

Remissvar

1 (7)

Datum

2009-03-24

Diarienummer (åberopas vid korrespondens)  
AD 009-14236-08Er referens  
M2007/4638/RMiljödepartementet  
103 33 StockholmÄven per e-mail  
registrator@environment.ministry.se och  
susanne.gerland@environment.ministry.se

## **Genomförande av Inspire-direktivet i svensk lagstiftning; förslag till ny miljöinformationslag och -förordning m.m.**

### **Sammanfattning**

Det remitterade författningsförslaget och underlaget för det har så stora brister att Säkerhetspolisen avstyrker att förslaget läggs till grund för lagstiftning utan ytterligare utredning och komplettering.

Om förslaget ändå genomförs vill Säkerhetspolisen framhålla vikten av en utförlig specialmotivering för att underlätta tillämpningen av de föreslagna bestämmelserna.

Säkerhetspolisen kan bidra med sin kompetens vid en fortsatt beredning i arbetsgrupp eller liknande.

### **Allmänna synpunkter**

Under arbetet med genomförandet av direktivet har Säkerhetspolisen pekat på behovet av ytterligare utredning i flera avseenden. Också Lantmäteriet framhöll i sin rapport, ”Införande av Inspire-direktivet i nationell lagstiftning – behovet av författningsändringar m.m.”, att det är nödvändigt att utreda vissa frågor särskilt. I rapporten fastslogs således att särskild utredning krävs bl.a. ifråga om säkerhetsskydds- och säkerhetsförfattningarnas tillämpning vid spridning av rumslig information, begränsning av datadelning mellan myndigheter på grund av sekretess samt vilka personuppgifter som ska kunna samköras i nättjänsterna.

Datum  
2009-03-24

Som underlag för det remitterade förslaget har bifogats en promemoria på sju sidor inklusive en mycket kortfattad författningskommentar. Av underlaget framgår inte vilka sammanställningar av information som i praktiken kommer att bli tillgängliga genom de informationshanteringstjänster som ska införas. Underlaget behandlar inte heller i övrigt de frågor som flera gånger understrukits som viktiga att utreda. Slutligen innehåller den knapphändiga författningskommentaren inte någon vägledning i hur författningarna i viktiga avseenden ska tillämpas.

Säkerhetspolisen är medveten om att arbetet med genomförandet av Inspire-direktivet bedrivs under stark tidspress. Icke desto mindre är det viktigt att genomförandet av direktivet analyseras på ett ingående sätt ur ett säkerhetsskyddsperspektiv eftersom konsekvenserna av att stora mängder information nu kommer att tillgängliggöras inte kan förutses. I värsta fall kan förslaget medföra att man tillgängliggör känslig information som kan användas vid planering av terroristattacker. Detta skulle få förödande och irreversibla konsekvenser.

Dessutom är det viktigt att sekretessfrågorna och personuppgiftsfrågorna analyseras. Författningsförslaget innebär att en ny och omfattande möjlighet till direktåtkomst införs. Förutom att direktåtkomsten innebär att myndigheterna i förväg måste göra en sekretessprövning beträffande all information som görs tillgänglig, så ger direktåtkomsten upphov till frågan om hur samkörningen förhåller sig till den s.k. finalitetsprincipen, som innebär att en personuppgift endast får behandlas för det ändamål den ursprungligen samlades in. Båda dessa frågor har stor betydelse för bland annat skyddet av den personliga integriteten.

Bristen på analys, tillräckligt utredningsunderlag etc. medför att det inte är möjligt att bedöma vilka konsekvenser förslagen får ur bl.a. säkerhetsskyddshänseende. Säkerhetspolisen kan därför inte tillstyrka det nu föreliggande författningsförslaget. Säkerhetspolisen kan vid en fortsatt beredning av författningsförslagen bidra med sin kompetens i en arbetsgrupp eller liknande.

Nedan redogör Säkerhetspolisen för bakgrunden till sitt ställningstagande såvitt avser säkerhetsskyddet. Vidare lämnar Säkerhetspolisen vissa synpunkter rörande författningsförslagen och även rörande den kostnads-nyttoanalys som hänvisas till i remissmissivet.

### **Frågor rörande säkerhetsskydd**

#### *Säkerhetsskyddslagstiftningen*

Säkerhetsskyddslagen (1996:627) med tillhörande säkerhetsskyddförordning (1996:633) gäller i allt väsentligt verksamhet hos staten, kommuner och landsting samt aktiebolag, handelsbolag, föreningar

Datum  
2009-03-24

och stiftelser över vilka staten, kommuner eller landsting utövar ett rättsligt bestämmande inflytande (1 § säkerhetsskyddslagen). Enligt lagen ska det i verksamhet där lagen gäller bland annat finnas ett säkerhetsskydd (5 §). Säkerhetsskyddet ska bland annat förebygga att uppgifter som omfattas av sekretess och som rör rikets säkerhet obehörigen röjs, ändras eller förstörs (informationssäkerhet) (7 §). Vid utformningen av informationssäkerheten ska behovet av skydd vid automatisk databehandling beaktas särskilt (9 §).

I säkerhetsskyddsförordningen finns bestämmelser om att de myndigheter och andra som förordningen gäller för, bland annat ska undersöka vilka uppgifter i deras verksamhet som ska hållas hemliga med hänsyn till rikets säkerhet. Resultatet av denna undersökning (säkerhetsanalys) ska dokumenteras (5 §). Innan en myndighet inrättar ett register som ska föras med hjälp av automatisk databehandling, och som kan förutses komma att innehålla sådana uppgifter att utlämnande av dem var och för sig eller sammanställda kan skada totalförsvaret, ska myndigheten samråda med Försvarmakten och, om det finns anledning till det, Rikspolisstyrelsen (12 §).

#### *Behovet av ett fullgott säkerhetsskydd*

Man kan idag utgå från att alla känsliga verksamheters rumsliga position är känd med tanke på de satellit- och flygfototjänster som finns att tillgå via Internet. Detta medför att kunskap om funktionerna vid de olika verksamheterna blir än mer skyddsvärda än de annars skulle vara. Genom att tillhandahålla information om funktioner m.m. vid olika verksamheter kan nämligen den totala mängden information bli så känslig att den kan betraktas som hemlig och påverka skyddet mot rikets säkerhet samt skyddet mot terrorism negativt. Det är också viktigt att hålla i minnet att även en kombination av olika typer av öppen information, t.ex. information om var en anläggning är geografiskt belägen kombinerad med information om dess funktion eller liknande (förmåga till hög el-överföring, klassning som skyddsobjekt etc.), kan leda till att uppgifter om hemliga anläggningar röjs. Sådana uppgifter ska hanteras och förvaras i enlighet med säkerhetsskyddslagstiftningen. I detta ingår bland annat, som nämnts ovan, en skyldighet för myndigheter samråda med Försvarmakten och, om det finns anledning till det, Rikspolisstyrelsen innan man inrättar ett IT-system med uppgifter som kan skada totalförsvaret.

Dessutom är det, för att syftet med direktivet ska kunna uppnås, angeläget att den geodata som finns i infrastrukturen är *riktig* när den ska användas vid samhällsplanering, katastrof, olycka eller kris. En tillgänglighetsattack mot IT-systemet eller en attack som tar sikte på att förändra information och innehåll i infrastrukturen kan i ett sådant akut läge få allvarliga konsekvenser.

Ett tillgängliggörande av information utan tillräckliga säkerhetsskyddsöverväganden medför en risk för att information

Datum  
2009-03-24

som skulle kunna utnyttjas för brottslig verksamhet, såsom inbrott, skadegörelse, sabotage eller terrorhandlingar, sprids och blir offentlig. Detta leder till att säkerheten i samhället minskar - ett faktum som måste vägas mot direktivets syfte att åstadkomma en bättre tillgång till rumslig information.<sup>1</sup>

I regeringens skrivelse Nationellt ansvar och internationellt engagemang – En nationell strategi för att möta hotet från terrorism, Skr. 2007/08:64, anförs bland annat att målet är att Sverige ska bli effektivare i sitt arbete med att avvärja, förebygga, skydda mot och hantera konsekvenser av terroristverksamhet. När det gäller det förebyggande arbetet är en viktig del att skydda individer och samhällsviktiga funktioner genom att minska sårbarheten. Viktiga åtgärder för att minska hoten från terrorister är bl.a. förbättrat skydd runt viktigare infrastrukturanläggningar, skydd för transporter och förbättrade instrument för att skydda samhällsviktiga funktioner. Genom att en mängd rumslig information görs tillgänglig på det sätt som nu föreslås kan det förebyggande arbetet direkt motverkas och kan om uppgifterna används för ett annat ändamål få förödande konsekvenser.

Säkerhetspolisen har från samverkande västerländska säkerhetstjänster information om att såväl inhemska terrorister i respektive hemland och internationella terrorister under den senaste 10-15-årsperioden visat intresse för och genomfört informationsinhämtning såväl digitalt som analogt rörande känsliga verksamheter som till exempel element inom olje-, gas- och elinfrastrukturerna i samband med planering av sabotageangrepp på dessa verksamheter. Dessa sabotageförsök har dess bättre alltid kunnat förhindras.

Uppgifter inom områdena telekommunikation, energiförsörjning, vattenförsörjning och transporter är särskilt skyddsvärda. Att göra uppgifter tillgängliga i den utsträckning som avses i förslaget skulle öka sårbarheten för många samhällsviktiga funktioner.

Säkerhetspolisen vill framhålla vikten av att säkerhetsfrågan utreds innan lagförslagen genomförs, eftersom det i detta sammanhang är

---

<sup>1</sup> Som exempel på avvägningsproblematiken mellan att tillgodose att medborgarna får nödvändig information och att motverka att antagonister som förbereder sig för sabotage inte skall få tillgång till information som sedan kan utnyttjas för sabotage, kan nämnas följande. Den 13 maj 2000 exploderade ett lager med fyrverkeripjäser i Enschede i Holland. 22 personer dog och 947 personer skadades. Cirka 1500 hem skadades eller förstördes vilket ledde till att 1250 personer blev hemlösa. Händelsen ledde till en lag som innebär att alla holländska medborgare hade rätt att ta del av vilka och hur allvarliga riskerna var i närmiljön med avseende på farligt gods. Riskerna presenterades via ett GIS-användargränssnitt på Internet för varje provins. Den holländska staten ansåg dock att den publika tillgången på information om risker också kunde utgöra ett hot mot säkerheten, vilket ledde till en debatt i den holländska riksdagen. Debatten ledde till att riksdagen den 9 september 2005 fattade ett beslut som innebär att man var tvungen att ta bort sådan information på Internet som potentiellt sett skulle kunna användas negativt av en angripare. Initialt vägrade provinserna ta bort den känsliga informationen. Den 14 oktober 2005 greps sju personer med kopplingar till terrorism för att ha förberett attacker mot den holländska riksdagen och den holländska säkerhetstjänsten. Den 1 januari 2006 togs den känsliga informationen bort från Internet. Se vidare Claudia Basta, Jeroen M.M. Neuvel, Sisi Zlatanova, Ben Ale, Risk-maps informing land-use planning processes. A survey on the Netherlands and the United Kingdom recent developments, Journal of Hazardous Materials, 145, (2007) 241–249.

Datum  
2009-03-24

betydelsefullt att uppgiften inte blir röjd, dvs. aldrig har publicerats på den förslagna portalen.

### **Synpunkter rörande författningsförslagen**

#### *Begränsningar av informationsansvarigas skyldigheter*

Säkerhetspolisen är medveten om att de aktuella författningsförslagen är avsedda att implementera ett tvingande direktiv och att utrymmet för nationella anpassningar därmed är begränsat. Det är dock viktigt att innebörden av den svenska författningstexten inte går utöver de minimikrav direktivet uppställer utan att detta första grundligt analyserats.

I detta sammanhang noterar Säkerhetspolisen att det i 2 kap. 7 § p. 2 den föreslagna miljöinformationslagen föreskrivs att fullgörandet av informationsansvar avseende information om utsläpp i miljön inte får begränsas med stöd av 6 § *första stycket* eller andra stycket 1, 3, 5 eller 6. Hänvisningen i 7 § p. 2 till 6 § första stycket medför att fullgörandet av informationsskyldighet beträffande utsläpp i miljön enligt förslaget *inte* får begränsas med hänsyn till internationella förbindelser, allmän säkerhet eller nationellt försvar. Enligt direktivet är det emellertid möjligt att begränsa informationsskyldigheten på dessa grunder (jfr att art. 13.2 direktivet hänvisar till punkterna 1 a, d, f, g och h samma artikel, men däremot inte till artikelns första stycke, som behandlar begränsningar med hänsyn till internationella förbindelser, allmän säkerhet och nationellt försvar).

Dessutom är 2 kap. 6-7 §§ den föreslagna miljöinformationslagen formulerade på ett sätt som får det att framstå som att möjligheterna att begränsa fullgörandet av informationsansvar är mer restriktiva enligt svensk lag än enligt direktivet (jfr formuleringen "*får fullgörandet begränsas endast i den mån...kan skada*" i 2 kap. 6-7 §§ den föreslagna miljöinformationslagen med formuleringen "*utan hinder av...får medlemsstaterna begränsa...om tillgången skulle inverka negativt*" i art. 13 direktivet).

Det är olyckligt om svensk lag i nämnda avseenden går utöver de minimikrav som anges i direktivet. 2 kap. 6-7 §§ den föreslagna miljöinformationslagen bör därför omformuleras så att bestämmelserna överensstämmer med direktivet.

Slutligen är det enligt Säkerhetspolisens mening angeläget att det i författningstexten, eller i vart fall i författningskommentaren, anges att skyddet av rikets säkerhet ska tillmätas särskild betydelse vid en intresseavvägning enligt 2 kap. 7 § den föreslagna miljöinformationslagen.

Datum  
2009-03-24

### *Övriga synpunkter*

Ovan har redogjorts för vikten av att noggrant analysera säkerhetsskyddsaspekterna innan information görs tillgänglig. Det är de myndigheter, kommuner och de andra organ som omfattas av miljöinformationslagen och –förordningen som enligt författningsförslagen har att göra de svåra överväganden som författningsförslagen innebär. Enligt Säkerhetspolisens mening är det av största vikt att myndigheterna m.fl. genom utförliga förarbeten får vägledning i fråga om hur lagen och förordningen ska tillämpas, hur bestämmelserna hänger samman med säkerhetsskyddslagstiftningen, sekretesslagstiftningen och annan lagstiftning som rör skyddet mot terrorism och skyddet för rikets säkerhet samt, inte minst, hur olika intressen ska vägas mot varandra vid intresseavvägningen vid begränsning av fullgörandet av informationsskyldigheten.

Säkerhetspolisen anser också att det i miljöinformationsförordningen bör anges hur 2 kap. 5 § förordningen förhåller sig till sekretesslagens bestämmelser samt att det i både lag och förordning bör införas tydliga definitioner som överensstämmer med direktivet (det saknas bland annat en tydlig definition av begreppet *metadata* i både lagen och förordningen).

Det bör också i förarbetena förtydligas i vilken utsträckning författningsförslagen avser reglering av bestämmelser som för närvarande finns i lagen (2005:181) om miljöinformation hos vissa enskilda organ respektive vilka bestämmelser som är avsedda att genomföra Inspire-direktivet i svensk lagstiftning.

Slutligen noteras, med anledning av vad Miljödepartementet vid Geodatarådets seminarium uppgett om att införandet av direktivet ska ske utifrån ett användarperspektiv, att man i det underlag som finns inte har påvisat på vilket sätt förslagen innebär en hjälp för enskilda och företag utanför kommuner respektive utanför Sverige. Även om regler m.m. ska förenklas i den utsträckning som är möjlig bör man hålla i minnet att de sekretessbegränsningar, begränsningar i behandling av personuppgifter och hanteringsregler avseende hemliga uppgifter som finns idag har ett legitimt syfte, nämligen att skydda ett intresse.

### **Kostnads- nyttoanalysen**

Eftersom den kostnads-nyttoanalys som gjorts av Lantmäteriet har betydelse såväl ur finansieringsperspektiv som ur andra hänseenden, vill Säkerhetspolisen lämna följande kommentarer rörande analysen.

De organisationer som belyses i analysen representerar bara en liten homogen grupp av intressenter som inte avspeglar de potentiella teman som anges i Inspire-direktivets bilaga 3, punkterna 6 (Allmännyttiga och offentliga tjänster) och punkten 8

Datum  
2009-03-24

(Produktionsanläggningar och industrianläggningar). De organisationer som ingår i analysen är Boverket, Enveco Miljöekonomi AB, ESRI S-GROUP, Krisberedskapsmyndigheten, Lantmäteriet, Lunds kommun, Sveriges Geologiska Undersökningar, SWECO Position AB samt Vägverket. Inga av dessa organisationer har verksamhet inom till exempel energiförsörjning och vattenförsörjning eller förfogar över industrianläggningar. Inom dessa typer av verksamheter läggs funktionell information om systemen ofta tillsammans med rumslig information. Denna funktionella information är ofta säkerhetskänslig ur såväl ett spionage- som sabotageförberedande perspektiv. Eftersom analysen inte omfattar denna typ av verksamhet har slutsatserna angående nyttan och konsekvenserna av direktivets genomförande dragits på grundval av ett ofullständigt underlag.

När det gäller finansieringsperspektivet noteras att kostnads- och nyttoanalysen inte innehåller uppskattningar av kostnader för eventuella säkerhetsincidenter som rör t ex sabotageförberedelser.

---

Detta yttrande har beslutats av säkerhetspolischefen Anders Danielsson. I den slutliga handläggningen har polisöverintendenten Doris Högne Rydheim, chefsjuristen Lars-Åke Johansson, polisintendenten Per Kihlström och chefsanalytikern Henrik Christiansson deltagit. Föredragande har varit verksjuristen Pia Cedermark.

Anders Danielsson

Pia Cedermark

Kopia till Justitiedepartementet, enheten för polisfrågor