Länsstyrelsen Östergötland

Datum
2024-05-22

Diarienummer
4055-2024

Försvarsdepartimentet
Rättssekretariatet
Fö2024/00496

Remissvar över delbetänkandet

Nya regler om cybersäkerhet (SOU 2024:18).

Sammanfattning

Länsstyrelsen Östergötlands remissvar har genomförts i samråd och samverkan med Länsstyrelsernas nationella organisation för informationssäkerhet och dataskydd.

Länsstyrelsen Östergötland bedömer att den föreslagna cybersäkerhetslagen kan bli svår att båda tillämpa och utöva tillsyn efter och avstryker betänkandets förslag i vissa delar.

5.2.1 Utgångspunkter

Länsstyrelsen stödjer användningen av vedertagna begrepp och normalt språkbruk. Att regleringen använder begrepp och språk som finns i annan reglering, standarder och normalt språkbruk kommer att underlätta tillämpningen av reglerna.

Utredningens begrepp ”riskhanteringsåtgärder” bör enligt Länsstyrelsen bytas ut mot det vedertagna begreppet ”säkerhetsåtgärder”.

Allmänna synpunkter

Hög cybersäkerhetsnivå

Länsstyrelsens uppfattning är att den föreslagna regleringen, i motsats till utredningens intentioner, riskerar att öka regelbörda och administration.

Som verksamhetsutövare är det, enligt Länsstyrelsens uppfattning, inte helt enkelt att förstå om den egna verksamheten omfattas av reglerna eller inte.

Regelverket innehåller en inte obetydlig mängd undantag. Dessutom har i vissa fall andra rättsregler företräde framför de föreslagna bestämmelserna.

Synpunkterna på dessa förslag har framförts nedan kopplat till avsnitt 5.4 och 5.5.

Sammantaget är det, enligt Länsstyrelsens uppfattning, tveksamt om de föreslagna reglerna kommer att uppnå syftet att uppnå en hög cybersäkerhet.

Länsstyrelsen Östergötland anser att det i förslag till lag om cybersäkerhet inte framgår vad som avses med hög cybersäkerhetsnivå.

Verksamhetsutövare bör genom lag om cybersäkerhet få kännedom om vad som avses med hög cybersäkerhetsnivå. Detta behöver förtydligas, och är en förutsättning för att uppnå efterlevnad av eftersträvad eller tilltänkt nivå av skydd. Det har flera kopplingar till vilka resurser som krävs och är en förutsättning för att uppnå efterlevnad.

I exempelvis Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för statliga myndigheter 2020:6 4 § återges på ett tydligt sätt vad som avses för att efterleva författningen genom att hänvisa till att verksamhetsutövaren ”ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete med stöd av informationssäkerhetsstandarden i ISO 27”. En sådan motsvarighet bör införas i lag om cybersäkerhet och det bör till och med vara så att lag om cybersäkerhet bör nämna ISO 27. Ta även ställning till om det är certifiering som ska avses mot regelverket för att ge förutsättningar för mätbarhet.

Vad som avses med hög cybersäkerhetsnivå behöver förtydligas med koppling till någon form av normgivande sammanställning som ger förutsättning för mätbarhet. Exempelvis kan certifiering anses vara mätbart, då denna process inbegriper bedömning om effektivitet och verkningsfullhet utefter tillämpliga bestämmelser/regler. Det är ett underlag som även möjliggör mekanism/er för kvalitativ uppföljning och kontroll.

5.2.2 Verksamhetsutövare

Länsstyrelsen anser att verksamhetsutövare är ett bra samlingsbegrepp för den som kan träffas av lagen. Det är ett vedertaget begrepp inom säkerhetsskyddsregelverket, vilket kan förenkla implementeringen.

Länsstyrelsen delar utredningens bedömning att hela verksamheten bör omfattas av lagens tillämpningsområde. Ett informationssystem verkar inte i ett vacuum utan har kopplingar och beröringspunkter med verksamheten i stort. Ett fullgott informationssäkerhetsarbete bygger på att hela verksamheten integreras.

Undantag

5.4 Undantag för sektorsspecifika rättsakter och andra författningar

För att uppnå en god cybersäkerhet i samhället anser Länsstyrelsens att reglerna behöver vara enkla och lättillgängliga. Det innebär att Länsstyrelsen gärna hade sett en reglering som inte innehåller omfattande undantag och som inte heller är subsidiär. Om det ska vara subsidiär behöver det framgå tydligt vilka rättsregler som har företräde. Allt för att göra lagen enkel att tillämpa och utöva tillsyn över med syfte att uppnå en god cybersäkerhet. Utredningens förslag om att göra cybersäkerhetslagen subsidiär vid krav på riskhanteringsåtgärder eller incidentrapportering med

motsvarande verkan bedöms bidra till oklarheter om tillämpningsområdet. Det riskerar att göra lagen både svår att tillämpa och utöva tillsyn efter.

5.5.4 Undantag för offentliga verksamhetsutövare

Länsstyrelsen instämmer med MSB och Säkerhetspolisens förslag (som redovisas i avsnitt 5.2.11) att hela den offentliga sektorn, utan undantag, borde ha omfattats av lagen. Länsstyrelsen anser vidare att det skulle underlätta tillämpningen och öka acceptansen för regelverket om samtliga aktörer omfattades av lagens tillämpningsområde. Länsstyrelsens uppfattning är därför att undantag inte bör göras för myndigheter som till övervägande del bedriver säkerhetskänslig eller brottsbekämpande verksamhet. Även för det fall en verksamhetsutövare bedriver säkerhetskänslig verksamhet eller brottsbekämpning krävs god cybersäkerhet.

5.5.5 Undantag för enskilda verksamhetsutövare

I enlighet med synpunkter lämnade på föreslagna undantag för offentlig verksamhet, är det Länsstyrelsens uppfattning att undantag inte bör göras för enskilda verksamhetsutövare som till övervägande del bedriver säkerhetskänslig eller brottsbekämpande verksamhet. Även för det fall en verksamhetsutövare bedriver säkerhetskänslig verksamhet eller brottsbekämpning krävs god cybersäkerhet.

8.4.2 Tillsynsmyndigheter i Sverige

Länsstyrelsen avstyrker förslaget att utpekade länsstyrelser ska utöva tillsyn över resterande länsstyrelser. Länsstyrelserna har gemensam it-drift och gemensamma strukturer för informationssäkerhet och utveckling. Förslaget skulle därför innebära att länsstyrelserna utövade tillsyn över sig självt.

Länsstyrelsernas gemensamma strukturer

Regeringskansliet har genom regleringsbrev förordnat att länsstyrelserna ska ha en gemensam och effektiv it-verksamhet. Länsstyrelserna har en överenskommelse som reglerar den gemensamma it-verksamheten med Länsstyrelsen Västra Götaland som värdlänsstyrelse. Värdlänsstyrelsen ansvarar för länsstyrelsernas it-säkerhet samt för att it-miljön ges en ändamålsenlig, effektiv och enhetlig utformning.

Länsstyrelserna har också en gemensam stödfunktion för informationssäkerhet och dataskydd, Safir, med Länsstyrelsen Stockholm som värdmyndighet. All anskaffning och utveckling av it hanteras

gemensamt på länsstyrelserna med en gemensam förvaltningsmodell som har länsstyrelsen Västmanland som värdlänsstyrelse. Sammanfattningsvis innebär det att länsstyrelsernas informations- och cybersäkerhetsarbete är väl integrerat och inte med lätthet kan tillsynas var för sig. De gemensamma strukturerna har en så pass stor påverkan på cybersäkerheten att en korsvis tillsyn inom länsstyrelserna skulle orsaka intressekonflikter och riskera att myndigheternas oberoende ifrågasätts.

8.4.5 Föreskrifter

För att göra det lätt att göra rätt anser länsstyrelsen att MSB bör få i uppdrag att ta fram gemensamma och generella föreskrifter för alla sektorer. Dessa föreskrifter kan därefter kompletteras med sektorsspecifika föreskrifter i de delar som inte täcks in av de generella föreskrifterna. Detta förslag skiljer sig från utredningens förslag där tillsynsmyndigheterna, förutom länsstyrelserna, ges föreskriftsrätt inom sitt tillsynsområde.

9.5.6 Förbud att utöva ledningsfunktion

När länsstyrelsen som är registreringsmyndighet har fått en underrättelse om förbud ska de avregistrera personen som befattningshavare hos verksamhetsutövaren i stiftelseregistret. Länsstyrelse som är registreringsmyndighet ska säkerställa att personen inte registreras på nytt som befattningshavare hos verksamhetsutövaren under förbudstiden. Det framgår inte närmare av betänkandet om detta är tillämpbart i enlighet med bestämmelserna i stiftelselagen och stiftelseförordningen. Detta behöver utredas eller förtydligas.

De som medverkat i beslutet

Beslutet har fattats av landshövding Carl Fredrik Graf med informationssäkerhetssamordnare Tonna Söderberg som föredragande. I föredragningen deltog försvarsdirektör Jenny Knuthammar och bitr. försvarsdirektör Andreas Lundberg. I den slutliga handläggningen har också dataskyddssamordnare Malin Reinhold och Daniel Göransson medverkat.