



### < kahn > pedersen

Hanna Bogsjö Österberg og Fredrik Sandström

# MCF:s nya förslag till föreskrifter om säkerhetsåtgärder och utbildning enligt cybersäkerhetslagen

Myndigheten för civilt försvar (MCF) har publicerat *en reviderad remissversion* av föreskrifter om säkerhetsåtgärder och utbildning enligt den kommande cybersäkerhetslagen (CSL). Föreskrifterna är ett centralt led i genomförandet av NIS2-direktivet i svensk rätt och syftar till att konkretisera dels de olika typer av säkerhetsåtgärder en verksamhetsutövare är skyldig att vidta för att uppfylla 2 kap. 3 § CSL, dels vilken utbildning som ledningen ska genomgå enligt 2 kap. 4 § CSL.

Det nya förslaget togs fram efter omfattande synpunkter på det första utkastet som skickades ut på extern remiss hösten 2025. Kritiken rörde då bland annat bristande tydlighet, särskilt kring vägledning hur proportionalitetsprincipen och riskbaserade avvägningar skulle tillämpas i praktiken, samt svårigheterna i att förena kraven med olika sektors behov. Ändringarna i det reviderade förslaget tar i huvudsak sikte på att gå från detaljerade, tvingande regler till mer övergripande funktionskrav, där detaljerna istället hanteras i form av rekommendationer i allmänna råd.

I korthet innebär det reviderade förslaget bland annat:

- Ett tydligt skifte av fokus mot att etablera processer och ett fungerande styrsystem istället för att i detalj ange vilka åtgärder som ska vidtas.
- Mer utförliga krav på ansvarsfördelning, roller och ledningens involvering samt krav på uppföljning och rapportering till ledningen.
- Att arbetet med cybersäkerhet ska integreras i den ordinarie verksamhetsstyrningen, vilket markerar en förskjutning från en isolerad IT-fråga till en central del av verksamhetsledningen.
- Nya och mer utvecklade krav på teknisk samverkan, omvärldsbevakning och kriskommunikation, inklusive användning av nationella stödfunktioner för hantering av sårbarheter, cyberhot och kriskommunikation.
- Att kraven på säkerhet i leveranskedjan i huvudsak har gått från tvingande regler för avtalsinnehåll med underleverantörer till allmänna råd, samtidigt som behovet av att se över och komplettera befintliga avtal med krav på cybersäkerhet tydliggörs.
- Att utbildningskraven har konkretiserats, särskilt när det gäller ledningens kompetens, vilket också har lyfts upp till ett eget kapitel.
- Att begrepp och struktur har förtydligats, vilket gör regleringen mer konsekvent och lättare att tillämpa.

Sammanfattningsvis ger det nya förslaget verksamhetsutövare större flexibilitet att anpassa sitt cybersäkerhetsarbete utifrån sin egen specifika kontext och riskprofil. Samtidigt får ledningen ett tydligare ansvar, inklusive kraven på tillräcklig kompetens och utbildning. Ändringarna medför således att NIS2-direktivets fokus på ledningsansvar speglas i större utsträckning och att cybersäkerhet i högre grad lyfts till en strategisk nivå.

*Hanna Bogsjö Österberg, advokat på Advokatfirman Kahn Pedersen. Hon arbetar inom byråns specialtområde Digital och särskilt med juridiska frågor i samband med digital transformation, IoT och strategiska sourcingprojekt.*

*Fredrik Sandström, advokat och Managing Associate på Advokatfirman Kahn Pedersen, arbetar främst med juridiska frågor kopplade till IT, digitalisering och teknikintensiva projekt inom bl.a. bank, försäkring, energi och industri.*