Myndigheten för samhällsskydd och beredskap, MSB

Förslag till Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet och föreskrifter om it-säkerhet för statliga myndigheter

Datainspektionen har granskat förslagen utifrån myndighetens uppgift att arbeta för att människors grundläggande fri- och rättigheter skyddas i samband med behandling av personuppgifter (dataskyddsperspektivet). Datainspektionen har också granskat förslagen utifrån att myndigheten omfattas av kraven i de remitterade förslagen.

Datainspektionen tillstyrker i allt väsentligt förslagen då ett strukturerat och riskbaserat informationssäkerhetsarbete är en av förutsättningarna för ett gott integritetsskydd. Tydliga föreskrifter, som de som föreslås, bidrar till att klargöra vad ett sådant arbete innebär och vad som förväntas av de berörda myndigheterna.

Datainspektionen lämnar följande synpunkter.

Flera perspektiv behöver beaktas vid bedömning av vilka säkerhetsåtgärder som är lämpliga. Bedömningen behöver ske utifrån såväl behovet av samhällsskydd i stort, myndigheternas verksamhetsskydd som utifrån ett dataskyddsperspektiv. Däremot kan behovet av vilken nivå av säkerhet som behövs variera beroende på utifrån vilket perspektiv som en riskanalys och lämplighetsbedömning genomförs. En lämplig åtgärd kan ur verksamhetsperspektiv vara mindre viktig i termer av vilken säkerhetsnivå som behöver uppnås (kanske på grund av att alternativa eller reaktiva åtgärder enkelt kan vidtas vid en incident) samtidigt som det utifrån ett dataskyddsperspektiv kan vara angeläget att åtgärden ger en hög nivå av skydd, eller vice versa.

I båda de remitterade föreskrifterna finns en bestämmelse om att om det i annan författning finns någon bestämmelse som avviker från bestämmelserna i förslagen så ska de avvikande bestämmelserna gälla istället (2 § respektive 1 kap. 2 §). Datainspektionen vill ändå påpeka att det finns en risk när tydliga och konkreta ”ska-krav” formuleras i subsidiära regelverk att de som ska tillämpa reglerna följer dem oreflekterat utan att beakta de regelverk som ska prioriteras.

Ett sådant exempel är olika typer av loggar. När tekniska säkerhetsåtgärder vidtas innebär det ofta att personuppgifter behandlas. Sådan personuppgifts-behandling underkastas såväl de grundläggande principerna i dataskyddsförordningen (art. 5) som kraven på proportionalitet (art. 24) och lämplighet (art. 32). MSB har i förslaget till föreskrifter om it-säkerhet 4 kap. 33 § angett att dokumentation över vilka som beretts tillträde till särskilda it-utrymmen ska sparas i fem år. Utifrån dataskyddsförordningen behöver det ske en bedömning i de enskilda fallen hur länge det är lämpligt att spara loggar, så att det inte blir en alltför omfattande personuppgiftsbehandling.

Datainspektionen avstyrker därför förslaget såsom det är formulerat och föreslår istället att det anges att myndighetens särskilda it-utrymmen ska skyddas genom ett tillräckligt skalskydd, att tillträde till särskilda it-utrymmen ska registreras på individnivå och att myndigheten ska besluta om en lämplig bevarandetid för den dokumentationen.

Beträffande kraven på flerfaktorautentisering i 4 kap. 9 § punkten 3 i de föreslagna it-säkerhetsföreskrifterna har datainspektionen följande synpunkter. Vid en begäran om utlämnande av en allmän handling ska myndigheten göra en sekretessprövning enligt offentlighets- och sekretesslagen (2009:400) för att avgöra om handlingen kan lämnas ut helt eller delvis eller inte alls. Eftersom samma allmänna handling under olika omständigheter kan bedömas olika utgör sekretess en problematisk utgångspunkt för krav på säkerhetsåtgärder vid åtkomst till informationssystem. Om det med hänvisningen till sekretess menas information som utgör allmänna handlingar borde det framgå istället. Det kan dock ifrågasättas om en sådan föreskrift skulle vara nödvändig för alla statliga myndigheter.

De föreslagna föreskrifterna i 4 kap. 12 och 13 §§ om kryptering verkar ha samma sakliga innebörd. Den ena bestämmelsen borde därför kunna strykas. Om någon skillnad avses behöver det klargöras.

Beträffande kraven på säkerhetsloggning och realtidsövervakning i 4 kap. 26 § har datainspektionen samma synpunkter på punkten 1 som redovisats angående flerfaktorautentisering ovan. Datainspektionen anser därutöver att ordet ”rättigheter” inte är rätt ord i detta sammanhang utan föreslår istället att uttrycket ”åtkomstmöjligheter” alternativt ”behörigheter” används istället.

Detta beslut har fattats av enhetschefen Katarina Tullstedt efter föredragning av it-säkerhetsspecialisten Magnus Bergström. Vid den slutliga handläggningen har även it-säkerhetsspecialisten Johan Ma, informationssäkerhetsansvarig Lukas Elestedt och it-ansvarig Joakim Nyberg medverkat.

Katarina Tullstedt, 2020-02-14 (Det här är en elektronisk signatur)