direktivet viktigt att det på unionsnivå skapas en reglering som syftar till att stärka kritiska verksamhetsutövares motståndskraft genom att fastställa harmoniserade minimiregler. Det är också viktigt att bistå verksamhetsutövarna genom enhetligt stöd och tillsynsåtgärder.

Genom CER-direktivet upphävdes rådets direktiv 2008/114/EG av den 8 december 2008 om identifiering av, och klassificering som, europeisk kritisk infrastruktur och bedömning av behovet att stärka skyddet av denna (ECI-direktivet).

I rådets direktiv 2008/114/EG föreskrivs ett förfarande för att klassificera infrastruktur i energi- och transportsektorerna som europeisk infrastruktur, vars driftstörning eller förstörelse skulle få betydande gränsöverskridande konsekvenser i minst två medlemsstater. Vid utvärderingen av det direktivet konstaterades att säkerhetsåtgärderna i det direktivet inte är tillräckliga för att förhindra alla störningar från att uppstå. Det är därför nödvändigt att säkerställa att risker redovisas bättre, att skapa

enhetlighet i rollen och uppgifterna för kritiska verksamhetsutövare och att anta unionsregler för att stärka kritiska verksamhetsutövares motståndskraft. Kritiska verksamhetsutövare bör kunna öka sin förmåga att förebygga, skydda sig mot, reagera på, stå emot, begränsa, absorbera, anpassa sig till och återhämta sig från incidenter som kan störa tillhandahållandet av samhällsviktiga tjänster.

Vidare anges i direktivet att kritiska verksamhetsutövare behöver rustas bättre eftersom det finns en dynamisk hotbild och ett ökande ömsesidigt beroende mellan infrastruktur och de olika sektorerna. Direktivet syftar till att åstadkomma en solid harmoniseringsnivå när det gäller de sektorer och kategorier av verksamhetsutövare som omfattas av tillämpningsområdet. Direktivet inrättar en övergripande ram för att hantera kritiska verksamhetsutövares motståndskraft med hänsyn till alla faror, oberoende av om det är naturliga faror eller orsakade av människan, olyckshändelser eller avsiktligt framkallade faror (skäl 1–4).

Riskbedömning av medlemsstaterna

Kommissionen ges i direktivet befogenhet att anta en delegerad akt för att komplettera direktivet med en icke uttömmande förteckning över samhällsviktiga tjänster inom de sektorer och undersektorer som omfattas av direktivet. De behöriga myndigheterna ska använda förteckningen för att göra en riskbedömning senast den 17 januari 2026 (medlemsstaternas riskbedömning). Medlemsstaternas riskbedömningar ska innehålla en redogörelse för relevanta risker för naturolyckor och risker orsakade av människan, inbegripet risker av sektorsövergripande eller gränsöverskridande slag, olyckor, naturkatastrofer, hot mot folkhälsan och hybridhot eller andra antagonistiska hot. Inom tre månader från att riskbedömningen har gjorts ska medlemsstaten förse kommissionen med relevant information om de typer av risker som har identifierats och resultatet av riskbedömningen per sektor och undersektor.

CER-direktivet handlar inte direkt om cybersäkerhet, men det definierar tydligt dess förhållande till NIS2-direktivet. Enligt skäl 9 och artikel 1.2 i CER-direktivet ska detta direktiv inte tillämpas på frågor som omfattas av NIS2-direktivet. Mot bakgrund av förhållandet mellan kritiska entiteters fysiska säkerhet och cybersäkerhet ska medlemsstaterna dock säkerställa att de två direktiven genomförs på ett samordnat sätt. Enligt artikel 9.6 i CER-direktivet måste det dessutom finnas en viss samordning mellan den nationella behöriga CER-myndigheten och den nationella behöriga myndigheten för NIS2-direktivet för att säkerställa att luckor inte finns.

Medlemsstaterna ska fastställa regler om sanktioner för överträdelse av de nationella åtgärder som antagits enligt detta direktiv och vidta alla nödvändiga åtgärder för att säkerställa att de tillämpas. Sanktionerna ska vara effektiva, proportionella och avskräckande.

Betydelse/konsekvenser för energisektorn

CER-direktivet implementeras i svensk lagstiftning genom förslag på lag om motståndskraft hos kritiska verksamhetsutövare (LOM). Lagen föreslås att träda i kraft 1 augusti 2025.

Bilagan till direktivet innehåller 11 sektorer däribland energi, med delsektorerna elektricitet, fjärrvärme eller fjärrkyla, olja, gas och vätgas. Undantagna är laddningsoperatörer som har ansvar för förvaltning och drift av en laddningspunkt som inte omfattas av CER-direktivet.

En skillnad mellan CER och NIS-2 direktivet är att enligt CER-direktivet ska kritiska entiteter identifieras och pekas ut av medlemsstaterna. Energimyndigheten föreslås bli tillsynsmyndighet för CER-lagstiftningen för energisektorn. Energimyndigheten kommer också att kommunicera direkt med de verksamhetsutövare som omfattas av den nya lagstiftningen om lagen om motståndskraft under sommaren 2026.

Vi återkommer med mer information när lag, förordning och föreskrifterna tagits fram.

Det här gäller säkerhetskänslig verksamhet

Enskilda verksamhetsutövare som bedriver säkerhetskänslig verksamhet omfattas av CER i den delen av verksamheten som inte är säkerhetskänslig. Är ni en verksamhetsutövare som har säkerhetskänslig verksamhet kan ni alltså behöva anmäla er till Energimyndigheten. Bedriver ni däremot enbart säkerhetskänslig verksamhet så kan ni falla utanför CER. I sådana fall ska ni inte anmäla er.

4. Nätkod för cybersäkerhet vid gränsöverskridande elflöden (NC CS)

Kort om förordningen

Nätkod om sektorsspecifika regler för cybersäkerhetsaspekter av gränsöverskridande elflöden (NC CS) syftar till att fastställa en europeisk standard för cybersäkerhet för gränsöverskridande elflöden. Här inbegrips regler om gemensam riskbedömnings- och riskhanteringsprocess, säkerhetskrav, övervakning, rapportering och krishantering. Nätföreskrifter är rättsligt bindande i alla medlemsstater. Förordningen kompletterar EU:s förordning (EU) 2019/943 genom att fastställa nätföreskrifter för sektorsspecifika regler som rör cybersäkerhetsaspekter av gränsöverskridande elflöden. Trädde i kraft den 13 juni 2024.

Förordningen syftar till att harmonisera regler och förfaranden mellan medlemsländerna för att förbättra samarbetet och hantera cyberhot på ett effektivt sätt. Den omfattar också gränsöverskridande elflöden i sammankopplade digitaliserade kraftsystem. Förordningen betonar vikten av att hantera cybersäkerhetsrisker för att upprätthålla en säker elförsörjning och säkerställa höga cybersäkerhetsnivåer inom energisektorn. Digitalisering och cybersäkerhet är avgörande för att tillhandahålla samhällsviktiga tjänster och är av strategisk betydelse för kritisk energiinfrastruktur.

Entiteter som identifieras ha stor påverkan och kritisk påverkan behöver inrätta ett riskhanteringssystem för cybersäkerhet, om det inte redan finns på plats. Nätföreskrifterna kräver att entiteter med stor påverkan och kritisk påverkan inrättar ett sådant ledningssystem för informationssäkerhet för att hantera cybersäkerhetsriskerna och genomförandet av cybersäkerhetskontroller, beroende på typen av enheter. De allmänna kraven på ett ledningssystem är huvudsakligen härledda från ISO/IEC 27001-standarden, men det krävs inte att enheter följer specifikt denna standard eller certifieras mot standarden.

Den omfattar också flöden för informationsutbyte om cybersäkerhet för att säkerställa information i rätt tid, främja snabba och samordnade reaktioner från berörda parter och tillhandahålla regler för incidenthantering och krishantering. Dessutom omfattar nätföreskrifterna en ram för cybersäkerhetsövningar för att förbättra alla operatörers beredskap, regler för skydd av informationsutbyte och en ram för övervakning, och incidentrapportering.

Överträdelser kan i nuläget inte resultera i ekonomiska sanktioner.

Betydelse för elsektorn

NC CS har direkta konsekvenser för elsektorn, och i synnerhet för den typ av enheter som anges nedan:

- leverantörer
- systemansvariga för distributionssystem
- systemansvariga för överföringssystem
- producenter
- aggregatorer
- lagringsoperatörer
- efterfrågeflexibilitet aktörer
- elhandelsföretag

Vilka entiteter som omfattas identifieras och pekas ut av medlemsstaterna. Energimyndigheten är av regeringen utsedd till Sveriges behöriga myndighet för NC CS och förväntas peka ut entiter (verksamhetsutövare) som omfattas av förordningen 8 månader efter att NC CS trätt i kraft, alltså under februari 2025.

5. AI-rättsakt

Kort om förordningen

AI-förordningen trädde i kraft den 1 augusti 2024 och ska skapa en enhetlig reglering för utveckling och användning av AI-system inom EU. Förordningen ska tillämpas fullt ut två år efter att den trätt i kraft vilket troligtvis sker under sommaren 2026 i Sverige.

I förslaget till förordning fastställs följande:

- Bred tillämplighet: Påverkar leverantörer, spridare, importörer, distributörer och tillverkare av AI-system inom EU, inbegripet dem vars AI-utdata används i EU, oavsett var de befinner sig.
- Stränga efterlevnadskrav: Upprättar rigorösa efterlevnadskrav, med undantag för militär-, försvars- och forskningsändamål.
- Krav på verkställighet: Förtydligar tillämpningsområdet, kraven och konsekvenserna av AI.
- Praktiska strategier för efterlevnad: Betonar vikten av AI-styrningsprogram och proaktivt engagemang för att uppnå efterlevnad.

Vidare innehåller den särskilda regler för AI-system som skapar en hög risk för fysiska personers hälsa och säkerhet eller grundläggande rättigheter. De omfattar regler om riskhanteringssystem, data och dataförvaltning, teknisk dokumentation, registerföring, transparens och tillhandahållande av information till användare, mänsklig tillsyn och noggrannhet, robusthet och cybersäkerhet. Utöver detta fastställs i förordningen regler om skyldigheter för leverantörer och användare av AI-system med hög risk och andra parter. Enheter inom energisektorn som använder eller överväger att använda AI-system som betraktas som AI-system med hög risk måste erkänna de regler som fastställs i rättsakten om artificiell intelligens.

Överträdelser av AI-förordningen kan resultera i betydande ekonomiska sanktioner. Sanktionsavgifterna kan uppgå till tre procent (3 %) av ett företags globala årsomsättning. För överträdelser av förbudet mot användning av AI-system inom riskgrupp 1 kan sanktionsavgifter uppgå till motsvarande sju procent (7 %).

Betydelse för energisektorn

AI-förordningen får ett brett tillämpningsområde. Producenter, importörer, återförsäljare och användare av AI-system omfattas alla i varierande grad av AI-förordningens bestämmelser, inklusive dess ansvarsbestämmelser. AI-system med hög risk omfattas som AI-system som är avsedda att användas som säkerhetskomponenter vid försörjning av vatten, gas, värme och el.

Regeringen har tillsatt en utredning för att se över behovet av nationella anpassningar till följd av EU:s nya förordning om AI (AI-förordningen). Det finns ännu inget besked om vilken svensk myndighet som ska få det övergripande ansvaret. Dock finns förväntningar på att Integritetsmyndigheten (IMY) förväntas bli ansvarig myndighet för AI-förordningen.

6. Säkerhetskyddslagstiftning

Kort om lagstiftningen

För att stärka säkerhetsskyddet infördes den 1 april 2019 den nya säkerhetsskyddslagen (2018:585). I säkerhetsskyddslagen finns bland annat bestämmelser om verksamhetsutövarens ansvar, säkerhetsskyddsanalys och säkerhetsskyddsåtgärder, samt om tillsynsmyndigheternas ansvar. Varje verksamhet ska själv utreda och bedöma om och i vilken omfattning verksamheten omfattas av säkerhetsskyddslagen och kraven på säkerhetsskyddsåtgärder. Bedömningen görs i en säkerhetsskyddsanalys. Exempel på främmande makts metoder för underrättelseinhämtning är öppna källor, signalspaning, cyberspionage mot skyddsvärda verksamheter i syfte att stjäla information eller att förbereda sabotage, flyg- och satellitspaning, traditionell personbaserad inhämtning.

För att stärka skyddet för Sveriges säkerhet ytterligare finns sedan 1 januari 2021 flera ändringar i säkerhetsskyddslagen. Den 1 december 2021 kom även en ny säkerhetsskyddsförordning (2021:955) för att ytterligare stärka verksamheter. Förordningen innehåller kompletterande bestämmelser till säkerhetsskyddslagen. I förordningen behandlas bland annat säkerhetsskyddschefens roll, informationssäkerhet och säkerhetsprövning.

Säkerhetspolisens föreskrifter om säkerhetsskydd (PMFS 2022:1) innehåller kompletterande bestämmelser till säkerhetsskyddslagen och säkerhetsskyddsförordningen, och gäller från 1 mars 2022. Till kraven på säkerhetsskyddsåtgärder finns flertalet vägledningar från Säkerhetspolisen som bland annat omfattar säkerhetsskyddanalys, informationssäkerhet, fysiskt skydd och personalsäkerhet med flera.

Sektorspecifika tillsynsmyndigheter för energisektorn

Svenska kraftnät och Energimyndigheten får utfärda föreskrifter om säkerhetsskydd för enskilda verksamhetsutövare inom el- och energiförsörjning. För elförsörjningen är Svenska kraftnät (Svk) tillsynsmyndighet. För övriga energislag är Energimyndigheten tillsynsmyndighet för säkerhetsskyddet från den 1 december 2021. Respektive tillsynsmyndighet tar fram föreskrifter och särskilda blanketter för anmälningar som kompletterar Säkerhetspolisens vägledningar. Se respektive tillsynsmyndighets hemsida.

Försvarsmaktens föreskrifter om signalskyddstjänsten gäller alla verksamhetsutövare som ska använda kryptografiska funktioner för att kommunicera säkerhetsskyddsklassificerade uppgifter till ett informationssystem utanför verksamhetsutövarens kontroll.

Offentlighets- och sekretesslagens (OSL) regler om sekretess måste vara tillämpbara för att uppgifter ska vara säkerhetsskyddsklassificerade. Företagen ska därför göra en prövning om en uppgift skulle ha omfattats av sekretess enligt den lagen, om den hade varit tillämplig även för dem. Enskilda verksamhetsutövare behöver hänvisa till den bestämmelse i OSL som sekretessen avseende en viss handling eller uppgift hänförs till, för att underlätta en korrekt hantering och transparens när det gäller säkerhetsklassificerade uppgifter och handlingar.

En sanktionsavgift ska bestämmas till lägst 25 000 kronor och högst 50 000 000 kronor enligt lag (2021:952). När sanktionsavgiftens storlek bestäms ska särskild hänsyn tas till de omständigheter som anges.

Betydelse för energisektorn

Säkerhetsläget är allvarligt i Sverige. Omvärldsförändringar och globalisering har flyttat gränserna för den nationella säkerheten. Det har lett till ett behov av att säkerhetsskyddslagstiftningen nu omfattar fler samhällssektorer, som vissa delar av energisektorn som bedriver verksamhet som är av betydelse för Sveriges säkerhet eller som omfattas av ett för Sverige förpliktande internationellt åtagande om säkerhetsskydd.

Innehavare av verksamheter har ett stort ansvar att svara mot samhällets krav på säkerhetsskydd som bland annat innebär att skyddsvärda uppgifter inte kommer i orätta händer, vilket om så sker kan leda till skada för Sverige. Det är därför viktigt att alla ägare av verksamhet inom energisektorn arbetar systematiskt med att klassificera sina informationstillgångar och därefter vidtar nödvändiga åtgärder för att skydda dessa tillgångar så att endast de som har behov och är behöriga har tillgång till dem.

Om ni har signalskyddsutrustning eller säkerhetsskyddsklassificerade uppgifter som inte omfattas av säkerhetsskyddsavtal så är det ändock att betrakta inom ramen för er säkerhetskänsliga verksamhet. För handledning, se ”Att säkerhetsskyddsklassificera skyddsvärda uppgifter” från Energiföretagen Sverige.

7. Riskberedskap inom elsektorn

Kort om den gällande lagstiftningen

I Europaparlamentets och rådets förordning (EU) 2019/941 av den 5 juni 2019 om riskberedskap inom elsektorn och om upphävande av direktiv 2005/89/EG, fastställs regler för samarbete mellan medlemsstaterna i syfte att förebygga, förbereda sig inför och hantera elkriser i en anda av solidaritet och öppenhet och med fullt beaktande av kraven på en konkurrensutsatt inre marknad för el.

I förordningen fastställs regler för riskbedömning med avseende på en trygg elförsörjning, inbegripen identifiering av de mest relevanta regionala och nationella elkrisscenarierna och upprättande av riskberedskapsplaner och åtgärder på grundval av dessa planer. I förordningen fastställs också regler för hantering av elkriser, inklusive regler för tidig varning, tillkännagivande av en elkris, samarbete och bistånd mellan medlemsstaterna samt efterhandsutvärdering.

Enligt skäl 7 i förordningen kompletterar det NIS-direktivet (EU) 2016/1148 genom att säkerställa att cyberincidenter identifieras korrekt som en risk och att de åtgärder som vidtas för att hantera dem återspeglas korrekt i riskberedskapsplanerna. Enligt skäl 2 sträcker sig konsekvenserna av elkriser ofta över nationsgränserna. Även om sådana kriser börjar lokalt kan deras effekter snabbt sprida sig över gränserna. Vissa extrema

omständigheter, som köldknäppar, värmeböljor eller cyberattacker, kan påverka hela regioner samtidigt.

Betydelse/konsekvenser för energisektorn

Förordningen säkerställer att medlemsstaterna och andra aktörer som operatörer, systemansvariga för överföringssystem (TSO:er) och systemansvariga för distributionssystem (DSO:er) kan samarbeta effektivt över gränserna. I direktivet fastställs också en gemensam ram med regler för hur elkriser ska förebyggas, förberedas och hanteras, vilket ger större insyn i förberedelsefasen under en elkris och säkerställer att åtgärder vidtas på ett samordnat och effektivt sätt. Som redan har nämnts ser förordningen också till att cybersäkerhetsrisker (nät- och informationssäkerhet) ingår i riskberedskapsplanerna. I Sverige är Energimyndigheten utpekad krisberedskapsmyndighet för energisektorn.

8. Elberedskapslagstiftning

Kort om lagstiftningen

Elberedskapen omfattas bland annat av elberedskapslag (1997:288), förordning (1997:294) om elberedskap samt affärsverket Svenska kraftnäts föreskrifter om elberedskap (SvKFS 2023:1).

Syftet med beredskap är att förebygga, motstå och hantera sådana störningar i elförsörjningen som kan medföra svåra påfrestningar på samhället, under fredstida kriser och i höjd beredskap. Att upprätta beredskapsplaner är en beredskapsåtgärd. Andra åtgärder är robusthöjande åtgärder som sambandskommunikation via Rakel, reparationsberedskap och ö-driftförmågor.

Betydelse för energisektorn

Elberedskapslagen gäller för de aktörer som bedriver produktion av el, handel med el eller sådan överföring av el som sker med stöd av nätkoncession enligt 2 kap. 1 § ellagen (1997:857). Elberedskapslagen innehåller även en skyldighet för elföretag att anmäla vissa förändringar i anläggningar eller i verksamheten som kan påverka elförsörjningens förmågor. Svenska kraftnät är av regeringen utsedd till Sveriges elberedskapsmyndighet.

9. Externa dokument

Nedan ges en sammanställning över länkar till relevanta externa dokument, såväl lagstiftningar som vägledningar.

- 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 union (NIS-direktivet)
- Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster
- Förordning (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster
- Myndigheten för samhällsskydd och beredskaps föreskrifter om anmälan och identifiering av leverantörer av samhällsviktiga tjänster (MSBFS 2024:4)
- Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för leverantörer av samhällsviktiga tjänster (MSBFS 2018:8)
- Myndigheten för samhällsskydd och beredskaps föreskrifter och allmänna råd om rapportering av incidenter för leverantörer av samhällsviktiga tjänster (MSBFS 2018:9)
- Energimyndighetens föreskrift STEMFS 2021: 3.pdf
- Vägledning inom informationssäkerhet för dig som arbetar utifrån NIS-direktivet inom energisektorn (energimyndigheten.se)
- Strategi och verktyg för säkerhet och vägledning av efterlevnad av NIS2-direktivet genom kontroller enligt ISO IEC27001 och IEC27002 (energiforetagen.se)
- EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävning av direktiv (EU) 2016/1148 (NIS 2-direktivet)
- Delbetänkande av utredningen om genomförande av NIS2- och CER-direktiven Nya regler om cybersäkerhet SOU 2024:18
- EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV (EU) 2022/2557 av den 14 december 2022 om kritiska entiteters motståndskraft och om upphävande av rådets direktiv 2008/114/EG (CER-direktivet)
- Slutbetänkande av utredningen om genomförande av NIS2- och CER-direktiven Motståndskraft i samhällsviktiga tjänster SOU 2024:64
- KOMISSIONENS DELEGERADE FÖRORDNING (EU) 2024/1366 av den 11 mars 2024 om komplettering av Europaparlamentets och rådets förordning (EU) 2019/943 genom inrättandet av en nätföreskrift om sektorsspecifika regler för cybersäkerhetsaspekter av gränsöverskridande elflöden (NC CS)
- Europaparlamentets och rådets förordning (EU) 2024/1689 av den 13 juni 2024 om harmoniserade regler för artificiell intelligens och om ändring av förordningarna (EG) nr 300/2008, (EU) nr 167/2013, (EU) nr 168/2013, (EU) 2018/858, (EU) 2018/1139 och (EU) 2019/2144 samt direktiven 2014/90/EU, (EU) 2016/797 och (EU) 2020/1828 (förordning om artificiell intelligens) (Text av betydelse för EES)

- Säkerhetsskyddslag (2018:585)
- Säkerhetsskyddsförordning (SFS 2021:955)
- Säkerhetspolisens föreskrifter om säkerhetsskydd (PMFS 2022:1)
- Affärsverket Svenska kraftnäts föreskrift om säkerhetsskydd (SvKFS 2022:1
- Statens energimyndighets föreskrifter om säkerhetsskydd (STEMFS 2023:2)
- Försvarsmaktens föreskrifter om signalskyddstjänsten (FFS 2021:1)
- Att säkerhetsskyddsklassificera skyddsvärda uppgifter, en handledning från Energiföretagen Sverige
- Offentlighets- och sekretesslag (2009:400)
- EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING (EU) 2019/941 av den 5 juni 2019 om riskberedskap inom elsektorn och om upphävande av direktiv 2005/89/EG
- Nationell riskberedskapsplan för Sveriges elförsörjning i enlighet med Europaparlamentets och rådets förordning (EU) 2019/941 av den 5 juni 2019 om riskberedskap inom elsektorn och om upphävande av direktiv 2005/89/EG
- Elberedskapslag (1997:288)
- Förordning (1997:294) om elberedskap
- Affärsverket Svenska kraftnäts föreskrifter om elberedskap (SvKFS 2023:1).
- Förordning (2022:524) om statliga myndigheters beredskap