Advokatfirman Kahn Pedersens skriftserie 2020:1

kahn pedersen

Juridisk informationssäkerhet

– Att samordna arbetet enligt säkerhetsskyddslagen, NIS-lagen, dataskyddsförordningen och annan lagstiftning om informationssäkerhet

Vi på Advokatfirman Kahn Pedersen ser det som en naturlig del av vår roll som specialistbyrå att delta i den offentliga diskussionen. Detta för att bidra till att föra fram och utveckla intressanta och inte sällan svåra rättsfrågor inom våra specialistområden. Ett led i detta arbete är denna skriftserie som publiceras med ett till två nummer per år. Tanken med skriftserien är att lite mer djupgående utreda aktuella och mer komplicerade rättsfrågor, som vi märker är av intresse för våra klienter och samhället i stort.

Eftersom målsättningen är att vårt arbete med rapporterna ska komma inte bara våra klienter och samarbetspartners till del, utan även ska kunna bidra till utvecklingen av de rättsområden som vi är specialiserade inom, tillhandahålls alla nummer av skriftserien kostnadsfritt på vår webbplats under en Creative Commons Erkännande-Inga Bearbetningar 4.0 Internationell Licens. Detta möjliggör mångfaldigande och spridning av materialet förutsatt att inga ändringar görs och att källan anges.

Ämnet för denna rapport, som har nummer 2020:1, är lagstiftarens och tillsynsmyndigheters reglering av informationssäkerhet och hur informationssäkerhetsarbetet enligt de olika regleringarna kan samordnas. Vi hoppas ni finner rapporten intressant.

ISBN 978-91-983215-8-6

1. Inledning

1.1 Varför en rapport om informationssäkerhet?

Informationssäkerhet blir allt viktigare i takt med att samhället blir mer och mer digitaliserat och sammankopplat. När informationssäkerheten brister drabbar det den part som ansvarat för exempelvis ett visst it-system, men även alla de vars information hanteras i systemet. För ett företag som ansvarar för sin egen affärskritiska information finns det ett tydligt kommersiellt intresse av att hålla informationssäkerheten på en hög nivå. Detta eftersom den direkta kostnaden för ett dataintrång eller extern manipulation kan vara mycket omfattande, och kan i de värsta fallen utgöra ett existentiellt hot mot företaget.

I andra fall kan skadan av en informationssäkerhetsincident drabba enskilda fysiska personer, nationella intressen eller andra skyddsvärden utanför företagets egna verksamhet. Det räcker därför inte att förlita sig på att företag i allmänhet strävar efter att minska sina kostnader för att se till att samhällets totala informationssäkerhet är på en tillräckligt hög nivå. Det kan krävas ytterligare incitament i form av reglering och sanktioner för att företag ska skydda även dessa värden.

På samma sätt behövs incitament för myndigheter och övriga aktörer för att prioritera informationssäkerhet. Informationssäkerhet är därför föremål för omfattande och växande regleringar. Dessa regleringar ålägger olika verksamheter skyldigheter att vidta åtgärder som ska gagna informationssäkerheten i verksamheten, ibland genom att till och med begränsa verksamheternas möjlighet att alls hantera viss information.

Regleringarna har olika avsändare och tar sikte på skilda skyddsintressen. Vi har skrivit den här rapporten för att ge en samlad bild av vilka krav på informationssäkerhet som dessa regleringar ställer. Vi har försökt att belysa de svårigheter som finns för verksamhetsansvariga att ta reda på vilka krav som ställs, men också hur dessa krav kan tillgodoses. Ett särskilt fokus har varit att behandla de potentiella konflikter som kan uppstå när olika regelverk ska tillämpas samtidigt.

Det primära syftet med rapporten är att tydliggöra och underlätta det juridiska informationssäkerhetsarbetet när flera lagstiftningar som rör informationssäkerhet är tillämpliga, med ett särskilt fokus på hur sådant arbete kan samordnas.

Målet är att en verksamhet inte ska behöva ha ett arbetssätt eller en process för att uppfylla en informationssäkerhetsreglering, en annan separat process för att uppfylla en ytterligare informationssäkerhetsreglering, en tredje för att uppfylla affärsmässiga krav, och så vidare. Såvitt vi känner till, har det tidigare inte tagits något samlat helhetsgrepp på detta område och det finns därför ett behov av att ge en

överskådlig bild av de frågeställningar och regelverk som dagens verksamheter möter. Vi avslutar därför rapporten med ett förslag på en process för att, på en översiktlig och samordnad nivå, uppfylla de juridiska informationssäkerhetskraven.

Den här rapporten är skriven av Kahn Pedersen, en advokatfirma som bl.a. ger rådgivning till klienter om hur de ska gå tillväga för att uppfylla legala informationssäkerhetskrav. Rapporten riktar sig i första hand till personer som arbetar med de legala aspekterna av informationssäkerhet, varför rapporten har en i allt väsentligt juridisk prägel. Informationssäkerhet som disciplin är dock inte i första hand en juridisk fråga, och inte heller nödvändigtvis en it-fråga.[1] Området har sina egna fundamentala begrepp, modeller och *best practices* som bara delvis speglas i tillämplig lagstiftning. Vi inleder därför med en allmän introduktion om vad informationssäkerhet egentligen är, som ett underlag till att bättre kunna förstå och tillämpa lagstiftningen.

1.2 Vad är informationssäkerhet?

Det är själva informationen som är i fokus för informationssäkerhetsarbete, inte de verksamhetsprocesser som skapar, samlar in, använder, förvaltar och avvecklar/förstör informationen. Men givet att det i ett visst sammanhang, exempelvis i ett it-system, finns information, så handlar informationssäkerhet i det sammanhanget även om att säkerställa denna informations konfidentialitet, riktighet och tillgänglighet. I regel talas det om den engelska beteckningen *CIA-triaden* (Confidentiality, Integrity, Availability). Dessa grundläggande begrepp kan beskrivas[2] enligt följande:

- **Konfidentialitet**: Informationen ska inte göras tillgänglig för andra personer, system eller processer än de som har behörighet att få tillgång till den.

- **Riktighet**:[3] Informationen ska inte ändras, läggas till eller raderas på annat sätt än av behöriga personer m.m. enligt bestämda rutiner. Detta syftar i slutändan till att säkerställa att informationen är korrekt för de ändamål som den behandlas för.

- **Tillgänglighet**: Informationen ska vara formellt och praktiskt åtkomlig för behöriga personer, system och processer under de tidsspann och med de hastigheter/volymer som har bestämts.

---

1 Det har förstås funnits reglering om informationssäkerhet långt innan det fanns datorer. Exempelvis innehöll en av föregångarna till vår tids offentlighets- och sekretesslag, lagen (1937:249) om inskränkningar i rätten att utbekomma allmänna handlingar, informationssäkerhetsavväganden till skydd för bl.a. rikets säkerhet.

2 Beskrivningarna av begreppen är våra egna och har valts för att vara så tydliga och förklarande som möjligt för den läsare som själv inte har praktisk erfarenhet från informationssäkerhetsarbete. Det finns andra definitioner av begreppen, exempelvis i den tekniska rapporten Terminologi för informationssäkerhet (SIS-TR 50:2015) eller den internationella standarden SS-EN ISO/IIC 20700:2017. Myndigheten för samhällsskydd och beredskaps (MSB) rapport ”Terminologi och begrepp inom informationssäkerhet – Hur man skapar en språkgemenskap” (MSB976, 2016) ger en kompletterande bild över vissa av dessa grundläggande begrepp används i olika yrkeskategorier.

3 Tidigare användes ofta den mer direktöversatta termen Integritet för detta begrepp.

En stor del av informationssäkerhetsarbetet handlar om att analysera såväl risker som möjliga åtgärder (säkerhetsåtgärder) för att hantera riskerna utifrån dessa grundläggande egenskaper. En identifierad risk kan exempelvis vara att informationens konfidentialitet kan brista på grund av nyupptäckta säkerhetsbrister i någon programvara i den kedja som levererar informationen. Säkerhetsåtgärder som hanterar en sådan risk kan då vara rutiner som garanterar snabb uppdatering (patchning) av den programvara som används, eller att förändra nätverkskonfigurationen så att endast de system som behöver utbyta information med varandra kan upprätta nätverksförbindelser.[4] Det kan även handla om rutiner kring hur information i fysisk form skyddas, exempelvis om och när pappershandlingar ska förvaras i säkerhetsskåp. En grundläggande åtgärd är att fastställa vem som ansvarar för säkerheten av vilken information.

Utöver de grundläggande begreppen i CIA-triaden finns även en uppsättning kompletterande faktorer som ingår i informationssäkerhetsbegreppet. Med vägledning av Terminologi för informationssäkerhet (SIS-TR 50:2015), följer här en icke-uttömmande beskrivning av olika sådana faktorer:

- **Oavvislighet**: Förmågan att kunna säkerställa vilka handlingar som skett och inte skett, samt deras ursprung.

- **Spårbarhet**: Förmågan att kunna säkerställa vilken identifierad användare som har utfört vilka aktiviteter i systemet.

- **Ansvarsskyldighet**: Principen att stå till svars och ta ansvar för konsekvenserna av beslut och aktiviteter.

- **Autenticitet**: Egenskapen att uppgifter är äkta, särskilt vad gäller identitet, ursprung och innehåll.

- **Auktorisation**: Att kunna fastställa vilka behörigheter som ska gälla för personer, system eller processer i relation till informationen.

- **Robusthet**: Förmåga att kunna hantera störningar utan att dessa leder till större informationssäkerhetsförlust (termen motståndskraft används ofta med i stort sett samma betydelse).

1.3 Vad hotar informationssäkerheten?

Eftersom informationssäkerhet handlar om att säkerställa informationens konfidentialitet, riktighet och tillgänglighet blir nästa fråga vad som kan hota dessa egenskaper. Det generella svaret är att det beror på informationen som sådan, dess roll i olika processer, externa förutsättningar och mycket mer. Syftet med en riskanalys är därför att hitta de specifika hoten mot en verksamhets information.

4 Observera att ingen av dessa åtgärder eliminerar den beskrivna risken fullständigt, utan minskar bara sannolikheten för att en skada ska inträffa.

Med detta sagt, kan vi på ett övergripande plan ändå nämna några kategorier av generella hot:

- Interna handhavandefel avser fall när konfiguration och administration av informationssystem inte utförs på rätt sätt. Det kan exempelvis vara fråga om bristande backuprutiner som leder till dataförlust (en oavhjälplig och permanent brist i tillgänglighet), integrationer mellan två system där konverteringen av data inte görs på rätt sätt som leder till brister i riktighet, eller felaktiga brandväggs- eller autentiseringsinställningar som gör en informationsmängd tillgänglig för personer – i värsta fall hela internet – som inte ska ha tillgång, vilket utgör en konfidentialitetsbrist.

- Externa generella attacker avser fall när en utomstående satt igång ett förlopp som leder till bristande informationssäkerhet genom att utnyttja generella brister i programvara eller konfiguration av it-system (eller dess användare). Det kan exempelvis röra sig om virusangrepp, nätfiske eller utpressningsprogram.[5]

- Riktade attacker avser fall när kunskap om enskilda personer och organisationer samt deras informationshantering används för att anpassa attacktekniker till just dessa förutsättningar. Sådana attacker har ofta inslag av ”social engineering”, vilket något förenklat innebär att personer inom en organisation luras att utföra åtgärder genom sina behörigheter (exempelvis ladda ner och köra ett program från angriparen). Dessa åtgärder ger i sin tur angriparen någon form av access till ett informationssystem inom organisationen.

1.4 De centrala lagstiftningarna inom informationssäkerhet

I denna framställning har vi valt att koncentrera oss på framför allt tre regelsystem:

- Säkerhetsskyddslagen (2018:585) och författningar som meddelats med stöd av denna lag.

- Lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster (fortsättningsvis ”**NIS-lagen**”) med bakomliggande EU-direktiv (”**NIS-direktivet**”)[6] och andra författningar som meddelats med stöd av denna lag.

- Dataskyddslagstiftningen med utgångspunkt från den allmänna dataskyddsförordningen, populärt benämnd GDPR (”**dataskydds-**

5 Med nätfiske (phishing) avses att lura till sig information, exempelvis lösenord, med bedrägliga metoder, exempelvis genom e-post med falsk avsändare. Med utpressningsprogram (ransomware) avses skadlig programvara som krypterar ett offers filer så att de blir oanvändbara, för att sedan kräva en lösensumma för att avslöja den dekrypteringsnyckel som sägs kunna återställa filerna.

6 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.

förordningen”), och nationell kompletterande lagstiftning, framför allt lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning (”**dataskyddslagen**”).

Gemensamt för de tre regleringarna är att de strävar efter att skydda ett visst värde (enskildas fri- och rättigheter, tillgängligheten till och motståndskraft hos vissa viktigare tjänster, eller Sveriges säkerhet) där informationssäkerhet är en central del för att uppnå detta skydd, och att det därför finns anledning att reglera formerna för hur denna informationssäkerhet ska säkerställas. De tre olika regelsystemen skiljer sig dock mycket åt i hur detaljerade och konkretiserade kraven på säkerhetsåtgärder är.

Utöver dessa tre stora system finns även en mängd av mer specifik lagstiftning som rör informationshantering och säkerhet inom specifika sektorer, t.ex. för banker, hälso- och sjukvård, myndigheter i stort samt elektronisk kommunikation. Det finns även myndigheter och institutioner som har till syfte att underlätta informationssäkerhetsarbete, vilka också styrs av lagstiftning. Sådan lagstiftning påverkar direkt eller indirekt vilka säkerhetsåtgärder som bör eller måste vidtas av olika aktörer i olika verksamheter.

Syftet med att behandla samtliga dessa regelverk i ett samlat sammanhang är att den enskilde verksamhetsutövaren inte kan nöja sig med att bara fokusera på ett av dem för att uppfylla krav på regelefterlevnad. Istället måste verksamhetsutövaren bedöma i vilken utsträckning respektive regelverk ska tillämpas på varje enskild del av verksamheten, och vid behov hantera konflikter mellan regelverken.

1.5 Ett systematiskt och riskbaserat informationssäkerhetsarbete

I Myndigheten för samhällsskydd och beredskaps (MSB) föreskrifter och i NIS-lagen ställs krav på ett systematiskt och riskbaserat informationssäkerhetsarbete. I detta avsnitt utgår vi från dessa begrepp för att beskriva hur informationssäkerhetsarbete vanligen bedrivs.

1.5.1 VAD INNEBÄR SYSTEMATISKT?

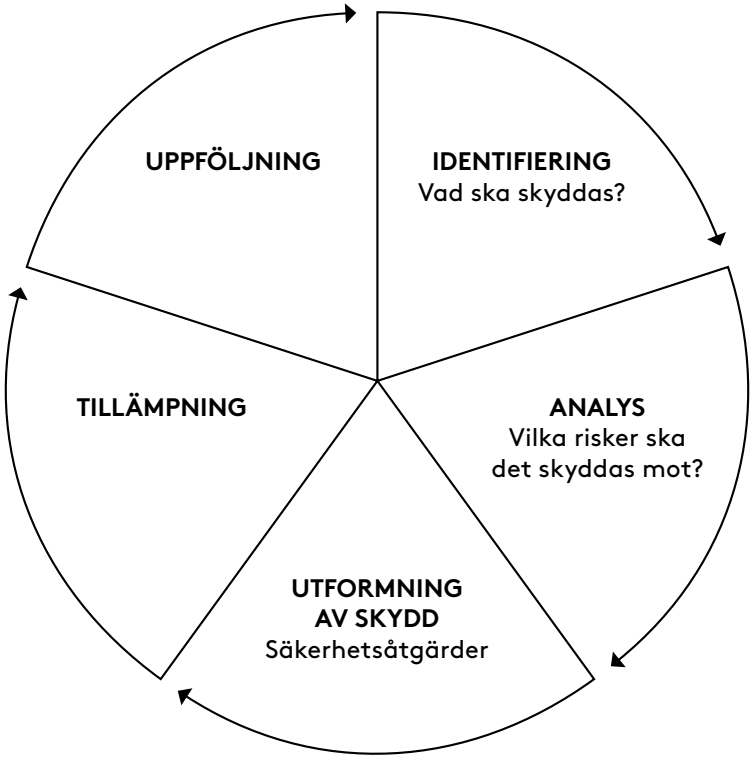
Med ett systematiskt informationssäkerhetsarbete avses att man arbetar strukturerat efter en bestämd process i syfte att planera, genomföra, kontrollera, följa upp, utvärdera och förbättra säkerheten i verksamhetens informationshantering. Vidare krävs att arbetet bedrivs långsiktigt, kontinuerligt och metodiskt samt att det finns en tydlig rollfördelning med särskilt utpekat ansvar. Myndigheter har länge varit ålagda att arbeta med informationssäkerheten på ett strukturerat sätt.[7] I och med NIS-regleringen har denna skyldighet

7 5 § i MSB:s föreskrifter om statliga myndigheters informationssäkerhet, MSBFS 2016:1.

även utsträckts till leverantörer av samhällsviktiga tjänster.[8] Men även utanför det reglerade området är det förstås vanligt att informationsarbete bedrivs på ett systematiskt sätt, exempelvis genom användning av ledningssystem för informationssäkerhet (se avsnitt 1.5.3 nedan).

De regelverk som vi går igenom i denna rapport har inslag av en sådan struktur på detaljerad eller generell nivå. Ett tydligt exempel är hur en säkerhetsskyddsanalys ska genomföras av den som utövar en säkerhetskänslig verksamhet.

Oavsett var och i vilken detaljeringsgrad ett systematiskt informationssäkerhetsarbete regleras kan det i allmänhet beskrivas i form av en cirkel:



Formen av en cirkel är viktig för att understryka att det är ett löpande arbete, inte en enstaka insats. Det är också en iterativ process där erfarenheter bör tas till vara för att ständigt förbättra arbetet.

En utgångspunkt för att arbeta systematiskt med informationssäkerhet är MSB:s metodstöd för systematiskt informationssäkerhetsarbete,[9] vilket i sin tur bygger på ISO 27000-serien.[10] En framgångsfaktor och viktig komponent i modeller för systematiskt informations-

8 11 § NIS-lagen.

9 Metodstödet finns beskrivet och dokumenterat på https://www.informationssakerhet.se/metodstodet/.

10 Angående ISO 27000-serien, se nedan avsnitt 1.5.3.

säkerhetsarbete är stöd i form av resurser, kompetenser, tilldelade roller och ansvar, samt förankring på ledningsnivå av arbetet. En viktig förutsättning är att informationssäkerhet inte bedrivs som ett internt arbete enbart inom it-avdelningen eller enbart inom juristavdelningen i en organisation.

1.5.2 VAD INNEBÄR RISKBASERAT?

Att arbetet bedrivs riskbaserat innebär att man försöker identifiera, värdera och analysera olika risker, för att anpassa vilka skyddsåtgärder som ska vidtas utifrån denna analys. På så vis kan säkerhetsåtgärderna anpassas till riskerna, så att ett så ändamålsenligt skydd som möjligt uppnås.

Det är exempelvis inte motiverat att införa mycket omfattande behörighetssystem för att garantera att en anställd aldrig någonsin har teknisk åtkomst till information som denne inte behöver för sina arbetsuppgifter, om informationen i fråga inte är känslig eller om bristande riktighet i informationen inte kan leda till särskilt stora skador. De kostnader som en sådan säkerhetsåtgärd kan medföra (startkostnader och löpande kostnad i form av support, lägre produktivitet m.m.) kan annars bli högre än kostnaden av den skada som blir följden av om en oönskad händelse med negativa konsekvenser inträffar.

I vissa sammanhang går det att sätta en prislapp på en identifierad risk genom att multiplicera kostnaden för organisationen om risken inträffar med sannolikheten för att risken förverkligas. En tänkt skyddsåtgärd kan därefter utvärderas utifrån hur mycket den minskar denna prislapp (eller om den kanske eliminerar risken helt). I andra sammanhang, särskilt om verksamheten omfattas av säkerhetsskyddslagen, kan sannolikheten vara närmast oväsentlig eftersom den riskanalys som ska utföras där utgår från konsekvenserna, med ett ytterst begränsat utrymme för organisationen att själv välja risknivå (se vidare avsnitt 7.4.2).

Om kostnaden för en viss risk faller på organisationen själv (exempelvis risken att en e-handelswebbplats görs otillgänglig till följd av ett externt angrepp, vilket medför en kvantifierbar kostnad för organisationen) är det möjligt att helt enkelt göra en bedömning av om det är företagsekonomiskt lönsamt att vidta säkerhetsåtgärden. Samma förhållningssätt kan användas för att välja bland flera tänkbara skyddsåtgärder som adresserar hot.

I andra fall är det inte organisationen som lider skada när risken realiseras. Om exempelvis vårdjournaler läcker är det i första hand patienterna som lider den direkta skadan, inte organisationen som sådan. I vissa fall kan lagstiftning eller avtal återföra kostnaden för risken till organisationen (exempelvis genom dataskyddsförordningens utrymme för sanktionsavgifter eller skadestånd). I andra fall kan dock riskerna inte mätas i pengar, exempelvis vad gäller skada på Sveriges säkerhet. I sådana situationer kan ovan nämnda avvägningar inte göras utan

det är i dessa fall därför viktigt att riskanalysen tar med alla relevanta risker, inte bara sådana som träffar den egna organisationen.

1.5.3 LEDNINGSSYSTEM FÖR INFORMATIONSSÄKERHET ENLIGT ISO

Lagstiftaren är inte den första att försöka skapa normer om vad som är en acceptabel informationshantering utifrån säkerhetssynpunkt. Konkreta riktlinjer, krav, standarder och hjälpmedel har utvecklats under lång tid inom bl.a. it-branschen.

Att arbeta med informationssäkerhet inom en organisation på ett systematiskt och riskbaserat sätt kräver att arbetet följer processer och rutiner. En beskrivning av processer för en viss inriktning, tillsammans med övergripande policyer och tilldelade roller och ansvarsområden kallas för ledningssystem. Begreppet ledningssystem används på många andra ställen inom organisationer, exempelvis för kvalitet, miljö och arbetsmiljö.

Ett ledningssystem för informationssäkerhet (”**LIS**”) utgörs alltså av en uttalad beskrivning av vilka rutiner och processer som används för att uppnå eller upprätthålla en önskad grad av informationssäkerhet. Ledningssystemet och de ingående processerna måste anpassas till organisationens förutsättningar, inkluderat vilka krav som med hänsyn till verksamheten bör ställas.

ISO 27000-standardserien utgör en standard för sådana ledningssystem. Den säger egentligen inte hur ett färdigt ledningssystem ska se ut och fungera, men den innehåller en uppsättning krav som ett sådant ledningssystem ska uppfylla (ISO/IEC 27001).[11] Utöver denna kärna innehåller standarden även en uppsättning gemensamma definitioner (ISO/IEC 27000)[12] och en katalog över informationssäkerhetsåtgärder (ISO/IEC 27002).[13] Standardserien innehåller även en vägledning (ISO/IEC 27003) till de krav som ställs, och kan ses närmast som en kommentar till den normativa text som ISO/IEC 27001 utgör. Utöver dessa kärndokument finns även ett fyrtiotal ytterligare standarder i serien som tar sikte på vissa specifika aspekter av LIS, exempelvis hur man mäter och utvärderar funktionen i ett LIS, samt hur revision och certifiering av ett LIS ska utföras.

Det är inte nödvändigt att en verksamhetsutövare följer just ISO 27000-serien för att kunna hävda att denna bedriver ett systematiskt och riskbaserat informationssäkerhetsarbete. Det är inte heller nödvändigt att verksamhetsutövaren formellt inrättat någon annan typ av ledningssystem. En fördel med just ISO 27000-serien är dock att det ledningssystem som införts kan certifieras, varpå verksamhets-

11 Utgör även svensk standard under beteckningen SS-EN ISO/IEC 27001:2017, med titeln Ledningssystem för informationssäkerhet – Krav.

12 SS-ISO/IEC 27000:2018, I-Ledningssystem för informationssäkerhet – Översikt och terminologi.

13 SS-EN ISO/IEC 27002:2017, Riktlinjer för informationssäkerhetsåtgärder.

utövaren kan få en försäkran från en utomstående part om att informationssäkerhetsarbetet håller en viss nivå. Detta kan utgöra såväl en rent kommersiell fördel som ett sätt för verksamhetsutövaren att visa för en tillsynsmyndighet att verksamheten bedrivs på ett sätt som skapar en presumtion för att även lagkrav följs.[14]

1.6 Juridisk informationssäkerhet

Informationssäkerhet i sin klassiska bemärkelse handlar till stor del om att bevara informationens önskade egenskaper på ett tekniskt plan. När informationssäkerheten regleras, i lag eller i avtalsrelationer, uppstår även frågor som kan sorteras in under begreppet *juridisk informationssäkerhet*. Vi som rapportförfattare ser ett behov av detta begrepp som ett komplement till teknisk informationssäkerhet och föreslår därför följande definition:

Juridisk informationssäkerhet: *Att säkerställa att information hanteras under känd jurisdiktion utan konflikt med tillämpliga rättsregler för informationsinnehavaren.*

Ett allt mer aktuellt exempel på vikten av juridisk informationssäkerhet är om ett svenskt företag vill använda sig av en amerikansk molntjänst för att hantera viss information som kan innehålla personuppgifter. Enligt dataskyddsförordningen kommer det svenska företaget i typfallet vara personuppgiftsansvarig och molntjänstleverantören kommer vara personuppgiftsbiträde. Enligt dataskyddsförordningen krävs att den personuppgiftsansvariga bara anlitar sådana personuppgiftsbiträden som kan uppfylla de krav som ställs i dataskyddsförordningen. Detta måste framgå av faktiska, sanktionerade och rättsligt giltiga avtalsvillkor. En amerikansk molntjänstleverantör kan dock, även om informationen fysiskt är belägen i datacenters inom EU, bli tvungen att med stöd av den s.k. Cloud Act[15] lämna ut uppgifter till amerikanska myndigheter utan inblandning eller rättslig bedömning av europeiska myndigheter. Detta skulle sannolikt strida mot dataskyddsförordningens regler om tredjelandsöverföring. I en sådan situation är det inte möjligt för den personuppgiftsansvarige att garantera att personuppgifterna kommer att behandlas i enlighet med dataskyddsförordningen.[16] Det är i dagsläget svårt att säga hur man ska kunna garantera juridisk informationssäkerhet i en sådan situation, vilket i

14 Det bör dock i sammanhanget understrykas att en ISO 27001-certifiering i dagsläget inte utgör en sådan godkänd certifieringsmekanism som avses i dataskyddsförordningens artikel 42. Det utgör däremot en stark presumtion för att man uppfyller NIS-regleringens krav på att bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete (11 § NIS-lagen).

15 Cloud Act, eller CLOUD Act, är benämningen på den amerikanska lagen Clarifying Lawful Overseas Use of Data Act, som antogs under 2018 av den amerikanska kongressen. Bakgrunden till lagen var en amerikansk domstolsprocess där en leverantör vägrade lämna ut en privatpersons uppgifter som lagrades på en server i Irland till amerikanska Justitiedepartementet. Genom Cloud Act tydliggörs att Stored Communications Act, som bl.a. ger amerikanska myndigheter rätt att begära ut uppgifter som lagras hos leverantörer, är tillämplig även när uppgifterna lagras i ett annat land.

16 Se EDPB-EDPS Joint Response to the LIBE Committee on the impact of the US Cloud Act on the European legal framework for personal data protection, https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb-edps-joint-response-libe-committee-impact-us-cloud-act_sv.

sin tur har givit upphov till en intensiv debatt om möjligheterna att använda amerikanska molntjänster för hantering av personuppgifter.[17]

Ett annat exempel på juridisk informationssäkerhet är situationen där ett kreditinstitut vill utkontraktera delar av sin it-drift. Kreditinstitutet är bundet av Finansinspektionens föreskrifter som bl.a. kräver att företaget, dess revisorer och Finansinspektionen har tillgång till uppgifter om den utlagda verksamheten samt tillträde till uppdragstagarens lokaler.[18] Standardavtalen för typiska molntjänster medger sällan att kunder har tillträde till leverantörens lokaler. Ett sätt att i denna situation garantera juridisk informationssäkerhet skulle kunna vara att förhandla fram ett tillägg till standardavtalet enligt vilket molntjänstleverantören garanterar att företaget, dess revisorer och Finansinspektionen har rätt att utföra de revisioner och inspektioner som krävs för att kontrollera såväl själva utkontrakteringslösningen som verksamhetsutövaren.

Det ska understrykas att juridiskt informationssäkerhetsarbete inte står i konflikt med traditionellt informationssäkerhetsarbete. I alla etablerade modeller och processer för informationssäkerhetsarbete ingår att man i en analysfas kartlägger även de rättsliga krav som är tillämpliga för verksamheten. Som ett komplement kan det dock vara givande att börja analysen utifrån rättsordningens systematik. I avsnitt 7.3 beskriver vi en modell för samordnad juridisk informationssäkerhet.

1.7 Disposition för den fortsatta framställningen

För att underlätta den fortsatta läsningen ska något sägas om dispositionen och strukturen i de kommande avsnitten 2–4. Vår ambition är att denna struktur ska underlätta ett systematiskt angreppssätt för informationssäkerhetsarbetet inom respektive regelsystem.

Inledande avsnitt

Varje avsnitt inleds med en presentation av det aktuella regelverket, bakgrunden till regelverket och en förenklad beskrivning av vad reglerna handlar om.

Regleringens avgränsningar

Denna del kommer främst att fokusera på tre aspekter som är särskilt relevanta för att utreda vilka avgränsningar som görs i respektive

17 Se bl.a. eSams juridiska expertgrupps uttalande om röjande och molntjänster (2018), http://www.esamverka.se/stod-och-vagledning/rattsliga-uttalanden/rojande-och-molntjanster.html och SKL:s ställningstagande om informationshantering i vissa molntjänster (2019), https://skr.se/tjanster/press/nyheter/nyhetsarkiv/molntjansternodvandigaforfortsattdigitalisering.27627.html. Läst den 24 februari 2020.

18 10 kap. 5 § 9 p. FFFS 2014:1.

regelsystem. Det handlar om *tillämpningsområdet* som sådant, vilket *skyddsintresse* som respektive regelverk ska skydda och *hotbilden* som föranleder skyddsbehovet.

Process

Det är svårt att uppnå eller upprätthålla informationssäkerhet utan en process för informationssäkerhetsarbetet. Regelsystemen ställer i detta avseende olika krav och det varierar kraftigt hur detaljerat kraven formuleras, men vissa gemensamma hållpunkter går att finna.

Först ska någonting *identifieras*, t.ex. vad det är som ska skyddas. Därefter ska detta något *analyseras*. Denna analys rör typiskt sett risker eller potentiella skador. Utifrån analysen ska *skyddet utformas* och slutligen ska skyddet *tillämpas och/eller följas upp*.

Konkreta informationssäkerhetskrav

I vissa avseenden saknar regelverken, enligt vår uppfattning, önskvärd tydlighet kring hur regelverken ska tillämpas i praktiken. Det förekommer dock ett antal konkreta krav på olika skyddsåtgärder som ska vidtas i olika situationer. Dessa kommer att beskrivas i denna del, låt vara att vi inte vågar påstå att redogörelserna är uttömmande.

Vi går igenom varje reglerings modell för informationsklassificering och hur denna eventuellt är kopplad till de konkreta krav på skyddsåtgärder som finns i varje lagstiftning. De tre lagstiftningarna varierar mycket, både i hur informationsklassificering ska gå till och i vilken mån denna klassificering direkt eller indirekt styr vilka skyddsåtgärder som ska vidtas. För säkerhetsskyddet är denna process reglerad i detalj, medan det för dataskyddet handlar mer om att vidta ”lämpliga” åtgärder, där informationens känslighet bara är en av många faktorer som styr denna lämplighet. Generellt kan sägas att de analyserade hoten, tillsammans med informationens klassificering, har en mycket stor påverkan på vad som är adekvata skyddsåtgärder. På vissa områden har lagstiftaren gjort åtminstone delar av denna adekvansbedömning på förhand, och på andra områden är det upp till den ansvarige att göra det själv. Det går dock i större eller mindre utsträckning att identifiera vissa ”minimiåtgärder” som måste vidtas, på grundval av informationens klassificering eller andra faktorer. I avsnitt 7.3 beskriver vi en modell för att samordna informationssäkerhetsarbetet utifrån bl.a. dessa informationsklassificeringsmodeller och minimiåtgärder.

Gränssnitt mot myndigheter

Sist i varje avsnitt beskriver vi även de olika roller som vissa myndigheter har inom varje regelsystem, något som vi kallat för ”gränssnitt mot myndigheter”, eftersom de rör de regler som styr vilka möjligheter

och skyldigheter som finns för att interagera med myndigheter i sina olika roller. Denna del består av fyra olika aspekter som är relevanta för den som träffas av något av de olika regelverken.

Det är någon eller några myndigheter som har att utöva *tillsyn* inom respektive regelsystem, det ställs krav på hur *incidenter ska rapporteras* och i vissa fall måste det ske *samråd* med någon myndighet. Slutligen beskrivs de olika *sanktionsmöjligheterna*, även om förhoppningen är att läsaren inte ska behöva bekanta sig närmare med sanktionsmöjligheterna än genom denna rapport.

2. Informationssäkerhet enligt säkerhetsskydds-lagen

2.1 Inledning

Den 1 april 2019 trädde den nya säkerhetsskyddslagen i kraft och ersatte därmed 1996 års säkerhetsskyddslag. 1996 års lag syftade i första hand till att skydda rikets säkerhet, vilket förknippades med fysiska gränser och rent militära förhållanden.[19] Lagstiftaren ansåg det emellertid nödvändigt att utveckla säkerhetsskyddslagstiftningen för att bättre möta de förutsättningar för säkerhetsskydd som gäller i dag, bl.a. vad gäller den utveckling som skett i fråga om dels samhällets digitalisering och användning av informationsteknik, dels det faktum att privata företag i allt större utsträckning utför säkerhetskänslig verksamhet.[20]

De grundläggande principerna och stora delar av den gamla lagen har förvisso förts över till den nya säkerhetsskyddslagen, men den nya lagen har uppdaterats i flera avseenden. Det har exempelvis blivit tydligare att säkerhetsskyddslagen ska tillämpas och följas av privata aktörer. Därutöver har säkerhetsskyddslagens tillämpningsområde utvidgats, även om det fortsatt är begränsat (se vidare avsnitt 2.2 nedan). Lagstiftarens ambition är att lagen ska stå sig över tid och ges ett starkare genomslag än 1996 års lag. Säkerhetsskyddslagen tar därför sin utgångspunkt i en mer generisk hotbild och är tänkt att vara oberoende av eventuella framtida förändrade samhällsförhållanden.[21]

Utöver bestämmelser om informationssäkerhet innehåller säkerhetsskyddslagen krav på såväl fysisk säkerhet och personalsäkerhet som den övergripande processen kring arbetet med säkerhetsskydd. Informationssäkerhet, dvs. ämnet för denna rapport, utgör alltså bara en av flera aspekter av det skydd som säkerhetsskyddslagens bestämmelser syftar till att skapa.

2.2 Säkerhetsskyddslagens avgränsningar

2.2.1 TILLÄMPNINGSOMRÅDET

I säkerhetsskyddslagen anges att lagen gäller för utövare av säkerhetskänslig verksamhet.[22] Med säkerhetskänslig verksamhet avses

19 Prop. 2017/18:89 *Ett modernt och stärkt skydd för Sveriges säkerhet – ny säkerhetsskyddslag*, s. 33.

20 Prop. 2017/18:89, s. 33-34.

21 Prop. 2017/18:89, s. 34-36.

22 1 kap. 1 § säkerhetsskyddslagen.

verksamhet som antingen (i) är av betydelse för Sveriges säkerhet, eller (ii) som omfattas av ett för Sverige förpliktande internationellt åtagande om säkerhetsskydd. I den fortsatta framställningen kommer i huvudsak bara led (i) att behandlas, d.v.s. verksamhet med betydelse för Sveriges säkerhet.

Lagen tar ingen hänsyn till verksamhetens eller verksamhetsutövarens form som sådan, utan det avgörande är vilken typ av verksamhet som utövas och om denna verksamhet är av betydelse för Sveriges säkerhet. Det innebär att det är av underordnad betydelse för lagens tillämplighet om verksamhetsutövaren är ett privat företag, en statlig myndighet eller en kommun. En av anledningarna till att säkerhetsskyddslagen utformats på detta sätt är att lagen ska vara relevant även om samhället eller hotbilder förändras. Det medför även att det inte finns någon sammanfattande uppställning över exakt vilka verksamheter som är att anse som säkerhetskänslig verksamhet, i och med att det kan variera över tiden. Ytterligare en anledning till att lagen inte räknar upp de verksamheter som omfattas är att det i säkerhetshänseende vore olämpligt att ange alla skyddsvärda verksamheter i Sverige. Det skulle riskera att främmande makter eller andra antagonistiska aktörer ges information om vilka de mest skyddsvärda verksamheterna i samhället är.[23]

För att förstå vilka verksamheter som i säkerhetsskyddslagens mening bedriver säkerhetskänslig verksamhet, måste det klargöras vad som avses med Sveriges säkerhet. Annorlunda uttryckt, för att avgöra vilka verksamheter som har betydelse för *Sveriges säkerhet*, måste det utredas vad Sveriges säkerhet är.

2.2.2 SKYDDSINTRESSE

Uttrycket *Sveriges säkerhet* låter sig svårligen definieras. Även om uttrycket förekommer på ett antal ställen i såväl säkerhetsskyddslagen som annan lagstiftning, finns det ingen legaldefinition eller annan uttalad och vedertagen förklaring av vad som avses med Sveriges säkerhet. Lagstiftaren har istället gett viss vägledning genom att konkretisera olika faktorer som är av betydelse vid bedömningen av huruvida en verksamhet är av betydelse för Sveriges säkerhet (och därmed att anse som säkerhetskänslig).[24] Först och främst görs en uppdelning mellan Sveriges yttre och inre säkerhet.

Sveriges yttre säkerhet avser den territoriella suveräniteten och den politiska självständigheten. Annorlunda uttryckt, förmågan att försvara Sveriges gränser, upptäcka och avvisa kränkningar av svenskt territorium och att värna om Sveriges rättigheter och nationella intressen såsom en suverän stat. Detta inbegriper framför allt Försvarsmaktens verksamhet, men kan även omfatta verksamheter inom t.ex. försvarsindustrin i fråga om produktion, forskning och utveckling.

---

23 Prop. 2017/18:89, s. 42.

24 Prop. 2017/18:89, s. 44-45.

Sveriges inre säkerhet rör i sin tur påverkan på förmågan att upprätthålla och säkerställa Sveriges statsidé avseende funktion, handlingsfrihet och oberoende. Detta avser till stor del skyddet av särskilt kritiska anläggningar, funktioner och informationssystem kopplade till Sveriges demokratiska statsskick, rättsväsende eller brottsbekämpande förmåga.[25]

Mellan dessa kategorier går det att finna ytterligare verksamheter som kan ha betydelse för Sveriges säkerhet och därmed utgöra s.k. säkerhetskänslig verksamhet i övrigt. Det handlar i regel om verksamheter inom energiförsörjning, livsmedelsförsörjning, elektroniska kommunikationer, vattenförsörjning, transporter och finansiella tjänster. Vad som ytterst avgör om en sådan verksamhet är säkerhetskänslig, är om en antagonistisk handling skulle kunna medföra skadekonsekvenser på nationell nivå. Det kan t.ex. vara i form av störningar i eller bortfall av leveranser, tjänster och funktioner som är nödvändiga för samhällets funktionalitet.[26]

Därutöver finns ytterligare några typverksamheter som kan vara säkerhetskänsliga, nämligen (i) anläggningar eller objekt där det bedrivs verksamhet som vid en antagonistisk handling kan leda till skadliga konsekvenser på nationell nivå på andra säkerhetskänsliga verksamheter, (ii) verksamheter där det hanteras säkerhetsskyddsklassificerade uppgifter eller stora mängder uppgifter som är känsliga utan att vara säkerhetskänsliga, och (iii) verksamheter som utför drifttjänster åt ett flertal myndigheter.[27]

2.2.3 HOTBILD

Syftet med säkerhetsskyddslagen är att skydda särskilt känsliga verksamheter, primärt mot antagonistiska angrepp såsom spionerі, sabotage, terroristbrott och andra brott.[28] Som anges i lagtexten kan även andra brott än de uppräknade utgöra antagonistiska angrepp. Brottet behöver inte ens syfta till att hota Sveriges säkerhet, utan det relevanta är om brottet kan ha en negativ påverkan på Sveriges säkerhet. Under arbetet med att ta fram lagen exemplifierades detta med stöld av datorer i ett luftövervakningssystem.[29] Även om stölden inte skulle syfta till att skada Sveriges säkerhet, kan stölden *de facto* medföra begränsningar i skyddet av Sveriges territorium. Säkerhetsskyddslagen måste därför ha som syfte att skydda mot alla typer av brott som på något sätt kan hota Sveriges säkerhet.[30]

25 Prop. 2017/18:89, s. 44.

26 Prop. 2017/18:89, s. 44.

27 Prop. 2017/18:89, s. 44-45.

28 1 kap. 2 § säkerhetsskyddslagen. Se även prop. 2017/18:89, s. 40, 50 och 134.

29 SOU 2015:25 *En ny säkerhetsskyddslag*, s. 278.

30 Prop. 2017/18:89, s. 50.

2.3 Processen för att fastställa säkerhetskrav – säkerhetsskyddsanalys

2.3.1 ALLMÄNT

Alla säkerhetskänsliga verksamheter ska naturligtvis inte vidta samma säkerhetsskyddsåtgärder. Vilka säkerhetsskyddsåtgärder som ska vidtas avgörs från fall till fall utifrån identifierade skyddsvärden och en genomförd säkerhetsskyddsanalys.[31] En säkerhetsskyddsanalys är, i korthet, en utredning av behovet av säkerhetsskydd i en verksamhet, och ska ge svar på vad som ska skyddas, mot vilka hot det ska skyddas och hur det ska skyddas.

Säkerhetsskyddslagen anger att verksamhetsutövare är skyldiga att genomföra en säkerhetsskyddsanalys, men innehåller inga materiella bestämmelser om hur den ska göras eller vad analysen ska innehålla.[32] Ändamålet med och vissa grundläggande principer för säkerhetsskyddsanalysen anges förvisso i säkerhetsskyddsförordningen (2018:658), men det är framför allt genom myndighetsföreskrifter och vägledningar från myndigheter som säkerhetsskyddet ges dess närmre utformning.

Vissa myndigheter har meddelat sektorspecifika föreskrifter om säkerhetsskydd inom deras respektive tillsynsområde, däribland Svenska kraftnät, Försvarsmakten och Transportstyrelsen. Däremot har Post- och telestyrelsen i nuläget inte utnyttjat denna möjlighet.[33]

Det är dock Säkerhetspolisens föreskrifter om säkerhetsskydd, PMFS 2019:2, som är av huvudsakligt intresse, eftersom Säkerhetspolisen dels utövar tillsyn över den absoluta majoriteten av alla statliga myndigheter och samtliga kommuner och regioner, dels har en jämförelsevis bred föreskriftsrätt.[34] Det bör dock nämnas att även Försvarsmaktens föreskrifter om signalskyddstjänsten, FFS 2019:9, har ett brett tillämpningsområde, inte minst som förskrifterna också omfattar kryptografiska funktioner som bl.a. är avsedda för skydd av säkerhetskänslig verksamhet.[35]

I det följande går vi på ett övergripande plan igenom några av de åtgärder som en säkerhetskänslig verksamhet ska vidta inom ramen för en säkerhetsskyddsanalys. Det ska sägas att identifieringen och

---

31 2 kap. 1 och 5 §§ säkerhetsskyddslagen samt 2 kap. 1 § säkerhetsskyddsförordningen.

32 2 kap. 1 § säkerhetsskyddslagen.

33 Per den 24 februari 2020. Avseende Svenska kraftnät, Försvarsmakten och Transportstyrelsen, se Affärsverket svenska kraftnäts föreskrifter och allmänna råd om säkerhetsskydd, SvkFS 2019:1, Försvarsmaktens föreskrifter om säkerhetsskydd, FFS 2019:2, och Transportstyrelsens föreskrifter om säkerhetsskydd, TSFS 2019:108. Därutöver har Post- och telestyrelsen samt länsstyrelserna bemyndigats föreskriftsrätt inom vissa områden, se 7 kap. 7 § jämförd med 7 kap. 1 § 1 st. 4-6 p. säkerhetsskyddsförordningen. För fullständighetens skull ska nämnas att även Regeringskansliet genom Utrikesdepartementet bemyndigats en tydligt avgränsad föreskriftsrätt, se 7 kap. 6 § säkerhetsskyddsförordningen.

34 Säkerhetspolisens föreskrifter om säkerhetsskydd, PMFS 2019:2. För Säkerhetspolisens tillsyn och föreskriftsrätt, se 7 kap. 1 § 1 st. 2 p. respektive 7 kap. 4 § säkerhetsskyddsförordningen.

35 Försvarsmaktens föreskrifter om signalskyddstjänsten, FFS 2019:9. Föreskriftsrätten följer av 7 kap. 5 § säkerhetsskyddsförordningen.

klassificeringen av skyddsvärden egentligen inte är en del av själva säkerhetsskyddsanalysen.[36] Vi anser dock att det blir för teoretiskt att göra en sådan distinktion i förevarande framställning, och har därför valt att inte upprätthålla en sådan strikt gränsdragning.

2.3.2 IDENTIFIERING

Först och främst måste verksamhetsutövaren identifiera vilka skyddsvärden som finns i verksamheten, dvs. vad det är som ska skyddas.[37] Det finns tre kategorier av säkerhetsskyddsvärden, nämligen (i) säkerhetsskyddsklassificerade uppgifter, (ii) verksamheter eller uppgifter som omfattas av ett för Sverige förpliktande internationellt åtagande om säkerhetsskydd, och (iii) säkerhetskänslig verksamhet i övrigt.

En viss uppgift är säkerhetsskyddsklassificerad om uppgiften rör säkerhetskänslig verksamhet och därför omfattas av sekretess enligt offentlighets- och sekretesslagen (2009:400, "**OSL**"), eller som skulle ha omfattats av sådan sekretess om lagen hade varit tillämplig. Det är bara sådana sekretessgrunder som avser att skydda säkerhetskänslig verksamhet som är relevanta i detta sammanhang, i första hand försvarssekretess enligt 15 kap. 2 § OSL, men även andra bestämmelser i OSL kan utgöra grund för att en uppgift är säkerhetsskyddsklassificerad. Det finns dock ingen uttömmande uppräkning. Det står däremot klart att sekretess till skydd för exempelvis den enskildes personliga förhållanden eller till skydd för enskilds affärsförhållanden inte medför att en uppgift är säkerhetsskyddsklassificerad. Bedömningen påverkas däremot inte om uppgifterna hanteras i en privat verksamhet som inte tillämpar OSL.

När verksamhetsutövaren identifierat säkerhetsskyddsklassificerade uppgifter ska uppgifterna delas in i säkerhetsskyddsklasser. Uppdelningen görs utifrån den skada som ett röjande kan medföra för Sveriges säkerhet. Det finns fyra olika säkerhetsskyddsklasser: kvalificerat hemligt, hemlig, konfidentiell och begränsat hemlig.[38] Dessa beskrivs närmre i avsnitt 2.4.1 nedan.

I fråga om säkerhetsskyddsklassificerade uppgifter som omfattas av ett för Sverige förpliktande internationellt åtagande om säkerhetsskydd ska dessa klassificeras med utgångspunkt i den skada som ett röjande kan medföra för Sveriges förhållande till annan stat eller mellanfolklig organisation. Om uppgifterna redan har klassificerats av en annan stat eller mellanfolklig organisation ska den gjorda klassificeringen godtas.[39]

Den säkerhetskänsliga verksamheten som i övrigt finns i verksamheten ska i sin tur identifieras utifrån olika konsekvenskategorier och därefter

36 Säkerhetspolisens *Vägledning i säkerhetsskydd – Säkerhetsskyddsanalys* (juni 2019), s. 10.

37 2 kap. 1 § PMFS 2019:2.

38 2 kap. 5 § 1 st. säkerhetsskyddslagen.

39 2 kap. 5 § 2 st. säkerhetsskyddslagen.

graderas enligt vissa konsekvensnivåer.[40] Identifieringen utgår från de skador som en antagonistisk handling riktad mot verksamheten skulle kunna medföra.[41]

2.3.3 ANALYS

Säkerhetsskyddsanalysen syftar ytterst till att verksamhetsutövaren ska utreda behovet av säkerhetsskydd. Utifrån analysen ska behövliga säkerhetsskyddsåtgärder planeras samt vidtas.[42] För att kunna göra detta måste verksamhetsutövaren, utöver att känna till vad som ska skyddas, också utreda vad verksamheten ska skyddas mot.[43]

Verksamhetsutövaren ska därför identifiera hot mot den säkerhetskänsliga verksamheten och hur hoten i så fall kan påverka verksamheten. Som stöd för att identifiera hotbilden tillhandahåller Säkerhetspolisen och Försvarsmakten hotbilder, även om dessa är generella och därför behöver kompletteras av verksamhetsutövaren.[44]

Nästa steg för verksamhetsutövaren är att analysera och dokumentera vilka sårbarheter som finns i den säkerhetskänsliga verksamheten. Verksamhetsutövaren ska härvidlag bedöma hur sårbarheterna kan påverka verksamhetens säkerhetsskydd och om det finns behov av att genomföra säkerhetsskyddsåtgärder.[45]

För att identifiera sårbarheter i verksamheten behöver verksamhetsutövaren i regel granska interna processer och rutiner, men det kan även vara nödvändigt att genomföra praktiska tester. Till exempel kan penetrationstester[46] eller liknande åtgärder ge tydliga svar på ett informationssystems säkerhetsförmågor.[47]

Om verksamhetsutövaren kommer fram till att det finns säkerhetshot mot vilka verksamhetens skyddsvärden inte skyddas, dvs. om den säkerhetskänsliga verksamheten är sårbar, ska säkerhetsskyddsåtgärder vidtas.[48]

---

40 2 kap. 2-3 §§ PMFS 2019:2.

41 2 kap. 2 § PMFS 2019:2.

42 2 kap. 1 § säkerhetsskyddslagen.

43 2 kap. 1 § säkerhetsskyddsförordningen.

44 Säkerhetspolisens *Vägledning i säkerhetsskydd – Säkerhetsskyddsanalys* (juni 2019), s. 19. För Säkerhetspolisens senaste hotbild, se Säkerhetspolisens hotbild mot säkerhetskänslig verksamhet (juni 2019), https://www.sakerhetspolisen.se/download/18.7acd465e16b4e0e54c64a/1560776860929/Hotbild-mot-sakerhetskanslig-verksamhet-juni-2019.pdf. Läst den 24 februari 2020.

45 2 kap. 9 § PMFS 2019:2.

46 Ett penentrationstest kan, typiskt sett, beskrivas som en metod för att utvärdera säkerheten i ett it-system genom att angripa it-systemet med samma metoder som en riktig angripare skulle ha använt, i syfte att ta reda på vilka sårbarheter som finns.

47 Säkerhetspolisens *Vägledning i säkerhetsskydd – Informationssäkerhet* (juni 2019), s. 52.

48 2 kap. 1-4 §§ säkerhetsskyddslagen och 2 kap. 1 § säkerhetsskyddsförordningen.

2.3.4 UTFORMNING AV SKYDD

Om verksamhetsutövaren i säkerhetsskyddsanalysen kommer fram till att det brister i verksamhetens säkerhetsskydd måste naturligtvis lämpliga skyddsåtgärder vidtas.

Lagstiftaren har valt att dela upp säkerhetsskyddsåtgärder i tre kategorier: (i) informationssäkerhet, (ii) fysisk säkerhet, och (iii) personalsäkerhet.[49] Det är dock viktigt att understryka, vilket även poängterades under lagstiftningsprocessen, att de olika åtgärdskategorierna inte är isolerade från varandra. Säkerhetsskyddsåtgärder inom de tre kategorierna ska istället samverka och ses som *"delar i ett system för att uppnå ett ändamålsenligt skydd"*.[50] Exempelvis kan informationssäkerhet svårligen upprätthållas utan både fysiska hinder som motverkar obehörig åtkomst och säkerställandet av att personer som hanterar informationen inte har för avsikt att missbruka den.

Verksamhetsutövaren ska beskriva vilka säkerhetsåtgärder som behöver vidtas på ett övergripande plan. Vad gäller informationssäkerhet, kan det handla om alltifrån att förhindra att personal ibland använder publika nätverk eller att e-post inte skickas krypterat, till att införa rutiner för kontroll av åtkomstbehörigheter eller lösenordshantering.[51]

Som sista steg ska samtliga delar i säkerhetsskyddsanalysen sammanställas och fastställas.[52] Den fastställda säkerhetsskyddsanalysen kommer ligga till grund för arbetet med att upprätta en säkerhetsskyddsplan.[53] Säkerhetsskyddsplanen ska, till skillnad från säkerhetsskyddsanalysen, på ett tydligt och detaljerat sätt ange vilka säkerhetsskyddsåtgärder som ska genomföras, när de ska genomföras och vem som ansvarar för att de genomförs.[54]

För verksamhetsutövare som bedriver *särskilt säkerhetskänslig verksamhet* gäller en annorlunda ordning.[55] För sådana verksamhetsutövare är det istället Säkerhetspolisen som tar fram en s.k. dimensionerande hotbeskrivning. En dimensionerad hotbeskrivning är en beskrivning av en befintlig antagonistisk aktör, som skulle kunna angripa Sveriges säkerhet[56], som säkerhetsskyddsåtgärderna förväntas kunna skydda mot, även om det inte föreligger något identifierat hot mot den säkerhetskänsliga verksamheten. Säkerhetsskyddsåtgärderna ska därefter anpassas utifrån den dimensionerande hotbeskrivningen.[57]

---

49 2 kap. 2-4 §§ säkerhetsskyddslagen. Denna uppdelning fanns redan i den gamla säkerhetsskyddslagen, om än med andra begrepp.

50 SOU 2015:25, s. 326.

51 Säkerhetspolisens *Vägledning i säkerhetsskydd – Informationssäkerhet* (juni 2019).

52 2 kap. 1 § säkerhetsskyddslagen.

53 2 kap. 11 § PMFS 2019:2.

54 2 kap. 11 § PMFS 2019:2.

55 Angående begreppet *särskilt säkerhetskänslig verksamhet*, se 2 kap. 6 § PMFS 2019:2.

56 Säkerhetspolisen använder uttrycket *"antagen antagonistisk förmåga"*, men förklarar inte vad som avses. I sammanhanget har vi dock valt att tolka det som att det är en möjlig, men ospecificerad, aktör som hypotetiskt skulle ha ett intresse av att rikta angrepp mot Sveriges säkerhet.

57 2 kap. 8 § PMFS 2019:2.

2.3.5 TILLÄMPNING

Förutom att genomföra de säkerhetsskyddsåtgärder som beslutats ska verksamhetsutövaren inrätta de funktioner som krävs för att säkerhetsskyddsarbetet ska kunna bedrivas, kontrolleras och följas upp.[58] Detta innefattar även en tydlig ansvarsfördelning mellan de olika funktionerna, men också att funktioner (t.ex. avdelningar) som kan ha olika intressen i fråga om säkerhetsskydd ska vara separerade från varandra.[59]

Verksamhetsutövaren har alltså ett ansvar för att organisera verksamheten på ett sätt som möjliggör säkerhetsskyddet, men även för att dokumentera verksamhetens säkerhetsskydd och säkerställa att nödvändiga resurser och kompetenser finns tillgängliga.[60]

2.3.6 UPPFÖLJNING

Till följd av att hotbilder kan förändras från en dag till en annan i fråga om både allvar och omfattning har verksamhetsutövaren en skyldighet att uppdatera säkerhetsskyddsanalysen vid behov.[61] Enligt Säkerhetspolisen ska den i vart fall uppdateras vartannat år.[62]

Detta är en tydlig indikation på att säkerhetsskyddsarbetet, likt mycket annat, svårligen låter sig utgöras av ett avgränsat projekt. Verksamheten måste istället kontinuerligt ha säkerhetsskydd i bakhuvudet, för att på så vis kunna identifiera förändrade hotbilder som kanske inte framstår som hot vid en första anblick.

2.4 Konkreta informationssäkerhetskrav

2.4.1 UPPGIFTSKLASSIFICERING

Säkerhetsskyddslagen delar in uppgifter (information) i fyra kategorier, s.k. säkerhetsskyddsklasser. Vid denna säkerhetsskyddsklassificering utgår man från vilken skada för Sveriges säkerhet som kan uppstå om uppgifterna röjs. De fyra säkerhetsskyddsklasserna är:

- **Kvalificerat hemlig** vid synnerligen allvarlig skada
- **Hemlig** vid allvarlig skada
- **Konfidentiell** vid inte obetydlig skada
- **Begränsat hemlig** endast ringa skada

58 2 kap. 13 § PMFS 2019:2.

59 2 kap. 14 § PMFS 2019:2.

60 2 kap. 15-16 §§ PMFS 2019:2.

61 2 kap. 1 § säkerhetsskyddsförordningen.

62 2 kap. 10 § PMFS 2019:2.

Det finns ett antal säkerhetsskyddsåtgärder som verksamhetsutövaren måste vidta avseende de handlingar och lagringsmedium som innehåller säkerhetsskyddsklassificerade uppgifter. Vissa säkerhetsskyddsåtgärder är unika för en viss klass, t.ex. ska handlingar som innehåller kvalificerat hemliga uppgifter förvaras av verksamhetsutövarens högsta chef, medan andra gäller oavsett säkerhetsskyddsklass.

Majoriteten av de krav på informationssäkerhet som är kopplade till säkerhetsskyddsklassificeringen och säkerhetsskyddsklassen återfinns i PMFS 2019:2, men det finns också en handfull krav i säkerhetsskyddslagen och säkerhetsskyddsförordningen. I de flesta fall kompletteras de dock av närmre bestämmelser i PMFS 2019:2.

2.4.2 MINIMIÅTGÄRDER

I nedan tabell har vi sammanställt de konkreta säkerhetsskyddsåtgärder som kan utläsas av säkerhetsskyddslagen med följdlagstiftning. Till en betydande del är kraven på skyddsåtgärder oberoende av vilken säkerhetsskyddsklass informationen delats in i, men många av de mer krävande åtgärderna ska endast tillämpas för de högre klassificeringarna.

			KVALIFICERAT HEMLIG	HEMLIG	KONFIDENTIELL	BEGRÄNSAT HEMLIG
1.	3 kap. 1 § PMFS 2019:2	Behandling på särskilda informationssystem och lagringsmedium	×	×	×	×
2.	3 kap. 2 § PMFS 2019:2	Informera mottagare om säkerhetsskyddsklassificering	×	×	×	×
3.	3 kap. 3 § PMFS 2019:2	Rutiner för att upprätthålla ett fullgott säkerhetsskydd	×	×	×	×
4.	3 kap. 7 § PMFS 2019:2	Anteckning om ny eller borttagande av säkerhetsskyddsklass	×	×	×	×
5.	3 kap. 10 § PMFS 2019:2	Förvaring i förhållande till skyddsdimensionering	×	×	×	×
6.	3 kap. 12 § PMFS 2019:2	Information i register där fysisk allmän handling är diarieförd	×	×	×	×
7.	3 kap. 7 § säkerhetsskyddsförordningen	Anteckning om ursprungsland	×	×	×	×
8.	3 kap. 21 § PMFS 2019:2	Medförande utanför verksamhetsutövarens lokaler	×	×	×	×

			KVALIFICERAT HEMLIG	HEMLIG	KONFIDENTIELL	BEGRÄNSAT HEMLIG
9.	3 kap. 25 § PMFS 2019:2	Förstöring av uppgifter	×	×	×	×
10.	4 kap. 4 § PMFS 2019:2	Egenutvecklad programvara i systemen ska granskas för säkerhetsbrister	×	×	×	×
11.	4 kap. 12 § PMFS 2019:2	Alla utställda identiteter ska vara unika över tid, och åtkomst ska vara spårbar till individ, system eller resurs	×	×	×	×
12.	4 kap. 13 § PMFS 2019:2	Behörigheter som ger särskild åtkomst ska tilldelas restriktivt, tidsbegränsat och följas upp	×	×	×	×
13.	4 kap. 14 § PMFS 2019:2	Flerfaktorsautentisering	×	×	×	×
14.	4 kap. 15 § PMFS 2019:2	Regler för lösenordshantering, bl.a. vad gäller återanvändning och komplexitet	×	×	×	×
15.	4 kap. 33 § PMFS 2019:2	Loggning av användning och ändring av vissa behörigheter till och roller i informationssystem	×	×	×	×
16.	4 kap. 38 § PMFS 2019:2	Kontroll av säkerhetskopior	×	×	×	×
17.	3 kap 1 § säkerhets-skyddsförordningen; 4 kap. 7 § PMFS 2019:2	Säkerhetsskyddsbedömning innan informationssystem tas i drift och genomföra tester av åtgärderna	×	×	×	×
18.	3 kap. 4 § säkerhets-skyddsförordningen	Krav på åtgärder för att upptäcka, försvåra och hantera skadlig inverkan och röjande signaler	×	×	×	×
19.	3 kap. 5 § säkerhets-skyddsförordningen; FFS 2019:9	Skydd genom kryptografiska funktioner vid kommunikation till externa informationssystem i fråga om krav på kryptografiska funktioner som sådana	×	×	×	×
20.	3 kap. 5 § PMFS 2019:2	Anteckning om handlingens beteckning, antal sidor och uppgift om bilagor	×	×	×	
21.	3 kap. 13 § PMFS 2019:2	Märkning av lagringsmedium	×	×	×	
22.	3 kap. 14 § PMFS 2019:2	Distribution av handlingar inom och utom verksamheten	×	×	×	
23.	4 kap. 29 § PMFS 2019:2	Intrångsdetektering och intrångs-skydd i informationssystem	×	×	×	

			KVALIFICERAT HEMLIG	HEMLIG	KONFIDENTIELL	BEGRÄNSAT HEMLIG
24.	2 kap. 6 § säkerhetsskyddslagen; 2 kap. 6 § säkerhetsskyddsförordningen; 7 kap. 3 § PMFS 2019:2	Upprättande av säkerhetsskyddsavtal	×	×	×	
25.	3 kap. 2 § säkerhetsskyddsförordningen	Samråd med Säkerhetspolisen eller Försvarsmakten innan informationssystemet tas i drift	×	×	×	
26.	3 kap. 6-8 §§ säkerhetsskyddslagen	Placering i säkerhetsklass	×	×	×	
27.	3 kap. 2 § säkerhetsskyddsförordningen	Samråd innan ett informationssystem som behandlar uppgifter tas i drift	×	×	×	
28.	3 kap. 4 § säkerhetsskyddsförordningen	Skyddsåtgärder mot röjande signaler för informationssystem	×	×	×	
29.	3 kap. 6 § PMFS 2019:2	Anteckning om handlingens exemplarnummer	×	×		
30.	3 kap. 17 § PMFS 2019:2	Anteckning på kvittens om återlämnande	×	×		
31.	3 kap. 8 § säkerhetsskyddsförordningen; 3 kap. 24 § PMFS 2019:2	Handlingar ska inventeras minst en gång per år	×	×		
32.	3 kap. 26 § PMFS 2019:2	Dokumentering av förstöring av allmän handling	×	×		
33.	4 kap. 11 § PMFS 2019:2	Årlig granskning av informationssäkerhet	×	×		
34.	4 kap. 20-21 §§ PMFS 2019:2	Fysisk och logisk separation av vissa informationssystem	×	×		
35.	4 kap. 21 § PMFS 2019:2	Envägskommunikation vid import och export i informationssystem	×	×		
36.	3 kap. 8 § PMFS 2019:2	Särskild beslutsordning vid ny eller borttagande av säkerhetsskyddsklass	×			
37.	3 kap. 9 § PMFS 2019:2	Särskild beslutsordning för kopia eller utdrag ur handling	×			
38.	3 kap. 11 § PMFS 2019:2	Handling ska förvaras hos högsta chef	×			

			KVALIFICERAT HEMLIG	HEMLIG	KONFIDENTIELL	BEGRÄNSAT HEMLIG
39.	3 kap. 17 § PMFS 2019:2	Kvittering med namnteckning och namnförtydligande på särskilt kvitto i två exemplar	×			
40.	3 kap. 17 § PMFS 2019:2	Kvittens ska bevaras i minst 25 år	×			
41.	3 kap. 18 § PMFS 2019:2	Anteckning om mottagare av elektronisk handling	×			
42.	3 kap. 20 § PMFS 2019:2	Anteckning om uppgifter i handling lämnas muntligen eller genom visning	×			
43.	3 kap. 23 § PMFS 2019:2	Särskilda beslutsordning för att medföra handling utanför verksamhetsutövarens lokaler	×			
44.	4 kap. 26 § PMFS 2019:2	Dokumentation av hård- och mjukvaror	×			
45.	4 kap. 34 § PMFS 2019:2	Säkerhetsloggar ska bevaras under minst 25 års tid	×			
46.	3 kap. 17 § PMFS 2019:2	Kvittering med namnteckning och namnförtydligande på särskilt kvitto i två exemplar, kvittens ska bevaras i minst 25 år	×			
47.	3 kap. 17 § PMFS 2019:2	Kvittering med namnteckning och namnförtydligande i register, liggare eller särskilt kvitto, kvittens ska bevaras i minst 10 år		×		
48.	3 kap. 22 § PMFS 2019:2	Medförande av handling till utlandet		×	×	×
49.	4 kap. 34 § PMFS 2019:2	Säkerhetsloggar ska bevaras under minst tio års tid		×	×	×
50.	7 kap. 1 § PMFS 2019:2	Annan reglering av säkerhetsskyddet än säkerhetsskyddsavtal vid säkerhetsskyddad upphandling				×

2.5 Särskilda krav på utkontraktering

I samband med offentliga upphandlingar ställer säkerhetsskyddslagen krav på att upprätta och ingå ett säkerhetsskyddsavtal med leverantören/-erna. Detta gäller om (i) det förekommer säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen konfidentiell eller högre i upphandlingen, eller (ii) upphandlingen i övrigt avser eller ger leverantören tillgång till säkerhetskänslig verksamhet av motsvarande betydelse för Sveriges säkerhet, t.ex. om leverantören ska delta i känslig verksamhet vid kärnkraftverk eller flygplatser.[63] Kravet på säkerhetsskyddsavtal ska uppfyllas av såväl enskilda verksamhetsutövare som statliga myndigheter, kommuner och regioner, låt vara att kravet innebär olika skyldigheter.[64] Dessa skyldigheter beskrivs nedan.

Om en enskild verksamhetsutövare har för avsikt att ingå ett säkerhetsskyddsavtal ska avtalet utan dröjsmål anmälas till den aktuella tillsynsmyndigheten.[65] Syftet med detta är att uppmärksamma tillsynsmyndigheten och att ge tillsynsmyndigheten underlag för eventuell tillsyn. När säkerhetsskyddsavtalet väl ingås, eller upphör, ska detta anmälas till Säkerhetspolisen.[66]

För statliga myndigheter uppstår en mer formell process avseende säkerhetsskyddsavtalet och dess upprättande.[67] De materiella reglerna för säkerhetsskyddsavtalets innehåll och process är dock desamma.[68] Det kan även bli aktuellt för verksamhetsutövaren att genomföra en s.k. särskild säkerhetsskyddsbedömning.[69]

Kärnan i säkerhetsskyddsavtal, som även genomsyrar säkerhetsskyddsarbetet i stort, är att de intressen som lagstiftningen skyddar ska ges samma skydd oavsett om skyddsvärdet förekommer inom det allmänna eller det privata. Inte heller ska säkerhetsskyddet försämras till följd av att en utomstående leverantör anlitas.[70]

Ett säkerhetsskyddsavtal ingås på en av tre olika nivåer. Nivån avgörs av var leverantören utför sitt uppdrag, vilken typ av uppgifter leverantören ges tillgång till och vilka åtgärder leverantören kan vidta avseende uppgifterna.[71] Ju högre nivå och därmed risk, desto högre krav ställs på verksamhetsutövarens kontroller av leverantören och de åtgärder leverantören måste vidta.[72]

Det är verksamhetsutövaren som har det huvudsakliga ansvaret att kontrollera leverantören.[73] Att som leverantör ingå säkerhetsskydds-

63 2 kap. 6 § säkerhetsskyddslagen och prop. 2017/18:89, s. 141.

64 2 kap. 6 § säkerhetsskyddsförordningen och 7 kap. 1-2 §§ PMFS 2019:2.

65 2 kap. 5 § säkerhetsskyddsförordningen.

66 2 kap. 7 § säkerhetsskyddsförordningen.

67 2 kap. 6 § säkerhetsskyddsförordningen och 7 kap. 1-2 §§ PMFS 2019:2.

68 7 kap. 3 och 5-12 §§ PMFS 2019:2.

69 Se 2 kap. 12 PMFS 2019:2.

70 Prop. 2017/18:89, s. 104.

71 7 kap. 3 § PMFS 2019:2.

72 7 kap. 5-10 §§ PMFS 2019:2.

73 7 kap. 7 § PMFS 2019:2.

avtal innebär även att leverantören ställs under den aktuella tillsynsmyndighetens tillsyn. Svenska kraftnät, Transportstyrelsen, Post- och telestyrelsen och länsstyrelserna får således utöva tillsyn över leverantörer och underleverantörer som omfattas av ett säkerhetsskyddsavtal inom sina respektive tillsynsområden.[74] Därtill har Säkerhetspolisen och Försvarsmakten rätt att utöva tillsyn inom de nämnda myndigheternas tillsynsområde samt över leverantörer som har uppdrag för flera verksamhetsutövare om leverantörens samlade uppdrag är av stor betydelse för Sveriges säkerhet.[75]

2.6 Gränssnitt mot myndigheter

2.6.1 MYNDIGHETERS TILLSYN

Som tidigare nämnts utövar olika myndigheter tillsyn över olika verksamhetsområden. Tillsynsmyndigheten bestäms utifrån tillsynsområdets art och uppdelningen ser ut som följer:

TILLSYNSMYNDIGHET	TILLSYNSOMRÅDE
Försvarsmakten	Fortifikationsverket, Försvarshögskolan, och Myndigheter som hör till Försvarsdepartementet
Säkerhetspolisen	Övriga statliga myndigheter (utom JK), Kommuner, och Regioner
Svenska kraftnät	Enskilda verksamhetsutövare som bedriver elförsörjningsverksamhet
Transportstyrelsen	Enskilda verksamhetsutövare som bedriver: • Flygtrafiktjänst för civil luftfart, • Flygtrafikledningstjänst för militär luftfart, eller • Verksamhet som är av betydelse inom luftfartsskydd, sjöfartsskydd eller hamnskydd
Post- och telestyrelsen	Enskilda verksamhetsutövare som bedriver verksamhet som avser: • Elektronisk kommunikation, eller • Posttjänst
Länsstyrelserna	Enskilda verksamhetsutövare som bedriver andra säkerhetskänsliga verksamheter än sådana som omfattas av Svenska kraftnäts, Transportstyrelsens eller Post- och telestyrelsens tillsyn

74 7 kap. 1 § säkerhetsskyddsförordningen.

75 7 kap. 2 § säkerhetsskyddsförordningen.

I vissa fall har Säkerhetspolisen och Försvarsmakten rätt att utöva tillsyn även utanför ovan nämnda områden, se avsnitt 2.4.1 ovan.

2.6.2 INCIDENTRAPPORTERING

Den verksamhet som omfattas av säkerhetsskyddslagen, omfattas även av en anmälningsplikt avseende s.k. säkerhetshotande händelser eller verksamhet.[76] Säkerhetsskyddsförordningen anger vad som är att anse som en sådan anmälningspliktig händelse eller verksamhet, medan Säkerhetspolisens föreskrifter anger hur säkerhetshotande händelser och verksamhet ska hanteras.[77]

En säkerhetshotande händelse eller verksamhet har inträffat om (i) en säkerhetsskyddsklassificerad uppgift kan ha röjts, (ii) det inträffat en it-incident i ett informationssystem som verksamhetsutövaren är ansvarig för och som har betydelse för säkerhetskänslig verksamhet ifall incidenten allvarligt kan påverka säkerheten i systemet, eller (iii) verksamhetsutövaren får kännedom eller misstanke om någon annan för denne allvarlig säkerhetshotande verksamhet.[78]

Om det uppstått en säkerhetshotande händelse ska verksamhetsutövaren skyndsamt anmäla detta till Säkerhetspolisen och, om verksamhetsutövaren tillhör Försvarsmaktens tillsynsområde, till Försvarsmakten.[79] Ifall verksamhetsutövaren tillhandahåller tjänster åt en annan verksamhetsutövare, t.ex. i form av drift av gemensamma it-system, åligger det verksamhetsutövaren att även informera och vid behov samråda med berörda verksamhetsutövare.[80]

2.6.3 SAMRÅD

Vad gäller informationssystem finns i vissa situationer en skyldighet att samråda med Säkerhetspolisen eller, i förekommande fall, Försvarsmakten.[81] Detta gäller dock endast om systemet redan på förhand kan tänkas komma att behandla säkerhetsskyddsklassificerade uppgifter i viss skyddsklass, eller om obehörig åtkomst till systemet kan medföra en inte obetydlig skada för Sveriges säkerhet.[82] Samråd ska ske innan en verksamhetsutövare tar informationssystemet i drift eller ändrar det väsentligt.

Vidare har statliga myndigheter en samrådsskyldighet inför upphandlingar som kräver säkerhetsskyddsavtal, om leverantören kan få tillgång till uppgifter i säkerhetsskyddsklassen hemlig eller högre utanför

76 2 kap. 1 § säkerhetsskyddslagen.

77 2 kap. 10-11 §§ säkerhetsskyddsförordningen och 2 kap. 20-25 §§ PMFS 2019:2. Vad gäller hanteringen vid informationssäkerhetsrelaterade incidenter ges närmre vägledning i *Vägledning i säkerhetsskydd – Informationssäkerhet* (juni 2019), se särskilt avsnitt 8.10.

78 2 kap. 10 § säkerhetsskyddsförordningen.

79 2 kap. 10 § 2 st. säkerhetsskyddsförordningen.

80 2 kap. 11 § 1 st. säkerhetsskyddsförordningen.

81 3 kap. 2 § säkerhetsskyddsförordningen.

82 Säkerhetsskyddsklass *konfidentiell* eller högre.

myndighetens lokaler, eller kan få tillgång till säkerhetskänsliga informationssystem utanför myndighetens lokaler och obehörig åtkomst till systemen kan medföra allvarlig skada för Sveriges säkerhet.[83]

2.6.4 SANKTIONER

I dagsläget saknar säkerhetsskyddslagstiftningen dedikerade sanktionsmöjligheter vid överträdelser. De allvarligaste överträdelserna av säkerhetsskyddslagen är förvisso straffbara enligt brottsbalkens (1962:700) bestämmelser om brott mot Sveriges säkerhet och tjänstefel, 19 respektive 20 kap. brottsbalken.

När den dåvarande regeringen tillsatte en särskild utredare för att göra en översyn av säkerhetsskyddslagstiftningen ingick det inte i uppdraget att föreslå nya sanktioner.[84] Under utredningens gång riktades kritik mot detta, varpå regeringen tillsatte en kompletterande utredning med uppdrag att bl.a. föreslå ett sanktionssystem för överträdelser av säkerhetsskyddslagstiftningen.[85]

Enligt utredningens förslag finns det inget behov av ändringar i strafflagstiftningen, men det föreslås att ett administrativt sanktionssystem ska införas i säkerhetsskyddslagen. Tillsynsmyndigheter ska, enligt förslaget, ta ut en sanktionsavgift mellan 5 000 och 10 miljoner kronor vid överträdelser av säkerhetsskyddslagen. Därtill föreslås även ytterligare befogenheter för tillsynsmyndigheter, bl.a. möjligheten att kunna utfärda föreläggande om att verksamhetsutövare ska vidta viss åtgärd.[86] Förslagen har i skrivande stund ännu inte lett till lagstiftning.[87]

Det bör uppmärksammas att utredningen anser att det kan uppstå ett behov för tillsynsmyndigheten att kunna jämka sanktioner ifall en och samma situation ger upphov till sanktionsavgifter enligt både säkerhetsskyddslagen, och dataskyddsförordningen, NIS-lagen eller sektorspecifik reglering (se vidare avsnitt 7.2.5 nedan).[88]

---

83 2 kap. 6 § säkerhetsskyddsförordningen.

84 Dir. 2011:94 *En modern säkerhetsskyddslag.*

85 Dir. 2017:32 *Utkontraktering av säkerhetskänslig verksamhet, sanktioner och tillsyn – tre frågor om säkerhetsskydd.*

86 Se SOU 2018:82 *Kompletteringar till den nya säkerhetsskyddslagen,* särskilt avsnitt 9.4-9.13, för utredningens överväganden avseende sanktionssystemets utformning. Angående föreslagna ändringar i säkerhetsskyddslagen, se SOU 2018:82, s. 41 ff.

87 Per den 24 februari 2020.

88 SOU 2018:82, s. 446.

3. Informationssäkerhet enligt NIS-lagen

3.1 Inledning

NIS-lagen är det svenska genomförandet av NIS-direktivet.[89] NIS-direktivet är i sin tur en del av EU:s övergripande strategi för informationssäkerhet. Denna strategi, som inleddes 2013,[90] omfattar även ett utökat mandat för EU:s cybersäkerhetsbyrå (”**ENISA**”) och antagandet av 2019 års ”cybersäkerhetsakt”.[91] NIS-direktivet kompletteras av genomförandeförordningen (EU) 2018/151.[92]

På nationell nivå har regeringen antagit en nationell strategi för samhällets informations- och cybersäkerhet.[93] Det genomgående temat är åtgärder för att främja en hög nivå på informationssäkerhet hos myndigheter, företag och i samhället överlag.

Både den unionsrättsliga och den nationella strategin utgår från att hot och angrepp mot informationssystem är ett hot mot säkerhet, stabilitet och ekonomiskt välstånd, och att en hög nivå på informationssäkerhet är en förutsättning för att potentialen i samhällets digitalisering ska kunna realiseras. Det är mot denna bakgrund man infört NIS-regleringen. Syftet är att höja nivån på säkerheten i nätverk och informationssystem (”**NIS**”) för vissa samhällsviktiga och digitala tjänster.

NIS-lagen kompletteras av förordningen (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster (”**NIS-förordningen**”) och ett antal myndighetsföreskrifter från MSB som utfärdats med stöd av NIS-förordningen.

3.2 Avgränsningar

3.2.1 TILLÄMPNINGSOMRÅDE

NIS-lagen gäller enbart för tillhandahållare av vissa samhällsviktiga och

89 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.

90 Se särskilt Europaparlamentets resolution av den 12 september 2013 om EU:s strategi för it-säkerhet: en öppen, säker och trygg cyberrymd (2013/2606[RSP]).

91 Europaparlamentets och Rådets förordning (EU) 2019/881 av den 17 april 2019 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik och om upphävande av förordning (EU) nr 526/2013.

92 Kommissionens genomförandeförordning (EU) 2018/151 av den 30 januari 2018 om tillämpningsföreskrifter för Europaparlamentets och rådets direktiv (EU) 2016/1148 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen vad gäller närmare specificering av de aspekter som ska beaktas av leverantörer av digitala tjänster när de hanterar risker som hotar säkerheten i deras nät- och informationssystem samt parametrarna för fastställande av om en incident har avsevärd inverkan.

93 Regeringens skrivelse 2016/17:213 *Nationell strategi för samhällets informations- och cybersäkerhet* av den 22 juni 2017.

digitala tjänster. Begreppen *samhällsviktig tjänst* och *digital tjänst* är legaldefinierade och betydligt snävare än vad vanligt språkbruk antyder. Därtill är det i viss mån olika regleringar beroende på om tjänsten ska klassificeras som samhällsviktig eller digital. Lagen gäller dock inte för verksamhet som omfattas av säkerhetsskyddslagen.

3.2.1.1 Samhällsviktiga tjänster

De sektorer och delsektorer som kan omfattas av NIS-lagstiftningen definieras i bilaga II till NIS-direktivet. Det rör vissa enheter inom sektorerna energi, transport, bankverksamhet, finansmarknadsinfrastruktur, hälso- och sjukvård, dricksvatten och digital infrastruktur. Avgränsningen av de enheter som träffas av lagstiftningen sker till stora delar genom befintliga legaldefinitioner av olika verksamheter i EU-lagstiftningen. Som exempel kan nämnas att elföretag avgränsas till sådana aktörer som bedriver "*leverans eller handel*" enligt definitionen i artikel 2.19 i direktiv 2009/72/EG.[94]

Utöver att en verksamhet ryms inom någon av definitionerna i NIS-direktivets bilaga II krävs att tjänsten är samhällsviktig. MSB har meddelat föreskrifter om hur leverantörer av sådana tjänster ska identifieras.[95] Föreskrifterna anger, för respektive tjänst, under vilka förutsättningar en leverantör av tjänsten är att betrakta som samhällsviktig och därför omfattas av NIS-regleringen. Förutsättningarna tar i huvudsak sikte på volymer i tjänsterna eller om de motsvarar vissa definitioner i nationell lagstiftning. Om NIS-regleringen är tillämplig är tjänsteleverantören skyldig att anmäla sig till ansvarig tillsynsmyndighet.[96]

Enligt NIS-direktivets definition av samhällsviktiga tjänster inom digital infrastruktur avses (i) internetknutpunkter, (ii) DNS-tjänster, och (iii) registreringsenheter för toppdomäner.[97] Detta är särskilt viktigt att notera, eftersom de lätt kan sammanblandas med *digitala tjänster*, vars definition utesluter just dessa tjänster (se avsnitt 3.2.1.2 nedan).

3.2.1.2 Digitala tjänster

Med *digitala tjänster* i NIS-lagens mening avses som utgångspunkt samma sak som artikel 1.1 b i det s.k. anmälningsdirektivet[98] benämner *informationssamhällets tjänster*, det vill säga tjänster som vanligtvis utförs mot ersättning på distans, på elektronisk väg och på

94 Europaparlamentets och rådets direktiv 2009/72/EG av den 13 juli 2009 om gemensamma regler för den inre marknaden för el och om upphävande av direktiv 2003/54/EG.

95 MSB:s föreskrifter om anmälan och identifiering av leverantörer av samhällsviktiga tjänster, MSBFS 2018:7.

96 23 § NIS-lagen.

97 Bilaga II till NIS-direktivet.

98 Europaparlamentets och rådets direktiv (EU) 2015/1535 av den 9 september 2015 om ett informationsförfarande beträffande tekniska föreskrifter och beträffande föreskrifter för informationssamhällets tjänster.

individuell begäran av en tjänstemottagare. Tillämpningen är dock begränsad till tre specifika typer av tjänster, nämligen (i) internetbaserade marknadsplatser, (ii) internetbaserade sökmotorer, och (iii) molntjänster.[99] Det är inte tydligt varför just dessa tre typer har ansetts som särskilt motiverade att särreglera.

Begreppen definieras i skälen 15-17 i NIS-direktivet. De avgränsningar som görs i dessa skäl medför bl.a. att endast sådana tjänster som är slutdestination för avtalsingående kan betraktas som marknadsplatser, vilket utesluter exempelvis prisjämförelsetjänster eller andra mellanhandstjänster. Enligt definitionen av sökmotor avses endast sådana som gör det möjligt att göra sökningar på i princip alla webbplatser, och sådana sökfunktioner som endast är begränsade till innehållet på en särskild webbplats undantas uttryckligen. Vad gäller molntjänster definieras dessa som tjänster som medger åtkomst till en skalbar och elastisk pool av delbara dataresurser. Denna tekniskt orienterade definition synes täcka såväl infrastrukturstjänster (IaaS), plattformstjänster (PaaS) och mjukvara som tjänst (SaaS).

3.2.1.3 Andra tjänster som är viktiga för samhällets funktionalitet

Enligt artikel 20 i NIS-direktivet får medlemsstaterna även meddela regler för leverantörer av sådana tjänster som faller utanför definitionerna *samhällsviktiga* respektive *digitala*. MSB har meddelat föreskrifter och allmänna råd om frivillig rapportering av incidenter i tjänster som är viktiga för samhällets funktionalitet.[100] Föreskrifterna tar enbart sikte på incidentrapportering och ställer alltså inga särskilda krav på formerna för informationssäkerhetsarbete eller specifika säkerhetsåtgärder. Det är upp till den enskilda leverantören att själv välja om man vill rapportera upptäckta incidenter. När så görs ska dock en liknande process som för samhällsviktiga och digitala tjänster följas.

Vi kan konstatera att i MSB:s föreskrifter inte är tydligt vare sig vilka aktörer som omfattas av föreskrifterna, eller vad skillnaden är mellan *samhällsviktiga tjänster* respektive *tjänster som är viktiga för samhällets funktionalitet*.

3.2.2 SKYDDSINTRESSE

Syftet med NIS-lagen är att uppnå en hög nivå på säkerheten i nätverk och informationssystem för de omfattade tjänsterna. Det är alltså inte säkerheten i själva tjänsterna som är skyddsintresset, utan de nätverk och informationssystem som används för att leverera tjänsterna.[101]

Anledningen till att detta är något som är värt att främja är att en

99 2 § 4 p. NIS-lagen.

100 MSB:s föreskrifter och allmänna råd om frivillig rapportering av incidenter i tjänster som är viktiga för samhällets funktionalitet, MSBFS 2018:11.

101 1 § NIS-lagen.

hög nivå av säkerhet är nödvändigt för att säkerställa kontinuiteten till tjänsterna. Genom en hög nivå av säkerhet ska den inre marknadens förbättras genom att skapa tillit och förtroende.[102] Detta innebär, annorlunda uttryckt, att regelverkets yttersta skyddsintresse är EU:s gemensamma inre marknad.

3.2.3 HOTBILD

Den hotbild som NIS-lagen tar sikte på utgår från omständigheter och händelser med negativ inverkan på säkerheten i nätverk och informationssystem, som rimligen kan identifieras. Med säkerhet i nätverk och informationssystem avses förmågan att motstå åtgärder som undergräver tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten hos uppgifter eller tjänster.[103]

I sammanhanget är det särskilt intressant att uppmärksamma det faktum att NIS-lagstiftningen i beskrivningen av hotbild och skyddsintresse avviker från den klassiska CIA-triaden genom att behandla autenticitet som separat egenskap och inte en del av egenskapen riktighet. Den svenska lagtexten använder denna term där den svenska översättningen av direktivet använder ”integritet”, för att bättre stämma överens med etablerad svensk terminologi.[104] Det framgår dock inte varför just detta begrepp har lyfts fram på samma nivå som övriga begrepp i CIA-triaden.

3.3 Process

3.3.1 ALLMÄNT OM PROCESSEN

Varken NIS-direktivet eller NIS-lagen anger någon närmare reglering av den process som ska användas för att säkerställa informationssäkerheten. Av NIS-lagen framgår att kraven på process skiljer sig åt beroende på om det är fråga om samhällsviktiga eller digitala tjänster.[105]

För *samhällsviktiga tjänster* ska leverantörerna bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete avseende de nätverk och informationssystem som de använder för att tillhandahålla samhällsviktiga tjänster.[106] I anslutning till lagen har MSB meddelat föreskrifter om hur sådant arbete ska bedrivas.[107] MSB anger bl.a. att varje leverantör ska bedriva ett arbete med stöd av standarderna SS-EN ISO/IEC 27001:2017 och SS-EN ISO/IEC 27002:2017 om ledningssystem för informationssäkerhet eller motsvarande.[108]

---

102 Skäl 1 NIS-direktivet.

103 Artikel 4.1.2 NIS-direktivet.

104 Prop. 2017/18:205 *Informationssäkerhet för samhällsviktiga tjänster och digitala tjänster*, s. 31.

105 11-14 §§ jämförda med 15-16 §§ NIS-lagen.

106 11 § NIS-lagen.

107 MSBFS 2018:7.

108 5 § MSBFS 2018:7.

Det finns alltså inget krav på att tillämpa eller certifiera sig enligt just ISO 27000-serien, men den struktur och den riskbaserade approach som framgår av standarden fungerar ändå som riktmärke för hur arbetet ska bedrivas. Det kan i sammanhanget uppmärksammas att MSB även meddelat föreskrifter för statliga myndigheters informationssäkerhet, som ålägger myndigheter att bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete med stöd av ett ledningssystem för informationssäkerhet och att i detta beakta standarderna ISO/IEC 27001:2014 och ISO/IEC 27002:2014.[109]

MSB har även tagit fram ett metodstöd för systematiskt och riskbaserat informationssäkerhetsarbete, som kan användas för att uppfylla kraven i NIS-lagen.[110] Metodstödet har en liknande struktur som ledningssystem för informationssäkerhet enligt SS-EN ISO/IEC 27001:2017, men definierar de olika stegen något annorlunda.

Vår tolkning är att en tjänsteleverantör av samhällsviktiga tjänster som omfattas av NIS-lagstiftningen inte är ålagd att följa någon av dessa processer, men det kan vara ett sätt att säkerställa att det informationssäkerhetsarbete som man är skyldig att bedriva uppfyller kraven på att vara systematiskt och riskbaserat. Om man jobbar efter en annan modell krävs att modellen är ”motsvarande” ISO 27000-standarden.

I lagstiftningen finns även specifika krav som kan placeras in i dessa processer. Vi har därför valt att utgå från MSB:s metodstöd i nedanstående genomgång, och där enskilda regleringskrav kan passas in i denna struktur lyfter vi särskilt fram dessa.

Utöver de nedanstående stegen bör även bestämmelserna i MSBFS 2018:8, om hur en tjänsteleverantör ska arbeta med informationssäkerhet, uppmärksammas.[111] Dessa innefattar krav på att (i) upprätta en informationssäkerhetspolicy och interna regler och stöd i övrigt, (ii) ha ett dokumenterat arbetssätt för informationsklassning, riskbedömning, införande av säkerhetsåtgärder, uppföljning och dokumentering av åtgärder, (iii) säkerställa att medarbetarna har kunskap om säker hantering av information, (iv) säkerställa att nätverk och informationssystem uppfyller de identifierade informationssäkerhetsbehoven, (v) minimera konsekvenserna av incidenter och avvikelser, och (vi) tydliggöra hur behovsanalys och säkerställande av kontinuitet m.m. sker.[112]

För *digitala tjänster* är kraven lägre och omfattar endast att leverantörerna ska vidta de tekniska och organisatoriska åtgärder som de anser ändamålsenliga och proportionella, men utan samma krav på att arbeta efter en systematisk process.[113]

---

109 MSB:s föreskrifter och allmänna råd om statliga myndigheters informationssäkerhet, MSBFS 2016:1.

110 Metodstödet är publicerat på https://www.informationssakerhet.se/metodstodet/. Läst den 24 februari 2020.

111 MSB:s föreskrifter och allmänna råd om informationssäkerhet för leverantörer av samhällsviktiga tjänster, MSBFS 2018:8.

112 7-12 §§ MSBFS 2018:8.

113 15 § NIS-lagen.

3.3.2 IDENTIFIERING

NIS-regleringen innehåller ingen reglering för hur skyddsvärda objekt inom nätverk och informationssystem ska identifieras. Enligt 10 § MSBFS 2018:8 ska samtliga nätverk och informationssystem för samhällsviktiga tjänster hanteras, men hur dessa identifieras och avgränsas får hanteras inom ramen för det strukturerade informationssäkerhetsarbete som tjänsteleverantören är skyldig att bedriva.

MSB:s metodstöd hanterar identifiering av skyddsvärda objekt som en del av analysfasen, specifikt som en del av verksamhetsanalysen. I denna fas identifieras skyddsvärda informationstillgångar utifrån bl.a. vilken information de omfattar och huruvida de är kritiska för verksamheten. Denna identifiering görs efter att organisationens interna intressenter och förutsättningar har inventerats. För att tillgångarna ska kunna bedömas som skyddsvärda måste dock en informationsklassificering genomföras för att identifiera vilken information som är skyddsvärd.

3.3.3 ANALYS

I analysfasen ställs krav på att göra en riskanalys med åtgärdsplan som ska ligga till grund för val av säkerhetsåtgärder.[114] Riskanalysen är dock bara en del av en fullständig analys, som enligt MSB:s metodstöd består av följande delar

- **Omvärldsanalys**, som omfattar kartläggning av externa krav. Den lagstiftning som man som tjänsteleverantör har att följa kartläggs som en del av de externa kraven.

- **Verksamhetsanalys** (beskrivs ovan i avsnitt 3.3.2).

- **Riskanalys**, som identifierar informationssäkerhetsrisker utifrån de tre frågorna ”Vad kan hända?”, ”Hur sannolikt är det?” och ”Vad blir konsekvenserna?”, och som också utgör grund för att välja relevanta säkerhetsåtgärder.

- **Gapanalys**, som fokuserar på gapet mellan de säkerhetsåtgärder man tar utgångspunkt i (från en lista på identifierade åtgärder) och den nuvarande statusen på respektive säkerhetsåtgärd.

3.3.4 UTFORMNING AV SKYDD

Analysfasen följs av en utformningsfas. Denna fas består av utformningen av organisation, informationssäkerhetsmål, styrdokument, klassningsmodell och handlingsplan. Fasen tar med andra ord sikte på mer än utformning av skyddsåtgärder, vilket görs som ett steg av framtagandet av en s.k. klassningsmodell.

---

114 12 § NIS-lagen.

Leverantörer av samhällsviktiga tjänster ska vidta dels ändamålsenliga och proportionella åtgärder för att hantera risker, dels lämpliga åtgärder för att förebygga och minimera verkningar av incidenter.[115] Närmare reglering av hur detta ska gå till ges i NIS-förordningen, som anger att man ska beakta accepterade standarder och vad som ska beaktas vid en bedömning om de utformade skyddsåtgärderna säkerställer en lämplig säkerhetsnivå.[116]

Motsvarande reglering för leverantörer av digitala tjänster finns i NIS-lagen, men begränsat till tillhandahållandet/erbjudandet av tjänsterna inom EU.[117]

3.3.5 TILLÄMPNING

I MSB:s metodstöd finns en efterföljande användningsfas, under vilken man klassar information enligt klassningsmodellen man tagit fram under förra fasen, genomför handlingsplanen och efterlever antagna styrdokument, samt utbildar och kommunicerar inom organisationen.

NIS-lagen innehåller ingen specifik reglering av hur informationssäkerhetsarbetet ska ske i denna fas. I den mån det uppstår incidenter ska leverantören dock hantera detta genom att bl.a. rapportera vissa incidenter till MSB. För leverantörer av samhällsviktiga tjänster gäller att det ska vara fråga om incidenter som har en betydande inverkan på kontinuiteten i tjänsten och för digitala tjänster att det ska vara fråga om incidenter som har en avsevärd inverkan på tillhandahållandet av tjänsten som de erbjuder inom EU.[118]

MSB, i egenskap av CSIRT-enheten (se vidare i avsnitt 3.6.2 nedan), tar sedan emot incidentrapporterna och fastställer omfattningen av de gränsöverskridande verkningarna.[119]

3.3.6 UPPFÖLJNING

I MSB:s metodstöd består denna fas av två delar: utvärdera och följa upp, respektive ledningens genomgång. Ledningsgenomgången kan sedan leda till en uppdaterad handlingsplan och styrdokument som tas omhand i utformningsfasen. Utvärderingen syftar ytterst till att bedöma om de beslutade säkerhetsåtgärderna och övriga delar av säkerhetsarbetet är ändamålsenliga och tillförsäkrar en lämplig säkerhetsnivå utifrån de risker som finns. Det kan i detta arbete även förekomma extern revision.

Den riskanalys som leverantören ska ta fram ska uppdateras årligen.[120]

---

115 13-14 §§ NIS-lagen.

116 5-6 §§ NIS-förordningen.

117 15-16 §§ NIS-lagen.

118 18 § respektive 19 § NIS-lagen.

119 13 § NIS-lagen.

120 12 § NIS-lagen.

Det framgår vidare av MSBFS 2018:8 att en leverantör efter en avslutad incidenthantering ska vidta åtgärder för att förhindra liknande incidenter.[121]

3.4 Konkreta informationssäkerhetskrav

3.4.1 ALLMÄNT

NIS-lagen innehåller i sig inte någon informationsklassificeringsmodell. Den primära indelningen handlar istället om huruvida man levererar en samhällsviktig tjänst eller en digital tjänst.

Det finns ett antal säkerhetsskyddsåtgärder som tjänsteleverantören måste eller bör vidta. Dessa är dock inte direkt kopplade till klassificering av uppgifter, utan beror på vilken typ av tjänst det är fråga om.

3.4.2 MINIMIÅTGÄRDER

Begreppet ”minimiåtgärder” är något svårtillämpat enligt lagstiftningens struktur. De skyddsåtgärder som anges nedan återfinns bara delvis i bindande lagstiftning. Vad gäller samhällsviktiga tjänster framgår vilka åtgärder som bör tillämpas i form av icke-bindande allmänna råd till MSBFS 2018:8. Vad gäller digitala tjänster framgår kraven av artikel 2 i EU:s genomförandeförordning (EU) 2018/151. Den senare förordningen förtydligar vad som ska innefattas i vissa krav på digitala tjänster enligt artikel 16.1 NIS-förordningen, vilken motsvaras av 6 § i den svenska NIS-förordningen. Minimiåtgärderna i de båda källorna överlappar delvis vad gäller huvudsyftet med varje åtgärd, även om åtgärderna beskrivs på olika sätt.

Utöver dessa minimiåtgärder är varje leverantör av samhällsviktiga eller digitala tjänster, så som de definieras i NIS-regleringen, skyldig att själv analysera behovet av skyddsåtgärder och införa dessa. De minimiåtgärder som framgår av MSB:s allmänna råd respektive genomförandeförordningen är översiktligt beskrivna. De är inte uttryckligen korrelerade med de kataloger över säkerhetsåtgärder som finns i exempelvis ISO/IEC 27002. Det är dock ofta uppenbart att enskilda säkerhetsåtgärder i sådana kataloger fyller motsvarande syfte som enskilda minimiåtgärder nedan. Exempelvis finns ett krav på hur informationsklassning ska ske enligt de allmänna råden till 8 § MSBFS 2018:8. Detta krav motsvaras i allt väsentligt av avsnitt 8.2 i ISO/IEC 27002, som dock är mycket mer detaljerat. Den vägledning som finns i exempelvis ISO/IEC 27002 torde vara relevant, i vart fall som inspiration, när man inför nedanstående minimiåtgärder.

121 11 § MSBFS 2018:8.

			SAMHÄLLSVIKTIG TJÄNST	DIGITAL TJÄNST
1.	Allmänna råd till 6 § MSBFS 2018:8	Säkerställ att medarbetare med särskilda roller inom informationssäkerhetsarbetet har nödvändig kunskap och kompetens för dessa	×	
2.	Allmänna råd till 6 § MSBFS 2018:8, jfr artikel 2.4 (b) i (EU) 2018/151	Utvärdera informationssäkerhetsarbetet regelbundet	×	×
3.	Allmänna råd till 8 § MSBFS 2018:8	Informationsklassning och riskbedömning ska ske efter bestämda kriterier och nivåer, vid bestämda tidpunkter och situationer, och av bestämda roller	×	
4.	Allmänna råd till 9 § MSBFS 2018:8	Utvärdera organisationens förmåga att förmedla kunskap om säker hantering av information minst vartannat år	×	
5.	Allmänna råd till 10 § MSBFS 2018:8	Tekniska hot och sårbarheter ska löpande identifieras och omhändertas	×	
6.	Allmänna råd till 10 § MSBFS 2018:8, jfr även artikel 2.1 (a) i (EU) 2018/151	Nätverk- och informationssystem ska vara korrekt och tillräckligt dokumenterade	×	×
7.	Allmänna råd till 10 § MSBFS 2018:8	Separata miljöer bör upprättas för test och utveckling som är skilda från produktionsmiljön	×	
8.	Allmänna råd till 10 § MSBFS 2018:8	Överväg alltid om krypto- och it-säkerhets-produkter ska vara tredjepartcertifierade mot relevanta standarder	×	
9.	Allmänna råd till 11 § MSBFS 2018:8	Loggning ska ske för att identifiera och verifiera händelser. Spårbar tid ska användas	×	
10.	11 § MSBFS 2018:8 med allmänna råd, samt artikel 2.2 i (EU) 2018/15	Konsekvenser av incidenter och avvikelser ska minimeras. Incidenter och avvikelser ska han-teras sammanhållet och leda till förbättringar	×	×
11.	Allmänna råd till 12 § MSBFS 2018:8 samt artikel 2.3 i (EU) 2018/15	Kontinuitet ska uppnås vid incidenter och avvikelser	×	×
12.	Artikel 2.1 (b) i (EU) 2018/15	Säkerhetsarbetet ska omfatta fysisk säkerhet och miljösäkerhet		×
13.	Artikel 2.1 (c) i (EU) 2018/15	Säkerhetsarbetet ska omfatta försörjnings-trygghet		×

			SAMHÄLLSVIKTIG TJÄNST	DIGITAL TJÄNST
14.	Artikel 2.1 (d) i (EU) 2018/15	Åtkomst till nätverk och informationssystem ska vara kontrollerad		×
15.	Artikel 2.4 (a) i (EU) 2018/151	Test av nät- och informationssystemen ska ske med en planerad sekvens av observationer och mätningar		×
16.	Artikel 2.4 (c) i (EU) 2018/151	Det ska finnas tekniska processer och personal för att avslöja brister i ett nät- och informations-systems säkerhetsmekanismer		×

3.5 Särskilda krav på utkontraktering

Utkontraktering av verksamhet som rör samhällsviktiga eller digitala tjänster är inte detaljreglerat. För samhällsviktiga tjänster ska dock kravet på systematiskt och riskbaserat informationssäkerhetsarbete omfatta även den hantering av nätverk och informationssystem som utkontrakteras till en extern aktör.[122] Inför utkontraktering ska därför risker för den samhällsviktiga tjänsten identifieras och hanteras. De säkerhetsåtgärder som den externa aktören ska vidta ska regleras i avtal. I MSB:s allmänna råd till MSBFS 2018:8 förordas även att det av avtalet ska framgå hur den externa aktören ska överlämna information till leverantören om misstänkta eller inträffade incidenter, avvikelser och sårbarheter, samt vilka krav på kunskap och kompetens avseende informationssäkerhet som ställs.

Det uppställs alltså inget krav på att underleverantören (den externa aktören) själv tillämpar ett systematiskt och riskbaserat informationssäkerhetsarbete, men tjänsteleverantören ansvarar för att även de delar som utkontrakteras hanteras på ett sådant sätt.

3.6 Gränssnitt mot myndigheter

3.6.1 MYNDIGHETERS TILLSYN

NIS-lagens tillämpningsområde vad gäller samhällsviktiga tjänster är strukturerat efter olika sektorer. Även tillsynen följer denna sektorindelning. Enligt 17 § NIS-förordningen ansvarar följande myndigheter för tillsyn:

122 2 § MSBFS 2018:8.

TILLSYNSMYNDIGHET	SEKTOR
Energimyndigheten	Energisektorn, t.ex. flyg- och järnvägstransport
Transportstyrelsen	Transportsektorn, t.ex. elproduktion och gasförsörjning
Finansinspektionen	Bankverksamhet och finansmarknadsinfrastruktur
Inspektionen för vård och omsorg	Hälso- och sjukvård
Livsmedelsverket	Leverans och distribution av dricksvatten
Post- och telestyrelsen	Digital infrastruktur samt även digitala tjänster

I tillsynsuppdraget ingår bl.a. att informera MSB om vilka tjänsteleverantörer som anmält att de omfattas av NIS-lagen, vartannat år rapportera om de leverantörer de utövar tillsyn över till MSB, ge vägledning för tillämpning av NIS-regelverket samt samarbeta med Datainspektionen vid hantering av incidenter som även utgör personuppgiftsincidenter enligt dataskyddsförordningen.[123]

Det sagda innebär att MSB inte har något eget tillsynsuppdrag som innebär direkt kontakt med tjänsteleverantörer. Däremot har myndigheten ett samordningsuppdrag i syfte att åstadkomma en effektiv och likvärdig tillsyn.[124] Myndigheten är också nationell kontaktpunkt enligt NIS-direktivet med ansvar för att bl.a. säkerställa gränsöverskridande samarbete mellan medlemsstaternas myndighet, lämna årliga rapporter till den EU-gemensamma samarbetsgruppen samt vidarebefordra vissa incidentrapporter till kontaktpunkter i andra medlemsstater som påverkats av incidenten.[125]

3.6.2 INCIDENTRAPPORTERING

En incident enligt NIS-lagstiftningen är en händelse med faktisk negativ inverkan på säkerheten i nätverks- och informationssystem.[126] Tjänsteleverantörer är skyldiga att rapportera vissa incidenter, men långt ifrån alla. Det avgörande kriteriet för om rapporteringsplikt föreligger är olika för samhällsviktiga respektive digitala tjänster.

I fråga om samhällsviktiga tjänster omfattas alla incidenter som har en betydande inverkan på kontinuiteten i tjänsten, medan rapporteringsplikten för digitala tjänster endast omfattar incidenter som har en avsevärd inverkan på tillhandahållandet av en tjänst som erbjuds

123 19 § NIS-förordningen.

124 21 § NIS-förordningen.

125 Se artiklarna 8.4 och 10.3 andra stycket NIS-direktivet.

126 2 § 10 p. NIS-lagen.

inom EU.[127] Vägledning till vad som ska beaktas vid dessa bedömningar finns i 9 och 10 §§ NIS-förordningen.

Rapportering ska ske till en särskild CSIRT-enhet (Computer Security Incident Response Team). I Sverige utgörs den av CERT-SE, som organisatoriskt är en del av MSB. Rapporteringsförfarandet är i båda fallen uppdelat i tre skeden, fokuserat på att till en början möjliggöra för CSIRT-enheten och MSB att hjälpa leverantören med incidenten och skapa en samlad lägesbild. Inom sex timmar från det att leverantören själv identifierat incidenten som rapporteringspliktig ska CERT-SE underrättas via telefon. Inom 24 timmar ska leverantören lämna skriftlig rapportering. Inom fyra veckor ska sedan en rapportering med utvärdering och förebyggande åtgärder levereras skriftligen. MSB har anvisat särskilda formulär för rapportering i skede 2 och 3.[128]

3.6.3 SAMRÅD

Det finns inga bestämmelser i den svenska lagstiftningen som reglerar samråd mellan tjänsteleverantörerna och någon myndighet om frågor som rör NIS-regleringen.

3.6.4 SANKTIONER

Det är tillsynsmyndigheten för den aktuella tjänsteleverantören som beslutar om sanktionsavgifter. Sanktionsavgift kan tas ut av den som underlåter att (i) göra en anmälan till tillsynsmyndigheten, (ii) vidta säkerhetsåtgärder, eller (iii) rapportera incidenter, och kan bestämmas till mellan 5 000 och 10 miljoner kronor.[129]

127 18-19 §§ NIS-lagen.

128 https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/nis-direktivet/incidentrapportering-for-nis-leverantorer/incidentrapportering-for-leverantorer-av-samhallsviktiga-tjanster/. Läst den 24 februari 2020.

129 29 § NIS-lagen.

4. Informationssäkerhet enligt dataskyddsförordningen

4.1 Inledning

Dataskyddsförordningen syftar till att skydda fysiska personer vid behandling av personuppgifter. Dataskyddsförordningen reglerar hur personuppgifter ska skyddas samt under vilka förutsättningar behandling av personuppgifter är tillåten. Begreppet *behandling* definieras mycket brett, och dataskyddsförordningen kan därför ses som en informationssäkerhetsreglering i bred bemärkelse.[130] De grundläggande principerna för personuppgiftsbehandling utgör grunden för skyddsåtgärder som ska förhindra att de registrerades personliga integritet, rättigheter och friheter kränks genom de risker som kan förekomma vid behandling av personuppgifter.[131]

Med detta sagt, finns det även delar av dataskyddsförordningen som tar sikte på informationssäkerhet i en snävare bemärkelse. Dataskyddsförordningen ställer krav på att den personuppgiftsansvarige ska utforma själva behandlingen genom att genomföra lämpliga tekniska och organisatoriska åtgärder för att skydda de registrerades rättigheter (s.k. inbyggt dataskydd) och för att säkerställa att personuppgifter endast behandlas om det är nödvändigt, med avseende på mängden uppgifter, behandlingens omfattning, tidsperiod för lagring och tillgänglighet för själva uppgifterna (s.k. dataskydd som standard).[132]

Både den personuppgiftsansvarige och personuppgiftsbiträdet ska säkerställa en lämplig säkerhetsnivå för behandlingen med hänsyn till möjligheter, kostnader och risker. De exemplifierande åtgärder som nämns i artikeltexten utgör vanliga informationssäkerhetsåtgärder, däribland pseudonymisering, kryptering och regelbundna tester, undersökningar och utvärderingar.[133] Av den grundläggande principen om integritet och konfidentialitet gäller även att personuppgifter ska behandlas på ett sätt som säkerställer lämplig säkerhet för personuppgifterna, inbegripet skydd mot obehörig eller otillåten behandling och mot förlust, förstöring eller skada genom olyckshändelse, med användning av lämpliga tekniska eller organisatoriska åtgärder.

Utöver dataskyddsförordningen finns även kompletterande nationell

130 Artikel 4.2 dataskyddsförordningen.

131 Se principerna i artikel 5 dataskyddsförordningen om a) laglighet, korrekthet och öppenhet, b) ändamålsbegränsning, c) uppgiftsminimering, d) korrekthet, e) lagringsminimering och f) integritet och konfidentialitet. Därutöver ska den personuppgiftsansvarige ansvara för och kunna visa på att dessa principer efterlevs, enligt principen om ansvarsskyldighet.

132 Artikel 25 dataskyddsförordningen.

133 Artikel 32 dataskyddsförordningen.

lagstiftning. För svenskt vidkommande är dataskyddslagen den mest centrala regleringen, men det finns även en rad sektorsspecifika regleringar. Bakgrunden till dessa är i många fall att behandling som är nödvändig för ett allmänt intresse eller för myndighetsutövning måste ha en grund i nationell rätt (eller unionsrätt). Sådana bestämmelser i nationell rätt kan även innehålla anpassande bestämmelser för hur behandlingen ska utföras.[134]

När det gäller behandling av känsliga personuppgifter som är nödvändig för ett viktigt allmänt intresse, av allmänt intresse på folkhälsoområdet eller för forskningsändamål, krävs det uttryckligen att den nationella regleringen innehåller bestämmelser om lämpliga och särskilda åtgärder för att säkerställa den registrerades rättigheter.[135] Ett sådant exempel är personuppgiftsbehandling för forskningsändamål. För att det ska vara tillåtet ställer 6 § lag (2003:460) om etikprövning av forskning som avser människor ett krav på att forskningen ska godkännas vid ett särskilt etikprövningsförfarande. Ett sådant godkännande kan förenas med villkor, som i sig kan vara informationssäkerhetsåtgärder, t.ex. att uppgifterna endast får behandlas på datorutrustning som inte är ansluten till nätverk.

Utöver bestämmelser i dataskyddsförordningen och nationell lagstiftning som antagits i samband med förordningen, öppnar dataskyddsförordningen för självreglering avseende informationssäkerhetsåtgärder genom uppförandekoder i enlighet med artikel 40.

4.2 Avgränsningar

4.2.1 TILLÄMPNINGSOMRÅDE

Dataskyddsförordningen har ett mycket brett tillämpningsområde och ska tillämpas av i princip alla som omfattas av unionsrätten – såväl myndigheter och företag som privatpersoner – i sådan verksamhet som inte är av rent privat natur eller som har samband med dennes hushåll.[136]

Som EU-rättsakt är dataskyddsförordningen bara tillämplig på områden som omfattas av unionsrätten. Det är inte alltid helt tydligt var gränsen mellan unionsrätt och rent nationell rätt går, men enligt dataskyddsförordningens skäl 16 nämns särskilt verksamhet rörande nationell säkerhet som ett sådant område. Den svenska dataskyddslagen utökar dock tillämpningsområdet på så sätt att den även omfattar området utanför unionsrätten, inklusive Sveriges säkerhet, om än med vissa undantag. Av särskild betydelse för den fortsatta framställningen är att reglerna för rapportering av personuppgiftsincidenter inte ska

134 Artikel 6.3 dataskyddsförordningen.

135 Artikel 9.2 g), i) och h) dataskyddsförordningen. Se även artikel 89 dataskyddsförordningen för säkerhetsåtgärder och undantag för behandlingen.

136 Artikel 2 och 3 dataskyddsförordningen där förordningens materiella och territoriella tillämpningsområde framgår.

tillämpas för behandling inom sådan verksamhet som omfattas av säkerhetsskyddslagen och dess reglering av incidentrapportering.[137]

I denna rapport har vi valt att fokusera på den personuppgiftsansvariges[138] skyldigheter att efterleva informationssäkerhetskraven i dataskyddsförordningen. Detta dels då personuppgiftsbiträden[139] endast ska behandla personuppgifter enligt den personuppgiftsansvariges instruktion, dels för att en personuppgiftsansvarigs skyldigheter är betydligt mer långtgående och omfattande än ett personuppgiftsbiträdes. Med det sagt, bär såväl personuppgiftsansvariga och personuppgiftsbiträden ett eget ansvar för att säkerställa att informationssäkerhetskraven efterlevs när denne behandlar personuppgifter.[140] Detta avsnitt är således ändå relevant för både personuppgiftsansvariga och personuppgiftsbiträden.

4.2.2 SKYDDSINTRESSE

Det skyddsintresse som anges i dataskyddsförordningen är den enskilda, fysiska personens grundläggande rättigheter och friheter, särskilt rätten till skydd av personuppgifter.[141]

Frågan om vad som utgör ett hot mot denna rätt är mångfacetterad, men klart är att det inte enbart handlar om när uppgifter blir tillgängliga för obehöriga. Även det fall att en aktör (personuppgiftsansvarig eller -biträde) har rätt att ha tillgång till uppgifterna, men använder uppgifterna för andra ändamål än vad behörigheten omfattar, utgör en kränkning av detta skydd. Skyddet för personuppgifter omfattar även den enskildes rätt att dennes personuppgifter ska vara korrekta.[142]

Vid en jämförelse med den klassiska CIA-triaden kan det sägas att dataskyddsförordningens skyddsintresse i första hand tar sikte på konfidentialitet, i andra hand riktighet. Även tillgänglighet tas i viss mån upp, särskilt genom krav på informationssäkerhet i samband med behandling av personuppgifter.

4.2.3 HOTBILD

Den hotbild som framgår av dataskyddsförordningen är en spegelbild av skyddsintresset. Regleringen syftar, i all sin enkelhet såväl som komplexitet, till att förebygga och hindra all form av behandling av enskildas personuppgifter som inte sker i enlighet med förordningen.

---

137 1 kap. 4 § dataskyddslagen.

138 En fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter, se artikel 4.7 dataskyddsförordningen.

139 En fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning, se artikel 4.8 dataskyddsförordningen.

140 Artikel 32.1 dataskyddsförordningen.

141 Artikel 1.2 dataskyddsförordningen.

142 Artiklarna 5.1 d) och 16 dataskyddsförordningen.

4.3 Process

4.3.1 ALLMÄNT OM PROCESSEN

Dataskyddsförordningen anger inte någon detaljerad process för hur informationssäkerhetsarbetet ska bedrivas, utan fokuserar på att den personuppgiftsansvarige ska säkerställa att personuppgifter behandlas enligt förordningen.[143] Det lämnas därför utrymme för självreglering av sådana processer, t.ex. genom uppförandekoder och/eller certifieringsmekanismer. Med detta sagt, är det ändå möjligt att utgå från den generella process som vi redogjort för i avsnitt 1.5 och ta hänsyn till vilka bestämmelser i dataskyddsförordningen som aktualiseras i de olika skedena.

För personuppgiftsbehandling som sannolikt leder till en hög risk för det skyddsintresse som förordningen ska skydda, är det obligatoriskt att utföra en bedömning av den planerade behandlingens konsekvenser för skyddet av personuppgifter. För att överhuvudtaget kunna ta ställning till om en viss behandling sannolikt leder till en hög risk för skyddsintresset, är vi av uppfattningen att en personuppgiftsansvarig först bör genomföra en s.k. riskanalys. Därefter, ifall riskanalysen visar att det är sannolikt att behandlingen ifråga kommer att leda till en sådan hög risk (givet att inget av de nedan angivna undantagen är tillämpliga, se avsnitt 4.3.3 nedan), ska en fullständig konsekvensbedömning genomföras.

4.3.2 IDENTIFIERING

Innan vare sig en riskanalys eller konsekvensbedömning kan genomföras måste den faktiska personuppgiftsbehandlingen identifieras, kartläggas och dokumenteras. Enligt dataskyddsförordningen ska den personuppgiftsansvarige föra ett register över behandling som utförs under dennes ansvar.[144] Registret ska innehålla följande:

- Namn och kontaktuppgifter för den personuppgiftsansvarige, samt, ifall av gemensamt personuppgiftsansvariga, den personuppgiftsansvariges företrädare samt dataskyddsombudet;
- Ändamålen med behandlingen;
- En beskrivning av kategorierna av registrerade och kategorierna av personuppgifter;
- De kategorier av mottagare till vilka personuppgifterna har lämnats eller ska lämnas ut, inbegripet mottagare i tredjeländer eller i internationella organisationer;

143 Det bör dock sägas att dataskyddsförordningens krav på inbyggt dataskydd och dataskydd som standard kan ses som en metod för hur personuppgiftsansvariga ska arbeta med informationssäkerhet, se artikel 25 dataskyddsförordningen.

144 Artikel 30 dataskyddsförordningen.

- I tillämpliga fall, överföringar av personuppgifter till ett tredjeland eller en internationell organisation, inbegripet identifiering av tredjelandet eller den internationella organisationen och, vid sådana överföringar som avses i artikel 49.1 andra stycket, dokumentationen av lämpliga skyddsåtgärder;

- Om möjligt, de förutsedda tidsfristerna för radering av de olika kategorierna av uppgifter; och

- Om möjligt, en allmän beskrivning av de tekniska och organisatoriska säkerhetsåtgärder som avses i artikel 32.1.

Utöver de obligatoriska uppgifterna ovan anser vi att även följande bör anges i registret, i syfte att dels få en mer fullständig överblick över personuppgiftsbehandlingen, dels underlätta arbetet vid förfrågningar från registrerade:

- Med vilket rättsligt stöd de aktuella personuppgifterna behandlas, även för känsliga personuppgifter, uppgifter om lagöverträdelse, personnummer;

- En beskrivning av flödet, dvs. hur personuppgifter samlas in och behandlas och slutligen raderas, bl.a. vilka it-system som används;

- En beskrivning av omfattningen av behandling bl.a. antalet registrerade, antalet uppgifter om varje registrerad, geografisk räckvidd, bevarandetid;

- Vilken information de registrerade har fått vid insamlingen av personuppgifterna;

- Om det förekommer automatiserat beslutsfattande och profilering;[145]

- De särskilda dataskyddsrisker som den aktuella behandlingen kan innebära;

- Vilka som har åtkomst till personuppgifterna;

- Om personuppgiftsbehandlingen omfattas av särskilda regler om t.ex. särskilda svenska regler om personuppgiftsbehandling (s.k. registerförfattningar), arkivering eller sekretess; och

- Hur rutiner för att tillgodose de registrerades rättigheter ser ut, t.ex. hur s.k. registerutdrag ska kunna lämnas ut, eller hur en begäran om rättelse eller radering ska utföras för de aktuella personuppgifterna.

Det är även lämpligt att därefter ange information om och dokumentera att en riskanalys, och/eller konsekvensbedömning, har utförts och vad slutsatsen var.[146]

---

145 Enligt dess definition i artikel 4.4 dataskyddsförordningen.

146 Jfr exempelvis artikel 35.7 dataskyddsförordningen.

4.3.3 ANALYS

För att den personuppgiftsansvarige ska kunna identifiera sådana särskilt riskfyllda behandlingar som omfattas av kravet på konsekvensanalys, ska den personuppgiftsansvarige ta ställning till om behandlingen kan medföra en hög risk för fysiska personers rättigheter och friheter.[147] Som framgår ovan anser vi att en inledande riskanalys alltid bör göras inför en ny behandling. Det är viktigt att riskanalyser utförs tidigt i planeringen av en behandling, dels eftersom det är en förutsättning för att kunna beakta principerna om inbyggt dataskydd och dataskydd som standard[148], dels för att göra en kompletterande konsekvensbedömning om nödvändigt.

Av dataskyddsförordningen framgår en icke-uttömmande lista på vilka risker vid behandling av personuppgifter som särskilt bör beaktas. Risker med en personuppgiftsbehandling tolkas brett, och innefattar fysiska, materiella och immateriella skador.[149]

Inledningsvis, och som en del av den initiala riskanalysen, bör riskerna med behandlingen naturligtvis bedömas. Riskerna ska beaktas utifrån behandlingens art, omfattning, sammanhang och ändamål. Respektive risk bör vidare utvärderas på grundval av en objektiv bedömning, genom vilken det fastställs huruvida personuppgiftsbehandlingen inbegriper en (normal) risk eller en hög risk.[150] Om behandlingen sannolikt leder till en hög risk för de registrerades rättigheter och friheter är den personuppgiftsansvarige, *innan* den planerade personuppgiftsbehandlingen påbörjas, skyldig att genomföra en konsekvensbedömning där dataskyddsombudet bistår.[151]

Datainspektionen har publicerat en förteckning med kriterier som kan innebära krav på att konsekvensbedömning utförs. Förteckningen innehåller även exempel på när en konsekvensbedömning typiskt sett behöver genomföras.[152] Enligt förteckningen ska, som huvudregel, en

---

147 Artikel 35 dataskyddsförordningen.

148 Se artikel 25 dataskyddsförordningen.

149 Se skäl 75 till dataskyddsförordningen. Riskerna gäller i synnerhet om behandlingen kan leda till diskriminering, identitetsstöld eller bedrägeri, ekonomisk förlust, skadat anseende, förlust av konfidentialitet när det gäller personuppgifter som omfattas av tystnadsplikt, obehörigt hävande av pseudonymisering eller annan betydande ekonomisk eller social nackdel; den registrerade kan berövas sina rättigheter och friheter eller hindras att utöva kontroll över sina personuppgifter; personuppgifterna som behandlas avslöjar särskilda personuppgifter (artikel 9) eller som rör fällande domar i brottmål samt överträdelser (artikel 10); personliga aspekter bedöms, framför allt analyser eller förutsägelser beträffande sådant som rör exempelvis arbetsprestationer, ekonomisk ställning, hälsa, personliga preferenser eller intressen, tillförlighet eller beteende, vistelseort eller förflyttningar i syfte att skapa eller använda personliga profiler; det sker behandling av personuppgifter rörande sårbara fysiska personer, framför allt barn; eller behandlingen inbegriper ett stort antal personuppgifter och gäller ett stort antal registrerade.

150 Se artikel 35.1 och skäl 76 dataskyddsförordningen.

151 Artikel 35.2 dataskyddsförordningen. Ett dataskyddsombud ska utses under särskilda omständigheter, se artikel 37 dataskyddsförordningen. Med det sagt finns det inget hinder för en personuppgiftsansvarig/personuppgiftsbiträde att utse ett dataskyddsombud enligt artikel 37 trots att ingen sådan skyldighet föreligger.

152 Datainspektionen, *Förteckning enligt artikel 35.4 i Dataskyddsförordningen* (2019), dnr. DI-2018–13200. Ytterligare vägledning, som även ligger till grund för Datainspektionens förteckning, finns i Artikel 29-gruppens *Riktlinjer om konsekvensbedömning avseende dataskydd och fastställande av huruvida behandlingen "sannolikt leder till en hög risk" i den mening som avses i förordning 2016/679,* beslutade den 4 april 2017, senast reviderade den 4 oktober 2017.

konsekvensbedömning genomföras om minst två av de kriterier som anges i sammanställningen är vid handen. I uppräkningen anges bl.a. omfattande behandling av personuppgifter, användning av ny teknik och automatiserade beslut med rättsliga följder. Det finns dock tre uttryckliga undantag i dataskyddsförordningen från skyldigheten att genomföra en konsekvensbedömning:

- Behandlingens art, omfattning, sammanhang och ändamål är mycket lik en annan behandling för vilken konsekvensbedömning redan har genomförts av den personuppgiftsansvarige. I dessa fall kan resultatet från den första konsekvensbedömningen även användas för den andra behandlingen som medför liknande höga risker.[153]

- Om en konsekvensbedömning har genomförts i samband med antagande av lagstiftning som behandlingen grundas på behöver inte bedömningen göras på nytt av den personuppgiftsansvarige. Det gäller när behandlingen grundas på de rättsliga grunderna, fullgörandet av en rättslig förpliktelse[154] eller utförandet av en uppgift av allmänt intresse[155]. Den nationella lagstiftaren kan dock föreskriva att en konsekvensbedömning trots detta ska utföras.

- Behandlingen finns uppräknad i den förteckning som Datainspektionen får upprätta och offentliggöra, över de slags behandlingsverksamheter för vilka det inte kommer att krävas att en konsekvensbedömning genomförs.[156]

Dataskyddsförordningen innehåller en uppräkning av ett antal element som en konsekvensbedömning i vart fall ska innehålla.[157] Artikel 29-gruppen har till sina riktlinjer om konsekvensbedömning bifogat en utförlig förteckning över kriterier för en godtagbar konsekvensbedömning.[158] Där anges bl.a. att den personuppgiftsansvarige ska systematiskt beskriva den planerade behandlingen och behandlingens syfte, behovet av och proportionaliteten hos den planerade behandlingen och hur risker för de registrerades rättigheter och friheter hanteras.

Därutöver åligger det den personuppgiftsansvarige att bedöma behovet av och proportionaliteten hos behandlingen i förhållande till syftena med densamma, men även vilka risker för de registrerades rättigheter och friheter som behandlingen kan leda till.

---

153 Artikel 35.1 dataskyddsförordningen, enligt vilken ”[e]*n enda bedömning kan omfatta en serie liknande behandlingar som medför liknande höga risker*”.

154 Artikel 6.1 c) dataskyddsförordningen.

155 Artikel 6.1 e) dataskyddsförordningen.

156 Artikel 35.5 dataskyddsförordningen. Se närmare Europeiska dataskyddsstyrelsens *Riktlinjer om konsekvensbedömning,* s. 14. Datainspektionen har ännu inte publicerat en sådan lista, och det är oklart om/när Datainspektionen kommer att göra det. Enligt uppgift från Datainspektionen den 15 januari 2020 är framtagningen av en sådan lista i dagsläget inte aktuellt.

157 Artikel 35.7 dataskyddsförordningen.

158 Artikel 29-gruppens *Riktlinjer om konsekvensbedömning avseende dataskydd och fastställande av huruvida behandlingen ”sannolikt leder till en hög risk” i den mening som avses i förordning 2016/679,* bilaga 2.

Utifrån detta ska den personuppgiftsansvarige beskriva de åtgärder som planeras för att hantera riskerna med behandlingen. Detta innefattar skyddsåtgärder, säkerhetsåtgärder, rutiner för att säkerställa dels skyddet av personuppgifterna, dels att dataskyddsförordningen faktiskt följs.

4.3.4 UTFORMNING AV SKYDD

Vilka skyddsåtgärder som krävs enligt dataskyddsförordningen beror på flera faktorer; den senaste utvecklingen, genomförandekostnaderna och behandlingens art, omfattning, sammanhang och ändamål samt riskerna (av varierande sannolikhetsgrad och allvar) för fysiska personers rättigheter och friheter. Samtliga dessa faktorer ska beaktas vid bedömningen av vad som är en lämplig säkerhetsnivå för den aktuella personuppgiftsbehandlingen. De säkerhetsåtgärder som ska vidtas avser såväl tekniska som organisatoriska säkerhetsåtgärder.[159]

Dataskyddsförordningen anger ett antal exempel på åtgärder som kan vidtas för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken, däribland:

- Pseudonymisering och kryptering av personuppgifter;
- Förmågan att fortlöpande säkerställa konfidentialitet, integritet, tillgänglighet och motståndskraft hos behandlingssystemen och -tjänsterna;
- Förmågan att återställa tillgängligheten och tillgången till personuppgifter i rimlig tid vid en fysisk eller teknisk incident; och
- Ett förfarande för att regelbundet testa, undersöka och utvärdera effektiviteten hos de tekniska och organisatoriska åtgärder som ska säkerställa behandlingens säkerhet.[160]

Därtill har Datainspektionen sedan tidigare utarbetat allmänna råd om säkerhet i samband med personuppgiftsbehandling. Dessa är förvisso inte längre gällande, eftersom de togs fram innan dataskyddsförordningen, men kan alltjämt ge vägledning. I de allmänna råden anges bl.a. exempel på fysiska säkerhetsåtgärder, behörighets- och tillträdeskontroll, skydd mot förlust av information och skydd mot skadlig programvara (se vidare avsnitt 4.4.3 nedan).[161]

Det bör noteras att dataskyddsförordningen inte innehåller några konkreta krav *per se* på vilka säkerhetsåtgärder som en personuppgiftsansvarig ska vidta för att säkerställa en lämplig säkerhetsnivå, utan detta överlämnas till den personuppgiftsansvarige att bedöma.[162]

---

159 Artikel 32.1 dataskyddsförordningen.

160 Artikel 32 dataskyddsförordningen.

161 Datainspektionens allmänna råd, *Säkerhet för personuppgifter,* rev. november 2008.

162 Notera att personuppgiftsbiträdet också har ett självständigt ansvar att säkerställa en lämplig säkerhetsnivå i förhållande till risken med personuppgiftsbehandlingen ifråga.

Av dataskyddsförordningen framgår det särskilt att behandlingar som omfattas av kravet på konsekvensbedömning även ska innehålla de åtgärder som planeras för att hantera de identifierade riskerna, inbegripet skyddsåtgärder, säkerhetsåtgärder och rutiner för att säkerställa skyddet av personuppgifterna och för att visa att denna förordning efterlevs, med hänsyn till de registrerades och andra berörda personers rättigheter och berättigade intressen.[163]

Vidare ska även den personuppgiftsansvarige, när det är möjligt, inhämta synpunkter från de registrerade eller deras företrädare om den avsedda behandlingen.[164]

4.3.5 TILLÄMPNING OCH UPPFÖLJNING

Även om den personuppgiftsansvarige genomfört en konsekvensbedömning innan behandlingen påbörjas, upphör inte ansvaret i och med den fullgjorda konsekvensbedömningen. Den personuppgiftsansvarige ska nämligen, enligt artikel 35.11, genomföra en översyn av bedömningen. Översynen ska förvisso göras vid behov, t.ex. när den risk som behandlingen medför ändras, men ett riktmärke föreslås vara att konsekvensbedömningen i vart fall bör uppdateras och genomföras på nytt vart tredje år.[165]

Att översynen ska göras vid behov ställer dock ett krav på den personuppgiftsansvarige. För att kunna identifiera behovet måste det finnas en riskmedvetenhet i behandlingen och/eller verksamheten. Det är en levande, kontinuerlig analys som kan påverkas av en mängd faktorer såsom ändrad behandling, ökade risker, ny teknik eller ökad omfattning.

I avsnitt 4.6.2 nedan kommer den personuppgiftsansvariges incidentrapportering att behandlas.

4.4 Konkreta informationssäkerhetskrav

4.4.1 ALLMÄNT

Dataskyddsförordningen innehåller ytterst få konkreta krav på informationssäkerhet, och består snarare av principiella och övergripande krav.[166] Kraven enligt dataskyddsförordningens krav är istället beroende av den aktuella personuppgiftsbehandlingens art, omfattning, sammanhang och ändamål samt riskerna.

Exempelvis anger dataskyddsförordningen att en lämplig säkerhetsnivå för personuppgifterna ska säkerställas. I dataskyddsförordningen listas icke-uttömmande exempel på lämpliga säkerhetsåtgärder,

163 Artikel 35.7 d) dataskyddsförordningen.

164 Artikel 35.9 dataskyddsförordningen.

165 Advokatfirman Kahn Pedersens skriftserie 2017:2, *GDPR – några tillämpningsfrågor*, s. 59.

166 Se exempelvis artikel 5 och 32 dataskyddsförordningen.

såsom pseudonymisering och kryptering.[167] Det är dock upp till den som behandlar personuppgifterna att bedöma vad som utgör en lämplig säkerhetsnivå samt vilka tekniska och organisatoriska åtgärder som behöver vidtas.

De mest konkreta kraven på informationssäkerhet anser vi snarare avser processer, såsom skyldigheten att iaktta inbyggt dataskydd och dataskydd som standard, genomföra konsekvensbedömningar, incidentrapportering och avtalskrav vid utkontraktering m.m.

Vilka säkerhetsåtgärder som krävs i samband med personuppgiftsbehandling är beroende av den senaste utvecklingen, genomförandekostnaderna och behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar för fysiska personers rättigheter och friheter. Det är således inte möjligt att ta fram en generisk sammanställning av vilka säkerhetsåtgärder som krävs för att uppnå en lämplig säkerhetsnivå.[168] Liksom framgår ovan innehåller dataskyddsförordningen dessutom nästan inga konkreta krav på vilka informationssäkerhetsåtgärder som ska vidtas i samband med personuppgiftsbehandling. Det är därför inte möjligt att sammanställa en lista på minimiåtgärder i betydelsen ”åtgärder som måste vidtas för behandling av vissa sorters information”.

Med det sagt, har ett antal säkerhetsåtgärder angetts såväl i själva dataskyddsförordningen som i praxis och i vägledningar från såväl Europeiska dataskyddstyrelsen[169] som Datainspektionen.[170] Dessa vägledningar är förvisso inte rättsligt bindande, men ger en indikation på hur informationssäkerhet kring dataskydd ska tillämpas. Krav på säkerhet kan också framgå av praxis från tillsynsmyndigheterna och domstolar. Som ett exempel kan nämnas att Datainspektionen har under en lång tid krävt stark autentisering vid överföring av känsliga personuppgifter via öppna nät.

4.4.2 INFORMATIONSKLASSIFICERING

I dataskyddsförordningen och av praxis framgår också ett antal olika typer av personuppgifter, vilket bildar en sorts informationsklassificering:

- **Ordinära personuppgifter**: personuppgifter som varken är integritetskänsliga eller känsliga personuppgifter.[171]

---

167 Artikel 32 dataskyddsförordningen.

168 Se artikel 32 dataskyddsförordningen.

169 Se Europeiska dataskyddsstyrelsen, Om EDPB, https://edpb.europa.eu/about-edpb/about-edpb_sv. Läst den 30 januari 2020.

170 Datainspektionens allmänna råd är inte bindande, utan utgör rekommendationer om hur kraven i dataskyddslagstiftningen kan uppnås. För mer information om säkerhetsåtgärder vid personuppgiftsbehandling, se bl.a. Datainspektionens allmänna råd för säkerhet för personuppgifter. Notera dock att de allmänna råden är från november 2008 och innehåller rekommendationer om tillämpningen av bestämmelser i den nu upphävda personuppgiftslagen. De är därför inte längre gällande, men kan fortfarande ge vägledning till den som ska tillämpa dataskyddsförordningen. De allmänna råden går att hitta här: https://www.datainspektionen.se/globalassets/dokument/ovrigt/faktabroschyr-allmannarad-sakerhet.pdf.

171 Som huvudregel betraktas exempelvis namn och telefonnummer inte som integritetskänsliga eller känsliga personuppgifter.

- **Integritetskänsliga personuppgifter**: uppgifter som Datainspektionen har bedömt varit särskilt skyddsvärda men som inte klassificeras som känsliga personuppgifter i dataskyddsförordningen.[172] I denna kategori ingår även uppgifter som rör lagöverträdelser, som regleras särskilt i dataskyddslagen.[173]

- **Känsliga personuppgifter**: Särskilda kategorier av personuppgifter enligt dataskyddsförordningen.[174]

- **Personnummer/samordningsnummer**: Alla medlemsstater har inte personnummer eller liknande system, varför dessa inte är reglerade i dataskyddsförordningen. Svenska personnummer och samordningsnummer är dock särskilt reglerade i dataskyddslagen.[175]

Det som styr valet av lämpliga skyddsåtgärder är dock inte denna informationsklassificering, utan snarare känslighet eller risk med hela behandlingen, där personuppgifternas typ är en av flera faktorer.

Vad gäller behandlingens känslighet eller risk finns det i lagstiftningen en tydlig gräns mellan ”ordinär” personuppgiftsbehandling och sådan personuppgiftsbehandling som sannolikt leder till en hög risk för den registrerade. För den senare kategorin krävs, som vi redogjort för i avsnitt 4.3.3 ovan, att en konsekvensbedömning genomförs. Detta styr inte heller vilka konkreta skyddsåtgärder som ska vidtas, men ställer mer detaljerade krav på processen för att ta fram dessa skyddsåtgärder.

4.4.3 MINIMIÅTGÄRDER

Mot bakgrund av det ovan sagda, är nedan en översiktlig förteckning över konkreta skyddsåtgärder som bör övervägas inför att en personuppgiftsbehandling inleds. Vissa åtgärder kommer i princip alltid att kunna vidtas (exempelvis kryptering vid överföring), medan andra bara är relevanta i särskilda sammanhang (exempelvis pseudonymisering). Vi har även försökt ange under vilka förutsättningar vissa åtgärder måste vidtas.

---

172 Datainspektionen anger icke-uttömmande att integritetskänsliga uppgifter kan vara exempelvis personnummer, löneuppgifter, uppgifter om lagöverträdelser, värderande uppgifter (t.ex. uppgifter från utvecklingssamtal, uppgifter om resultat från personlighetstester eller personlighetsprofiler), information som rör någons privata sfär, uppgifter om sociala förhållanden.

173 Se 3 kap. 8-9 §§ dataskyddslagen.

174 Se artikel 9 dataskyddsförordningen, där det framgår att särskilda kategorier av uppgifter är uppgifter om: etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i en fackförening, hälsa, en persons sexualliv eller sexuella läggning, genetiska uppgifter och biometriska uppgifter som används för att entydigt identifiera en person. I svensk tradition kallas dessa för ”känsliga personuppgifter”, vilket i viss mån har påverkat terminologin även inom EU.

175 Se 3 kap. 10-11 §§ dataskyddslagen.

	KÄLLA/LAGRUM	ÅTGÄRDER ATT ÖVERVÄGA	MÅSTE GENOMFÖRAS?
1.	Datainspektionens allmänna råd, s. 12	Fastställd skriftlig säkerhetspolicy som innehåller bl.a. organisationens säkerhetsstrategi, ansvarsfördelning och övergripande mål för säkerheten	
2.	Datainspektionens allmänna råd, s. 12	Rutiner för rapportering och uppföljning av säkerhetsincidenter	
3.	Datainspektionens allmänna råd, s. 13	Arbetsrutiner för personal att arbeta och tänka säkerhetsmedvetet	
4.	Artikel 32 samt skäl 76 dataskyddsförordningen	Identifiera hotbilden och genomför en riskanalys	
5.	Artikel 35 dataskyddsförordningen	Genomför konsekvensbedömning och förhandssamråd med Datainspektionen	Om sannolikt leder till hög risk
6.	Artikel 36 dataskyddsförordningen	Genomför förhandssamråd med Datainspektionen	Om kvarvarande hög risk efter konsekvensbedömning och vidtagna åtgärder
7.	Datainspektionens allmänna råd, s. 20	Åtgärder för fysisk säkerhet som lås, inpasseringskontroll, larm, säkerhetsskåp m.m.	
8.	Datainspektionens allmänna råd, s. 22	Personliga inloggningsuppgifter	
9.	Artikel 32.1 a) dataskyddsförordningen	Kryptering vid lagring av information	
10.	Artikel 32.1 a) dataskyddsförordningen	Kryptering vid överföring av information	Om känsliga personuppgifter
11.	Artikel 32.1 a) dataskyddsförordningen	Pseudonymisering	
12.	Datainspektionens allmänna råd, s. 22	Behandlingshistorik/loggning	
13.	Datainspektionens allmänna råd, s. 24	Säkerhetskopiering	
14.	Datainspektionens allmänna råd, s. 25	Skydd mot skadliga program, t ex virus	
15.	Artikel 28.3 dataskyddsförordningen	Teckna personuppgiftsbiträdesavtal med personuppgiftsbiträden	Om personuppgiftsbiträde används
16.	Artikel 26 dataskyddsförordningen	Ingå datadelningsavtal med gemensamt personuppgiftsansvariga	Om personuppgiftsansvaret är gemensamt med annan part
17.	Datainspektionens allmänna råd, s. 26	Verifiering av informationssäkerheten	

	KÄLLA/LAGRUM	ÅTGÄRDER ATT ÖVERVÄGA	MÅSTE GENOMFÖRAS?
18.	Artikel 30 data-skyddsförordningen	Register över samtliga behandlingar	Ja
19.	Artiklarna 5.1 f), 25.2 samt 32.1 b) data-skyddsförordningen	Behörighetshantering	
20.	Artikel 5.1 c) data-skyddsförordningen	Uppgiftsminimering	Ja
21.	Artikel 5.1 e) data-skyddsförordningen	Lagringsminimering	Ja
22.	Artikel 13-14 data-skyddsförordningen	Information till registrerade om personuppgiftsbehandlingen	Ja
23.	Artikel 25 data-skyddsförordningen	Privacy by design and default	Ja
24.	Artikel 7 dataskydds-förordningen	Loggning av samtycken/återkallade samtycken	Om samtycke är rättslig grund för behandlingen
25.	Artikel 21.1 data-skyddsförordningen	Loggning av personer som motsatt sig behandling med stöd av intresse-avvägning som laglig grund	Om intresseavvägning är rättslig grund för behandlingen
26.	Artikel 45 data-skyddsförordningen	Säkerställande av adekvat skyddsnivå vid överföring av personuppgifter utanför EU/EES	Om uppgifter överförs utanför EU/EES

4.5 Särskilda krav vid utkontraktering

Det är vanligt att en personuppgiftsansvarig anlitar ett personuppgiftsbiträde som i sin tur kanske anlitar ett annat personuppgiftsbiträde, ett s.k. underbiträde[176].[177] Artikel 28 i dataskyddsförordningen anger särskilda villkor som måste vara uppfyllda för att ett sådant anlitande ska vara tillåtet. Enligt vår mening, till skillnad från exempelvis säkerhetsskyddslagen och NIS-lagen (se avsnitten 2 och 3 ovan), utgör dataskyddsförordningens krav vid utkontraktering (personuppgiftsbiträden) en typ av säkerhetsåtgärd. Detta följer av det faktum att kraven som ställs på såväl den personuppgiftsansvarige som personuppgiftsbiträdet och eventuella underbiträden, direkt syftar till att skydda den registrerades personuppgifter (inbegripet den registrerades rättigheter och friheter).

176 Begreppet ”underbiträde” förekommer inte i dataskyddsförordningen. I pedagogiskt syfte har vi dock valt att kalla det personuppgiftsbiträde som ett personuppgiftsbiträde i sin tur anlitar för underbiträde.

177 *Nota bene!* Andra bolag inom personuppgiftsbiträdets koncern är antingen att betrakta som flera biträden (där den personuppgiftsansvarige behöver ingå personuppgiftsbiträdesavtal med samtliga, detta kan lämpligen ske genom att personuppgiftsbiträdet som tecknar avtalet med den personuppgiftsansvarige har fått fullmakt från koncernbolagen att ingå avtalet även för deras räkning) eller personuppgiftsbiträdets underbiträden.

För det första måste den personuppgiftsansvarige försäkra sig om att personuppgiftsbiträdet ger tillräckliga garantier om att genomföra lämpliga tekniska och organisatoriska åtgärder på ett sådant sätt att behandlingen som biträdet ska utföra uppfyller kraven i dataskyddsförordningen och säkerställer att den registrerades rättigheter skyddas.[178]

Om ett personuppgiftsbiträde anlitas måste den personuppgiftsansvarige, enligt artikel 28.3, ingå ett s.k. personuppgiftsbiträdesavtal med biträdet. Avtalet ska innehålla följande information och instruktioner:

- Att personuppgiftsbiträdet endast får behandla personuppgifter på dokumenterade instruktioner, inbegripet även när det gäller överföringar av personuppgifter till ett tredjeland eller en internationell organisation;

- Att personer som är behöriga att behandla personuppgifterna omfattas av ett sekretessåtagande eller lämplig lagstadgad tystnadsplikt;

- Att personuppgiftsbiträdet är skyldigt att vidta alla säkerhetsåtgärder som krävs enligt artikel 32;

- Att personuppgiftsbiträdet, beroende på vad den personuppgiftsansvarige bestämmer, inte får anlita ett underbiträde utan antingen ett särskilt eller allmänt skriftligt förhandstillstånd från den personuppgiftsansvarige;

- Att personuppgiftsbiträdet är skyldigt att i sin tur ingå ett personuppgiftsbiträdesavtal med eventuella underbiträden som ålägger underbiträdena samma skyldigheter i fråga om dataskydd som de som fastställs i personuppgiftsbiträdesavtalet;

- Att personuppgiftsbiträdet är fullt ansvarig gentemot personuppgiftsansvarige för utförandet av underbiträdets skyldigheter;

- Att personuppgiftsbiträdet, med hänsyn till behandlingens art, ska hjälpa den personuppgiftsansvarige genom lämpliga tekniska och organisatoriska åtgärder, i den mån detta är möjligt, så att den personuppgiftsansvarige kan fullgöra sin skyldighet att svara på begäran om utövande av den registrerades rättigheter;

- Att biträdet ska bistå den personuppgiftsansvarige med att se till att skyldigheterna enligt artiklarna 32–36 fullgörs, med beaktande av typen av behandling och den information som personuppgiftsbiträdet har att tillgå;

- Att, beroende på vad den personuppgiftsansvarige väljer, personuppgiftsbiträdet ska radera eller återlämna alla personuppgifter

178 Artikel 28.1 dataskyddsförordningen. Notera att detsamma gäller personuppgiftsbiträdet, för det fall personuppgiftsbiträdet i sin tur anlitar ett annat personuppgiftsbiträde. Därtill, för att underbiträdet ska få behandla personuppgifter, måste personuppgiftsbiträdet ha fått tillstånd från den berörde personuppgiftsansvarige att underbiträdet får behandla uppgifterna ifråga, se artikel 28.2 dataskyddsförordningen.

till den personuppgiftsansvarige efter det att tillhandahållandet av behandlingstjänster har avslutats, och radera befintliga kopior såvida inte lagring av personuppgifterna (med undantag för om det finns någon tvingande lagbestämmelse som personuppgiftsbiträdet omfattas av som kräver fortsatt behandling);

- Att personuppgiftsbiträdet ska ge den personuppgiftsansvarige tillgång till all information som krävs för att visa att de skyldigheter som anges i artikel 28 uppfylls samt möjliggöra och bidra till granskningar, inbegripet inspektioner, som genomförs av den personuppgiftsansvarige eller av en annan revisor som bemyndigats av den personuppgiftsansvarige; och

- Att personuppgiftsbiträdet är skyldigt att omedelbart informera personuppgiftsansvarig om biträdet anser att en instruktion strider mot tillämplig dataskyddslagstiftning.

Därutöver bör det anges, vanligtvis i en s.k. specifikation som biläggs personuppgiftsbiträdesavtalet, en beskrivning av behandlingen där uppgift om föremålet för behandlingen, behandlingens varaktighet, art och ändamål, typen av personuppgifter och kategorier av registrerade framgår.

Instruktion om eventuella tredjelandsöverföringar, avseende både personuppgiftsbiträdet och dess eventuella underbiträden, bör även anges i personuppgiftsbiträdesavtalet; huruvida de är tillåtna, under vilka förutsättningar, vilka skyddsåtgärder enligt artikel 46 dataskyddsförordningen som ska vidtas.

Vidare anser vi att det är lämpligt att ange, antingen i en egen bilaga eller i specifikationen och utan att begränsa personuppgiftsbiträdets självständiga ansvar att säkerställa en lämplig säkerhetsnivå enligt artikel 32 dataskyddsförordningen, vilka säkerhetsåtgärder som personuppgiftsbiträdet kommer att vidta. Detta för att personuppgiftsansvarig bl.a. ska kunna uppfylla sin skyldighet att försäkra sig om att personuppgiftsbiträdet kommer att behandla personuppgifter i enlighet med artikel 28.1.

Avslutningsvis bör något sägas om skillnaden mellan personuppgiftsbiträden och s.k. medhjälpare.[179] Medan ett personuppgiftsbiträde i princip alltid är en juridisk person (med undantag för enskilda näringsidkare) och alltid finns utanför den personuppgiftsansvariges organisation, är en medhjälpare någon som arbetar under den personuppgiftsansvariges överinseende och ledning, exempelvis anställda.

179 Artikel 29 dataskyddsförordningen.

4.6 Gränssnitt mot myndigheter

4.6.1 MYNDIGHETERS TILLSYN

Varje EU-medlemsstat ska utse en tillsynsmyndighet som ska övervaka tillämpningen av dataskyddsförordningen inom respektive medlemsstats territorium.[180] För svenskt vidkommande har denna tillsynsuppgift ålagts Datainspektionen.[181]

Det är inte ovanligt att en viss personuppgiftsbehandling berör personer från flera olika medlemsstater eller att den personuppgiftsansvarige är verksam i flera länder. För att undvika att flera nationella tillsynsmyndigheter genomför parallell tillsyn har dataskyddsförordningen bestämmelser om ansvarig tillsynsmyndighet vid gränsöverskridande behandling och hur olika tillsynsmyndigheter ska förhålla sig till varandra. Detta kan t.ex. röra utredningsinsatser eller informationsutbyte.[182]

4.6.2 INCIDENTRAPPORTERING

Den enda situation då en personuppgiftsincident inte behöver anmälas till en tillsynsmyndighet är när det är osannolikt att incidenten medför en risk för fysiska personers rättigheter och friheter.[183] Det är särskilt viktigt att notera att sannolikhetsbedömningen tar sikte på huruvida det uppstått en risk, inte huruvida incidenten faktiskt fått någon skadlig effekt.

Vid en personuppgiftsincident ska den personuppgiftsansvarige, efter att ha fått kännedom om incidenten, anmäla incidenten till behörig tillsynsmyndighet utan onödigt dröjsmål. Detta ska ske inom 72 timmar, men om det inte är möjligt ska en sådan fördröjning motiveras.[184] Den personuppgiftsansvarige kan dock inte vara passiv när det finns tecken på att en incident kan ha inträffat, utan måste vidta alla lämpliga tekniska och skyddsåtgärder och organisatoriska åtgärder för att omedelbart fastställa om en personuppgiftsincident ägt rum.[185]

Anmälningsskyldigheten börjar alltså löpa när den ansvarige fått vetskap om incidenten, inte när incidenten utretts. Om det inte är möjligt att tillhandahålla all information samtidigt, får informationen dock lämnas i omgångar, t.ex. allteftersom utredningen fortskrider.[186] Många gånger behöver den personuppgiftsansvarige göra flera

180 Artikel 51 dataskyddsförordningen.

181 3 § förordningen (2018:219) med kompletterande bestämmelser till EU:s dataskyddsförordning.

182 Artiklarna 60 och 61 dataskyddsförordningen.

183 Artikel 33.1 dataskyddsförordningen.

184 Artikel 33.1 dataskyddsförordningen.

185 Artikel 29-gruppens *Riktlinjer om anmälan av personuppgiftsincidenter*, beslutade den 3 oktober 2017, senast reviderade den 6 februari 2018, s. 11.

186 Artikel 33.4 dataskyddsförordningen.

undersökningar och följa upp undersökningarna i ett senare skede. Detta är tillåtet, men förutsätter att den personuppgiftsansvarige anger skälen till förseningen.[187]

Anmälan om personuppgiftsincident ska innehålla (i) en beskrivning av incidentens art, de kategorier av registrerade som berörs och hur många som berörs, (ii) kontaktuppgifter till dataskyddsombudet, (iii) en beskrivning av de sannolika konsekvenserna av incidenten, och (iv) en beskrivning av vidtagna och föreslagna åtgärder med anledning av incidenten.[188] Datainspektionen har tagit fram närmre vägledning för anmälan av personuppgiftsincidenter, bl.a. anvisat ett särskilt formulär för anmälan.[189]

Ifall incidenten sannolikt leder till hög risk för fysiska personers rättigheter och friheter, föreligger även en skyldighet för den personuppgiftsansvarige att informera de registrerade om incidenten.[190] Denna skyldighet är dock inte absolut, utan försedd med vissa undantag, däribland:

- Om personuppgifterna är oläsbara för obehöriga, t.ex. genom kryptering;

- Om den personuppgiftsansvarige vidtagit åtgärder i relation till den som fick tillgång till personuppgifterna; eller

- Om det skulle innebära en oproportionerlig ansträngning att kontakta de enskilda, t.ex. när kontaktuppgifterna gått förlorade p.g.a. incidenten.[191]

4.6.3 SAMRÅD

Inför riskfyllda behandlingar föreligger en samrådsskyldighet med tillsynsmyndigheten, om det efter en genomförd konsekvensbedömning kvarstår höga risker för de registrerades friheter och rättigheter.[192] Samrådsskyldigheten innebär att den personuppgiftsansvarige ska lämna följande information till tillsynsmyndigheten:

- I tillämpliga fall, de respektive ansvarsområdena för de personuppgiftsansvariga, gemensamt personuppgiftsansvariga och personuppgiftsbiträden som medverkar vid behandlingen, framför allt vid behandling inom en koncern;

---

187 Artikel 29-gruppens *Riktlinjer om anmälan av personuppgiftsincidenter*, s. 16.

188 Artikel 33.3 dataskyddsförordningen.

189 Datainspektionen, Blankett för Anmälan av personuppgift, v. 1.5 av den 3 januari 2019, https://www.datainspektionen.se/globalassets/dokument/blankett-2-anmalan-av-personuppgiftsincident--sv.pdf. Läst den 24 februari 2020.

190 Artikel 34.1 dataskyddsförordningen.

191 Artikel 34.3 dataskyddsförordningen. Se även Artikel 29-gruppens *Riktlinjer om anmälan av personuppgiftsincidenter*, s. 23.

192 Artikel 36 dataskyddsförordningen.

- Ändamålen med och medlen för den avsedda behandlingen;
- De åtgärder som vidtas och de garantier som lämnas för att skydda de registrerades rättigheter och friheter enligt denna förordning;
- I tillämpliga fall, kontaktuppgifter till dataskyddsombudet;
- Konsekvensbedömningen; och
- All annan information som begärs av tillsynsmyndigheten.

Om tillsynsmyndigheten anser att den planerade behandlingen skulle strida mot dataskyddsförordningen, särskilt om den personuppgiftsansvarige bedöms att inte i tillräcklig mån ha fastställt eller reducerat risken, ska tillsynsmyndigheten inom åtta veckor från det att begäran om samråd mottagits, återkoppla skriftligen med råd till den personuppgiftsansvarige och i tillämpliga fall personuppgiftsbiträdet.[193] Om den planerade behandlingen är särskilt komplicerad, kan åttaveckorsperioden komma att förlängas med upp till sex veckor.

4.6.4 SANKTIONER

Datainspektionen har ett antal olika sanktioner att tillgå, däribland att utfärda varningar och att förelägga den personuppgiftsansvarige att vidta vissa åtgärder.[194] Den sanktion som rent ekonomiskt är den mest kännbara är dock möjligheten att besluta om administrativ sanktionsavgift när myndigheten konstaterar överträdelser av dataskyddsförordningen eller kompletterande lagstiftning. Bristande säkerhetsåtgärder och avsaknaden av inbyggt dataskydd och dataskydd som standard kan således medföra sanktionsavgift, både för den personuppgiftsansvarige och för personuppgiftsbiträden.

Storleken på sanktionsavgifter för överträdelser av dataskyddsförordningen beror på vilken bestämmelse som har överträtts, och delas därför upp i två olika nivåer.

Den första nivån av överträdelser (eller snarare bestämmelser) kan ge upp till 10 miljoner euro i sanktionsavgift eller, om det gäller företag, upp till 2 % av den totala globala omsättningen (beroende på vilket värde som är högst).[195]

Avseende de mer allvarliga överträdelserna kan sanktionsavgiften uppgå till 20 miljoner euro eller, om det gäller ett företag, 4 % av den

193 Notera att tillsynsmyndigheten även får utnyttja alla de befogenheter som den har enligt artikel 58, såsom att begära in information, utöva tillsyn, meddela korrigerande åtgärder m.m.

194 Artikel 58 dataskyddsförordningen.

195 Artikel 83.4 dataskyddsförordningen. Denna nivå består av (i) personuppgiftsansvarigas och personuppgiftsbiträdens skyldigheter enligt artiklarna 8, 11, 25–39, 42 och 43, (ii) certifieringsorganets skyldigheter enligt artiklarna 42-43, och (iii) övervakningsorganets skyldigheter enligt artikel 41.4.

totala globala årsomsättningen (beroende på vilket värde som är högst).[196]

För överträdelser av artiklarna 25 och 32 dataskyddsförordningen gäller den lägre nivån av avgifter. Observera dock att allvarliga överträdelser kan anses strida mot principen om integritet och konfidentialitet i artikel 5.1 f och medföra sanktionsavgift enligt den högre nivån.

Utöver dessa sanktionsavgifter kan det även bli aktuellt att betala skadestånd till varje person som lidit skada till följd av överträdelse av dataskyddsförordning.[197]

196 Artikel 83.5 dataskyddsförordningen. Denna nivå består av (i) de grundläggande principerna för behandling, inklusive villkoren för samtycke, enligt artiklarna 5, 6, 7 och 9, (ii) registrerades rättigheter enligt artiklarna 12–22, (iii) överföring av personuppgifter till en mottagare i ett tredjeland eller en internationell organisation enligt artiklarna 44–49, (iv) alla skyldigheter som följer av medlemsstaternas lagstiftning som antagits på grundval av kapitel IX, och (v) underlåtenhet att rätta sig efter ett föreläggande eller en tillfällig eller permanent begränsning av behandling av uppgifter eller ett beslut om att avbryta uppgiftsflödena som meddelats av tillsynsmyndigheten i enlighet med artikel 58.2 eller underlåtelse att ge tillgång till uppgifter i strid med artikel 58.1.

197 Artikel 82 dataskyddsförordningen.

5. Informationssäkerhet enligt områdesspecifik lagstiftning

5.1 Allmänt

Utöver den lagstiftning som redogjorts för i tidigare avsnitt finns ytterligare bestämmelser som rör informationssäkerhet inom olika verksamheter. Dessa bestämmelser träffar främst verksamheter inom specifika områden och ger ofta detaljerade anvisningar om hur informationssäkerhetsarbetet ska ske. I detta kapitel har vi gjort ett urval av sådan lagstiftning, vilket innebär att det även kan finnas annan lagstiftning om informationssäkerhet som inte behandlas i rapporten. Vi har i denna rapport valt att redogöra för lagstiftning som träffar följande aktörer, branscher, tekniska funktioner och skyddsområden:

- Statliga myndigheter
- Hälso- och sjukvård
- Tillhandahållare av elektroniska kommunikationstjänster
- Banker
- Identitetstjänster
- Bokföringsskyldiga personer
- Cybersäkerhetscertifiering
- Offentlighet och sekretess

Bestämmelserna återfinns till stor del i myndighetsföreskrifter och allmänna råd. Föreskrifterna är, likt lagar och förordningar, bindande, medan allmänna råd inte är juridiskt bindande, även om de kan ge värdefull vägledning. Varje avsnitt nedan redogör för bestämmelserna inom en viss verksamhet/sektor/område, låt vara att vi gjort ett urval bland de relevanta rättsakterna. Till följd av att den områdesspecifika regleringen i vissa delar varierar, kan även redogörelserna i de olika avsnitten variera i omfattning och utformning.

5.2 Statliga myndigheter

TILLSYN OCH TILLÄMPLIGA FÖRFATTNINGAR

Samordnande myndighet	Myndigheten för samhälls-skydd och beredskap (MSB)
Förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap (krisberedskaps-förordningen)	Syftar till att statliga myndigheter ska minska sårbarheten i samhället och utveckla sin förmåga att hantera sina uppgifter under fredstida kris-situationer och inför och vid höjd beredskap.
MSB:s föreskrifter och allmänna råd om statliga myndigheters informationssäkerhet, MSBFS 2016:1	Ställer krav på en god säkerhetskultur, vilket bl.a. innefattar: • ledningssystem för informations-säkerhet • informationssäkerhetspolicy • genomförandet av riskanalyser • rutiner för incident- och kontinuitetshantering • åtgärder i samband med utkontrak-tering av informationshantering
MSB:s föreskrifter och allmänna råd om statliga myndigheters rapporte-ring av it-incidenter, MSBFS 2016:2	Ställer krav på statliga myndigheters rapportering av it-incidenter och krav på överlåtelseavtalet vid utkontrak-tering av informationshantering.

5.2.1 MYNDIGHETEN FÖR SAMHÄLLSSKYDD OCH BEREDSKAP

MSB är en statlig myndighet som ansvarar för att stödja samhällets beredskap för olyckor, kriser och civilt försvar. MSB meddelar därför, med stöd från olika förordningar, föreskrifter om hur myndigheter ska hantera olika typer av krissituationer.

Förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap (nedan ”**krisberedskapsför-ordningen**”) syftar till att statliga myndigheter genom sin verksam-het ska minska sårbarheten i samhället samt utveckla sin förmåga att hantera sina uppgifter såväl i fredstid som under krissituationer, och inför och vid höjd beredskap. Genom krisberedskapsförordning-en bemyndigas MSB att meddela ytterligare föreskrifter som behövs bland annat för säkerställandet av en säker informationshantering.[198]

MSB har därtill beslutat två föreskrifter, om statliga myndigheters

198 21 § krisberedskapsförordningen.

informationssäkerhet (MSBFS 2016:1) och om statliga myndigheters rapportering av it-incidenter (MSBFS 2016:2).

5.2.2 STATLIGA MYNDIGHETERS ARBETE MED INFORMATIONSSÄKERHET

MSB:s föreskrifter om statliga myndigheters informationssäkerhet ansluter till bestämmelserna i 19 § krisberedskapsförordningen, som anger att varje myndighet ansvarar för att dess informationshanteringssystem uppfyller sådana säkerhetskrav att verksamheten kan utföras på ett tillfredställande sätt. Föreskrifterna gäller som komplement till övriga bestämmelser om statliga myndigheters informationssäkerhet, och ska bara tillämpas i den mån de inte avviker från övriga bestämmelser.

Varje myndighet ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete med stöd av ett ledningssystem, vilket enligt föreskrifterna definieras som ett sätt att styra arbetet med informationssäkerhet i syfte att planera, genomföra, kontrollera, följa upp, utvärdera och förbättra säkerheten i verksamhetens informationshantering.[199] Detta kan jämföras med det likalydande kravet på leverantörer av samhällsviktiga tjänster som ställs i 11 § NIS-lagen (se vidare avsnitt 3.3.1) MSB:s föreskrifter är dock mer detaljerade i exakt hur detta ska gå till. Som en del av inrättandet av ett ledningssystem ska myndigheten särskilt vidta följande åtgärder:

- Myndigheten ska upprätta en *informationssäkerhetspolicy* där bl.a. ansvarsfördelningen för verksamhetens informationsmängder ska framgå.[200]

- Myndigheten ska eftersträva att alla i organisationen har kunskap om och förståelse för behoven av säker informationshantering genom att informera medarbetare om kraven som ställs, t.ex. genom utbildningar rörande informationssäkerhet.[201]

- Myndigheten ska pröva sin kontinuitetshantering genom att genomföra övningar som testar och utvecklar säkerhetsåtgärderna.[202]

- Myndigheten ska göra riskanalyser i syfte att hantera hot och risker som rör informationssäkerheten. Riskanalysen ska ske med stöd av en modell som:

  - Klassar informationen med utgångspunkt i konfidentialitet, riktighet och tillgänglighet i olika nivåer utifrån de konsekvenser som kan uppstå vid bristande skydd.

199 5 § MSBFS 2016:1.

200 7 § MSBFS 2016:1.

201 8 § MSBFS 2016:1.

202 8 § MSBFS 2016:1.

- Identifierar, analyserar och bedömer eventuella hot och risker för verksamhetens information, system och tjänster.

- Identifierar åtgärder som krävs för att säkerställa skyddet.

- Följer upp och utvärderar vidtagna åtgärder och gjorda bedömningar av hot och risker.

- Kontinuerligt utvecklar skyddet för att upprätthålla säkerheten över tid.

- Löpande dokumenterar vidtagna åtgärder enligt ovan.[203]

- Myndigheten ska vidare ha rutiner för att identifiera, rapportera, bedöma, hantera och dokumentera incidenter som kan påverka säkerheten i myndighetens informationshantering. Rutiner ska finnas på plats för att lära av sådana eventuella inträffade incidenter samt av de åtgärder som då vidtogs.[204] Myndigheten ska vidare ha rutiner för kontinuitetshantering där det ska tydliggöras hur informationshanteringen upprätthålls vid betydande störningar och avbrott.[205]

5.2.3 UTKONTRAKTERING

Ansvaret för säker informationshantering gäller även när information som en myndighet innehar hanteras av en extern aktör. I det fall en myndighet anlitar en annan myndighet för att fullgöra uppgifter som regleras av föreskrifterna ska det på ett tydligt sätt dokumenteras hur samarbetet ser ut samt vilken myndighet som är ansvarig för att uppfylla de krav som ställs.[206] Informationsklassningen ska dock alltid utföras av den myndighet som äger informationen.[207]

I de fall en myndighet överlåter sin informationshantering till en icke statlig aktör ska myndigheten i överlåtelseavtalet säkerställa att motparten åtar sig att uppfylla samma krav på incidentrapportering som ställs på myndigheten.[208]

5.2.4 RAPPORTERING AV IT-INCIDENTER

Statliga myndigheter ska rapportera it-incidenter till MSB ifall incidenten allvarligt kan påverka säkerheten i den informationshantering myndigheten ansvarar för.[209] För att skapa en systematisk och samlad rapportering av sådana allvarliga it-incidenter, och för att på så sätt

203 9 § MSBFS 2016:1.

204 10 § MSBFS 2016:1.

205 11 § MSBFS 2016:1.

206 3 § MSBFS 2016:1.

207 3 § MSBFS 2016:1.

208 9 § MSBFS 2016:2.

209 20 § krisberedskapsförordningen.

bidra till att öka samhällets informationssäkerhet, har MSB meddelat ytterligare föreskrifter om hur rapporteringen ska gå till.[210]

Rapporteringspliktiga it-incidenter kan exempelvis vara störningar i mjuk- eller hårdvara, driftstörningar, informationsförlust, informationsförvanskning eller hindrad tillgång till information.[211]

Rapporteringen ska lämnas till MSB senast 24 timmar efter det att myndigheten upptäckt it-incidenten.[212] Rapporten ska innehålla information om:

- Vilken myndighet det gäller;
- Hur it-incidenten gått till, inklusive en redovisning av händelseförlopp och vidtagna åtgärder;
- När it-incidenten inträffade;
- När myndigheten upptäckte it-incidenten;
- Vilken kategori av incidenter som it-incidenten tillhör; samt
- Myndighetens initiala bedömning av både it-incidentens omfattning och vilka potentiella konsekvenser som kan uppstå som följd.[213]

I de fall en fullständig rapport inte kan lämnas i tid får myndigheten i samråd med MSB lämna en preliminär rapport.[214] En sådan överenskommelse ska ske inom tidsfristen på 24 timmar. Den preliminära rapporten ska innehålla den information som finns att tillgå vid rapporteringstillfället, samt (i) när myndigheten upptäckte it-incidenten, (ii) huruvida den fortfarande pågår, och (iii) vilken kategori av incident som orsakat it-incidenten.[215]

5.2.5 KOMMANDE (EVENTUELLA) ÄNDRINGAR I REGLERINGEN

I skrivande stund finns ett förslag om ändring av krisberedskapsförordningen och de föreskrifter som MSB meddelat med stöd av denna.[216] I korthet föreslås att viss reglering som i dag finns i MSB:s föreskrifter förs över till krisberedskapsförordningen. Det kommer därigenom redan av krisberedskapsförordningen framgå att varje myndighet ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete med stöd av ett ledningssystem för informationssäkerhet.

---

210 MSBFS 2016:2 föreskrifter och allmänna råd om statliga myndigheters rapportering av it-incidenter.

211 Se 3 § MSBFS 2016:2.

212 4 § MSBFS 2016:2.

213 6 § MSBFS 2016:2.

214 8 § MSBFS 2016:2.

215 8 § MSBFS 2016:2.

216 Ändring i krisberedskapsförordningen, Ju2019/03194/L4.

5.3 Hälso- och sjukvård

TILLSYN OCH TILLÄMPLIGA FÖRFATTNINGAR

Tillsynsmyndighet	Datainspektionen (i fråga om dataskydd) IVO (i fråga om patientsäkerhet) Läkemedelsverket (i fråga om föreskrifter om it-system som medicinsk-teknisk produkt)
Patientdatalagen (2008:355)	Tillämpas på vårdgivare som behandlar personuppgifter. Syftar till att skydda patienters integritet, t.ex. genom informationssäker journalföring och krav på konfidentialitet.
Patientdataförordningen (2008:360)	Bemyndigar Socialstyrelsen och Datainspektionen att meddela föreskrifter om behandling av uppgifter enligt PDL.
Gemensamma författningssamlingen avseende hälso- och sjukvård, socialtjänst, läkemedel, folkhälsa m.m., HSLF-FS 2016:40	Kompletterar patientdatalagen och ger detaljerade bestämmelser för hur vårdgivare ska behandla personuppgifter på ett informationssäkert sätt. Ställer bl.a. krav på: • Ledningssystem för informationssäkerhet • Informationssäkerhetspolicy • Genomförandet av riskanalyser • Informationssystem för personuppgiftsbehandling • Åtkomstkontroller • Skyddsåtgärder • Utkontraktering

5.3.1 KRAV PÅ VÅRDGIVARE SOM BEHANDLAR PERSONUPPGIFTER

Patientdatalagen (2008:355) (”**PDL**”) utgör ett komplement till dataskyddsförordningen och tillämpas vid vårdgivares behandling av personuppgifter inom hälso- och sjukvården. Vid en eventuell konflikt mellan PDL och dataskyddsförordningen har dock den senare företräde.[217] Lagen ska tillämpas av alla vårdgivare inom både offentlig och privat sektor. Syftet med lagen är att skydda patienters och övriga registrerades integritet. PDL innehåller därför bestämmelser om skyldigheten att föra patientjournal samt om hur journalerna ska hanteras på ett informationssäkert sätt.[218]

Datainspektionen utövar tillsyn över hur vårdgivare tillämpar data-

217 Se Datainspektionens vägledning om PDL: https://www.datainspektionen.se/lagar--regler/patientdatalagen/.

218 3 kap. PDL.

skyddsbestämmelserna i PDL, vilket omfattar en kontroll av huruvida vårdgivare vidtar tillräckliga säkerhetsåtgärder för att skydda patientuppgifter.[219]

5.3.1.1 Hantering av patientjournaler

I syfte att uppfylla kravet att ändringar av informationen i en journal ska kunna hänföras till en identifierbar person, dvs. ett krav på spårbarhet, ska det vid alla anteckningar i en patients journal framgå dels vem som gjort anteckningen, dels när anteckningen gjordes.[220]

Uppgifter i en journalhandling får inte heller utplånas eller göras oläsliga. Bestämmelsen syftar till att hålla informationen riktig och tillgänglig. Det är dock värt att notera att det finns ett undantag till bestämmelsen då Inspektionen för vård och omsorg kan besluta att journalen helt eller delvis ska förstöras.[221] För att uppfylla kravet att informationen ska hållas tillgänglig, ska journaler bevaras i minst tio år efter att den sista uppgiften infördes.[222] Om en journalhandling har lämnats ut ska det även dokumenteras vem som har fått ta del av den samt när detta skedde.[223]

5.3.1.2 Inre sekretess

PDL:s regler om inre sekretess är relevanta ur ett informationssäkerhetsperspektiv då de reglerar behörighet till uppgifter. Detta har direkt bäring på informationens konfidentialitet.

Reglerna är utformade utifrån principen om begränsad behörighet, med vilket avses att inte fler personer än de som verkligen behöver det ska få tillgång till vissa uppgifter. Tillgång till dokumenterade uppgifter om en patient ska därför endast ges till de som deltar i vården av patienten eller av annat skäl behöver uppgifterna för sitt arbete inom hälso- och sjukvården.[224] Vårdgivaren ska dokumentera vilka som får åtkomst till uppgifter om patienten och även systematiskt och återkommande kontrollera att ingen obehörig har åtkomst till sådana uppgifter.[225]

5.3.2 YTTERLIGARE KRAV PÅ ARBETET MED INFORMATIONSSÄKERHET

Patientdataförordningen (2008:360) bemyndigar Socialstyrelsen och Datainspektionen att meddela föreskrifter om behandling av personuppgifter enligt PDL. Socialstyrelsen har, efter samråd med Data-

219 Datainspektionens vägledning om PDL: https://www.datainspektionen.se/lagar--regler/patientdatalagen/.

220 3 kap. 6 § PDL.

221 8 kap. 4 § PDL.

222 3 kap. 17 § PDL.

223 3 kap. 11 § PDL.

224 4 kap. 1 § PDL.

225 4 kap. 3 § PDL.

inspektionen, kungjort föreskrifter och allmänna råd om journalföring och behandling av personuppgifter i hälso- och sjukvården. Dessa föreskrifter ingår i den gemensamma författningssamlingen avseende hälso- och sjukvård, socialtjänst, läkemedel, folkhälsa m.m. (HSLF-FS 2016:40).

Föreskrifterna utgör ett komplement till bestämmelserna i PDL och ska således tillämpas då vårdgivare behandlar patienters personuppgifter inom hälso- och sjukvården. [226]

I sammanhanget bör även kort nämnas Läkemedelsverkets tillsyn över patientsäkerhet och medicinsk teknik. I takt med digitaliseringen kan medicinsktekniska produkter, t.ex. en EKG-apparat, nu överföra data direkt till patientadministrativa system, vilket har lett till att gränserna mellan it och medicinteknik inte längre är lika tydliga.[227] I syfte att ge vägledning i frågan har Läkemedelsverket gett ut en skrift där det bl.a. lyfts att begreppet patientsäkerhet, när det används för medicinska informationssystem, inte bör skiljas från begreppet informationssäkerhet.[228] Patientsäkerheten ska snarare anses utgöra en del av informationssäkerheten, och bör därför beaktas inom organisationer som har system för hanteringen av sin informationssäkerhet. [229]

5.3.2.1 Ledningssystem

Enligt Socialstyrelsens föreskrifter och allmänna råd om ledningssystem för systematiskt kvalitetsarbete (2011:9) ansvarar varje vårdgivare för att det finns ett ledningssystem för verksamheten i syfte att systematiskt och fortlöpande utveckla och säkra verksamhetens kvalitet.

Enligt 3 kap. HSLF-FS 2016:40 ska ledningssystemet även säkerställa tillgänglighet, riktighet, konfidentialitet och spårbarhet för de personuppgifter som hanteras av vårdgivaren. Enligt de allmänna råd som hör till föreskriften bör en vårdgivare vid uppbyggnaden av ledningssystemet använda sig av svenska standarder för informationssäkerhet, exempelvis ISO/IEC 27000-serien.[230]

5.3.2.2 Informationssäkerhetsarbete

Vårdgivaren har ansvar för att ta fram en informationssäkerhetspolicy som anger övergripande mål för arbetet med informationssäkerheten i syfte att säkerställa personuppgifters tillgänglighet, riktighet, konfidentialitet och spårbarhet.[231] Vårdgivaren ska även utföra dokumen-

226 1 kap. 1 § HSLF-FS 2016:40.

227 Se Läkemedelsverkets vägledning om medicinska IT-system och programvaror.

228 Läkemedelsverket, *Medicinska informationssystem – vägledning för kvalificering och klassificering av programvaror med medicinskt syfte.*

229 Läkemedelsverket, *Medicinska informationssystem – vägledning för kvalificering och klassificering av programvaror med medicinskt syfte*, s. 31.

230 HSLF-FS 2016:40 *Allmänna råd* till 3 kap. 2 §.

231 3 kap. 4 § HSLF-FS 2016:40.

terade riskanalyser samt se till att informationssäkerhetsarbetet samordnas och leds av en eller flera personer.[232]

5.3.2.3 Informationssystem för behandling av personuppgifter

Vårdgivaren ska dokumentera de beslut som fattats om att ta i drift ett informationssystem för behandling av personuppgifter. Enligt Socialstyrelsens allmänna råd ska dokumentationen innehålla en beskrivning av systemets syfte och hur det ska användas, samt en validering av att systemet följer informationssäkerhetspolicyn som finns på plats.[233] För varje informationssystem som används för behandling av personuppgifter ska vårdgivaren även säkerställa att det finns uppdaterad och tillgänglig driftdokumentation. Vidare ska vårdgivaren vid utveckling, idrifttagande och ändring av informationssystemen säkerställa att uppgifternas tillgänglighet, riktighet, konfidentialitet samt spårbarhet inte riskeras. Vårdgivaren ska därutöver ha en plan för hur ett återställande av information ska ske vid en eventuell funktionsstörning av informationssystemet.[234]

Vad avser personuppgifter som behandlas i informationssystem ska dessa säkerhetskopieras regelbundet. Säkerhetskopiorna ska sedan förvaras på ett säkert sätt och vara väl åtskilda från originaluppgifterna.[235]

Informationssystemet ska även rent fysiskt skyddas mot skada, störning och obehörig åtkomst, vilket syftar uppfylla kraven på tillgänglighet och konfidentialitet.[236]

5.3.2.4 Åtkomst till uppgifter

Följande bestämmelser från Socialstyrelsens föreskrifter och allmänna råd om journalföring och behandling av personuppgifter i hälso- och sjukvården kompletterar de bestämmelser i PDL som rör behörighet för åtkomst till uppgifter om patienter.

I syfte att förhindra att obehöriga får tillgång till informationen ska varje användare tilldelas en individuell behörighet för åtkomst till personuppgifter. Vårdgivarens beslut om tilldelning av sådana behörigheter ska föregås av en behovs- och riskanalys. Vårdgivaren ska ta även ta fram rutiner för ändring och borttagning av dessa behörigheter samt regelbundet följa upp vilka behörigheter som tilldelats för att säkerställa att dessa är riktiga och aktuella.[237]

---

232 3 kap. 5-6 §§ HSLF-FS 2016:40.

233 HSLF-FS 2016:40 *Allmänna råd* till 3 kap. 7 §.

234 3 kap. 7-11 §§ HSLF-FS 2016:40.

235 3 kap. 12 § HSLF-FS 2016:40.

236 3 kap. 14 § HSLF-FS 2016:40.

237 4 kap. 2 § HSLF-FS 2016:40.

5.3.2.5 Kontroll av åtkomst till uppgifterna

All information som rör åtkomst till patientens uppgifter ska loggas, vilket ska omfatta information om vem som vidtagit vilken åtgärd och när. Bestämmelsen har direkt bäring på kravet på spårbarhet. Informationen om vem som tagit del av en patients uppgifter ska vårdgivaren på begäran lämna till patienten enligt 8 kap. 5 § PDL. Informationen ska vara utformad så att patienten själv kan bedöma huruvida åtkomsten var befogad eller inte. Därutöver ska en enskilds direktåtkomst till uppgifter om sig själv endast tillåtas i det fall dennes identitet har säkerställts genom stark autentisering.[238]

5.3.2.6 Konkreta krav på patientjournaler

I 5 kap. 1 § HSLF-FS 2016:40 ställs det krav på att informationen i en patientjournal ska finnas tillgänglig på ett överskådligt sätt för de som är behöriga att ta del av den.

Därtill ska vårdgivaren säkerställa att uppgifterna i en patientjournal är entydiga. För att försäkra sig om detta bör vårdgivaren, enligt Socialstyrelsens allmänna råd, använda sig av Socialstyrelsens termbank och andra tillämpliga publikationer.[239] Vårdgivaren måste även säkerställa att uppgifter i patientjournalen förvaras på ett sådant sätt att de är läsbara, och att uppgifter i en patientjournal inte kan ändras eller utplånas annat än med stöd av PDL.[240] För att säkerställa spårbarheten ska vårdgivaren även som säkerhetsåtgärd säkerställa att det finns rutiner för signering av de anteckningar som görs i journaler.[241]

5.3.2.7 Åtgärder till skydd mot obehörig åtkomst

I syfte att skydda informationen från åtkomst från obehöriga ska hälso- och sjukvårdspersonalen ansvara för att lösenord och de hjälpmedel som möjliggör autentisering inte blir tillgängliga för andra. Personalen ska även ansvara för att datorer och andra enheter där det kan finnas uppgifter om patienter är skyddade mot obehörig åtkomst (konfidentialitet).[242]

5.3.2.8 Övriga krav

Föreskrifterna innehåller därutöver följande krav på informationssäkerhet:[243]

---

238 4 kap. 11 § HSLF-FS 2016:40.

239 Se HSLF-FS 2016:40 *Allmänna råd* till 5 kap. 2 § för en uttömmande uppräkning.

240 6 kap. 6-7 §§ HSLF-FS 2016:40.

241 6 kap. 4 § HSLF-FS 2016:40.

242 6 kap 1 § HSLF-FS 2016:40.

243 3 kap. 15 och 18-20 §§ samt 6 kap. 9 § HSLF-FS 2016:40.

- I det fall vårdgivaren behandlar personuppgifter i öppna nät ska denne ansvara för att överföringen sker så att inte obehöriga kan ta del av dem samt att åtkomst föregås av stark autentisering.

- Vårdgivaren ansvarar för att årligen utvärdera skyddet mot intern och extern olovlig åtkomst till datornätverk och informationssystem.

- Om vårdgivaren tillåter ett flyttbart medium för lagring av personuppgifter ska denne säkerställa att uppgifterna inte går förlorade samt att obehöriga inte får tillgång till dem.

- När ett medium för informationslagring ska avvecklas ska det ske på ett sådant sätt att uppgifterna inte kan läsas eller återskapas.

- Om vårdgivaren anlitar hälso- och sjukvårdspersonal som får föra patientjournal på annat språk än svenska ska denne säkerställa att kravet på noggrannhet upprätthålls.

5.3.3 INCIDENTRAPPORTERING

De personer som leder och samordnar informationssäkerhetsarbetet ska minst en gång om året sammanställa information om arbetet till vårdgivaren. Sammanställningen ska bl.a. innehålla information om de incidenter som har påverkat informationssäkerheten och som medfört eller hade kunnat medföra vårdskada.[244]

244 3 kap. 6 § 2 st. 2 p. HSLF-FS 2016:40.

5.4 Elektronisk kommunikation

TILLSYN OCH TILLÄMPLIGA FÖRFATTNINGAR

Tillsynsmyndighet	Post- och telestyrelsen
Lagen (2003:389) om elektronisk kommunikation	Tillämplig på den som tillhandahåller en allmänt tillgänglig elektronisk kommunikationstjänst. Syftar till att ge enskilda och myndigheter tillgång till säkra och effektiva elektroniska kommunikationer, bland annat i fråga om informationssäkerhet. Ställer krav på att tekniska och organisatoriska åtgärder ska vidtas för en informationssäker kommunikation.
Post- och telestyrelsens föreskrifter om skyddsåtgärder för behandlade uppgifter, PTSFS 2014:1	Ger detaljerade bestämmelser om de tekniska och organisatoriska åtgärderna som ska vidtas enligt lagen (2003:389) om elektronisk kommunikation. Bestämmelserna ställer krav på bland annat: • Åtkomst och behörighetshantering • Loggning • Lagring av uppgifter • Kryptering • Integritetsincidenter
Förordningen (2003:396) om elektronisk kommunikation	Ställer krav på att Post- och telestyrelsen årligen ska lämna en sammanställning om rapporterade störningar eller avbrott av betydande omfattning till Europeiska kommissionen och den europeiska byrån för nät- och informationssäkerhet.
Post- och telestyrelsens föreskrifter om krav på driftsäkerhet, PTSFS 2015:2	Bestämmelser om tekniska och organisatoriska åtgärder för driftsäkerhet som den som tillhandahåller allmänna kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster ska vidta enligt 5 kap. 6 b § lagen om elektronisk kommunikation.

5.4.1 KRAV PÅ LÄMPLIGA TEKNISKA OCH ORGANISATORISKA ÅTGÄRDER

Lagen (2003:389) om elektronisk kommunikation (”**LEK**”) syftar till att ge enskilda och myndigheter tillgång till säkra och effektiva elektroniska kommunikationer. Lagens 6 kap. reglerar hur trafikuppgifter[245]

245 Med trafikuppgifter avses enligt 6 kap. 1 § LEK uppgifter som behandlas i syfte att befordra ett elektroniskt meddelande via ett elektroniskt kommunikationsnät eller för att fakturera detta meddelande.

ska behandlas och det skydd för uppgifternas riktighet som då ska gälla.

I förhållande till informationssäkerheten är 6 kap. 3 § LEK relevant. Bestämmelsen är tillämplig på den som tillhandahåller en allmänt tillgänglig elektronisk kommunikationstjänst och fastställer att denne ska vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa att de uppgifter som behandlas i samband med tjänsten åtnjuter ett tillräckligt skydd.

Åtgärderna ska ha som syfte att säkerställa en säkerhetsnivå som är anpassad till risken för integritetsincidenter. Säkerhetsnivån ska anpassas med beaktande av både tillgänglig teknik och kostnaderna för att åtgärderna ska kunna genomföras.[246]

Utöver detta finns ett krav på driftsäkerhet för den som tillhandahåller allmänna kommunikationsnät och allmänt tillgängliga elektroniska kommunikationstjänster i 5 kap. 6 b § LEK. Enligt bestämmelsen ska lämpliga tekniska och organisatoriska åtgärder vidtas för att säkerställa att verksamheten uppfyller rimliga krav på driftsäkerhet.

5.4.2 SKYDDSÅTGÄRDER FÖR BEHANDLADE UPPGIFTER

Post- och telestyrelsen (PTS) har genom PTSFS 2014:1 meddelat föreskrifter och allmänna råd om skyddsåtgärder för behandlade uppgifter. Bestämmelserna är tillämpliga på sådana tekniska och organisatoriska åtgärder som avses i 6 kap. 3 § LEK och ger således ytterligare föreskrifter på en mer detaljerad nivå.

Bestämmelserna gäller aktörer som tillhandahåller allmänt tillgängliga elektroniska kommunikationstjänster (tjänstetillhandahållare) och innebär i korthet att dessa ska:

- Bedriva ett långsiktigt, kontinuerligt och systematiskt säkerhetsarbete. Detta innebär bland annat att det ska finnas en tydlig rollfördelning när det gäller ansvar för arbetet och att rutiner för detta ska dokumenteras.

- Identifiera informationsbehandlingstillgångar där behandlade uppgifter förekommer samt analysera riskerna för att integritetsincidenter ska inträffa för dessa tillgångar.

5.4.3 KRAV

5.4.3.1 Åtkomst och behörighetshantering

De bestämmelser som rör åtkomst- och behörighetshantering är särskilt relevanta när det rör informationssäkerhetskravet *konfidentialitet*.

246 6 kap. 3 § LEK.

Av bestämmelserna framgår bland annat att tjänstetillhandahållaren ska säkerställa att åtkomst till behandlade uppgifter endast ges till den som (i) behöver det för att kunna utföra sitt arbete, (ii) har relevant utbildning med hänsyn till de uppgifter denna hanterar, samt (iii) har upplysts om tystnadsplikten i 6 kap. 20–21 §§ LEK.[247]

5.4.3.2 Loggning

Föreskrifterna innehåller även bestämmelser som är relevanta för informationssäkerhetskravet *spårbarhet*, det vill säga att all aktivitet ska kunna härledas till en identifierad användare som kan hållas ansvarig för åtgärden.[248] I 7 § PTSFS 2014:1 anges att tjänstetillhandahållaren ska logga all läsning, kopiering, ändring och utplåning av behandlade uppgifter. Loggningen ska ske på sådant sätt att det tydligt framgår vem som har vidtagit vilken åtgärd med vilka uppgifter samt vid vilken tidpunkt. Därutöver ska tjänstetillhandahållaren systematiskt och återkommande kontrollera dessa loggar samt dokumentera genomförda kontroller.

5.4.3.3 Lagring av uppgifter

Vidare omfattar föreskrifterna bestämmelser som avser skydda de lagrade uppgifterna från att försvinna. Föreskrifterna ställer bl.a. ett krav på tjänstetillhandahållaren att denne ska vidta åtgärder för att säkerställa att de uppgifter som lagras är skyddade mot oavsiktlig eller otillåten utplåning och förlust.[249] En sådan bestämmelse kan anses uppfylla kravet på att informationen ska vara *tillgänglig* för de som behöver den. I dessa fall rör det sig om ett mer fysiskt skydd för uppgifterna. Enligt föreskrifterna ska informationsbehandlingstillgångar där uppgifterna lagras placeras i utrymmen som har skydd mot intrång. Rutinerna för placeringen av dessa tillgångar ska dokumenteras av tjänstetillhandahållaren.[250] Av de allmänna råden till bestämmelsen framgår att tjänstetillhandahållaren även bör säkerhetskopiera uppgifterna för att säkerställa skyddet mot utplåning eller förlust.[251]

5.4.3.4 Kryptering

För att säkerställa att informationen inte nås av obehöriga, innehåller föreskrifterna även en bestämmelse om kryptering. Av bestämmelsen framgår att behandlade uppgifter som överförs via internet ska skyddas genom kryptering, förutsatt att det inte rör en överföring till den berörde användaren som vid det enskilda tillfället samtyckt till att överföringen sker utan kryptering. Vidare gäller att krypteringen ska

247 5 § PTSFS 2014:1.

248 7 § PTSFS 2014:1.

249 8 § PTSFS 2014:1.

250 8 § PTSFS 2014:1.

251 PTSFS 2014:1 *Allmänna råd* till 8 §.

ske med en allmänt erkänd krypteringsmetod, att krypteringsnycklarna ska hanteras på ett säkert sätt, och att rutiner för kryptering och hantering av krypteringsnycklar ska dokumenteras.[252]

5.4.3.5 Robusthet

Tillhandahållare måste även beakta bestämmelsen i 5 kap. 6 b § LEK som föreskriver att dessa måste vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa att verksamheten uppfyller rimliga krav på driftsäkerhet. PTS har genom PTSFS 2015:2 meddelat detaljerade föreskrifter med krav på sådana åtgärder, bl.a. i form av att genomföra risk- och konsekvensanalyser. Analyserna ska behandla risken för att dokumenterade tillgångar och förbindelser orsakar störningar eller avbrott i de tillhandahållna kommunikationsnäten eller kommunikationstjänsterna. Tillhandahållaren ska även vidta de åtgärder som är nödvändiga för att skydda tillgångarna mot de identifierade riskerna. Vidare ska tillhandahållaren se till att ha en handlingsplan för hur inträffade risker ska hanteras, vilket bland annat omfattar åtgärder för att begränsa konsekvenserna som kan uppstå, samt åtgärder för att återställa kritiska verksamhetsdelar till normal funktionsförmåga efter en inträffad händelse (kontinuitetsplanering). I denna process ska tillhandahållaren klassificera tillgångarna utifrån det antal aktiva anslutningar som kan omfattas av störningar eller avbrott i fall tillgången upphör att fungera normalt. Därefter ska tillhandahållaren säkerställa tillgångarnas funktion genom redundans i den utsträckning som följer av klassificeringen.

5.4.4 INTEGRITETSINCIDENTER

Tjänstetillhandahållaren ska slutligen även ha dokumenterade rutiner för eventuella integritetsincidenter.[253] Dokumentationen ska innehålla rutiner för identifiering, intern rapportering, hantering och uppföljning av sådana incidenter. Rutinerna ska säkerställa att viktiga uppgifter om incidenten förs in i den förteckning som tjänstetillhandahållaren ska föra enligt 6 kap. 4 b § LEK, bland annat datum, beskrivning av händelsen, uppskattat antal användare, bedömda konsekvenser, samt vidtagna åtgärder. Rutinerna ska även säkerställa att inträffade integritetsincidenter och dess orsaker beaktas vid riskanalyser, samt att skyddsåtgärder vidtas för att undvika att liknande incidenter upprepas.[254]

5.4.5 TILLSYN

Post- och telestyrelsen utövar tillsyn över regelefterlevnaden enligt LEK

252 9 § PTSFS 2014:1.

253 10 § PTSFS 2014:1.

254 10 § PTSFS 2014:1.

och anslutande föreskrifter.[255] Vad gäller informationssäkerhet omfattar tillsynsansvaret att ta emot incidentrapporter enligt 6 kap. 4 a § LEK.

5.4.6 UTVECKLING FRAMÖVER

Genom lagen (2003:389) om elektronisk kommunikation (LEK) införlivades det så kallade ePrivacy-direktivet i svensk lagstiftning. EU-kommissionen har nu lämnat ett förslag till en ny förordning om integritet och elektronisk kommunikation (ePrivacy-förordningen), som fortfarande förhandlas mellan EU:s medlemsstater.[256] ePrivacy-förordningen föreslås upphäva ePrivacy-direktivet och gälla som ett komplement till dataskyddsförordningen. När ePrivacy-förordningen väl godkänns och träder i kraft kommer det få effekten att bland annat LEK måste uppdateras utifrån de nya bestämmelserna.

5.5 Banker

TILLSYN OCH TILLÄMPLIGA FÖRFATTNINGAR

Tillsynsmyndighet	Finansinspektionen
Finansinspektionens föreskrifter och allmänna råd om informationssäkerhet, it-verksamhet och insättningssystem, FFFS 2014:5	Tillämpas på kreditinstitut och värdepappersbolag. Ställer krav på dels ett strukturerat och metodiskt informationssäkerhetsarbete, dels styrning och processer för it-verksamheten samt krav på säkerheten för insättningssystem. I arbetet med informationssäkerhet ska bland annat ett ledningssystem användas.
Europeiska bankmyndighetens riktlinjer om outsourcing, EBA/GL/2019/02	Riktlinjerna gäller för kreditinstitut, värdepappersbolag, betalningsinstitut och institut för elektroniska pengar. Syftar till att precisera riskhanteringsarbetet som dessa ska tillämpa vid utkontraktering.

5.5.1 KRAV PÅ INFORMATIONSSÄKERHETSARBETET

De krav som ställs på banker gällande informations- och cybersäkerhet[257] utgår från de regler om riskhantering som återfinns i 6 kap. 2 § lagen (2004:297) om bank och finansieringsrörelse (”**BFL**”). Dessa inne-

255 2 § förordningen (2003:396) om elektronisk kommunikation.

256 I skrivande stund finns senaste förslag på https://data.consilium.europa.eu/doc/document/ST-13808-2019-INIT/en/pdf.

257 Cybersäkerhet omfattar de mekanismer och åtgärder som används för att skydda en cyberdomän mot de hot som är förknippade med eller som kan skada dess ömsesidigt beroende nätverk och informationsinfrastruktur, se SOU 2015:23 Informations- och cybersäkerhet i Sverige – strategi och åtgärder för säker information i staten, Betänkande av NISU 2014, s. 41.

bär att kreditinstitut ska ha kontroll över de risker som dess rörelse är förknippad med. Till dessa regler tillkommer Finansinspektionens föreskrifter och allmänna råd, i detta avseende framför allt FFFS 2014:1 om styrning, riskhantering och kontroll i kreditinstitut, FFFS 2014:4 om hantering av operativa risker, samt FFFS 2014:5 om informationssäkerhet, it-verksamhet och insättningssystem.

Föreskrifterna gäller för kreditinstitut och värdepappersbolag, men i denna del har vi valt att tala om banker.[258]

FFFS 2014:1 ställer krav på att företagen ska ha ändamålsenliga it-system och rutiner för att skydda konfidentialitet, riktighet och tillgänglighet i sin information, med beaktande av den berörda informationens art.[259] Av FFFS 2014:4 följer att bankerna ska ha regler, rutiner och processer för att dels identifiera risker, dels hantera incidenter.[260]

Till skillnad från Finansinspektionens övriga föreskrifter, har FFFS 2014:5 ett tydligt fokus på informationssäkerhet. FFFS 2014:5 ställer krav på att bankerna ska arbeta strukturerat och metodiskt med informationssäkerhet genom att använda sig av ledningssystem.[261] Bankerna ska således dokumentera mål och inriktning för informationssäkerheten samt säkerställa en tydlig fördelning av ansvaret för informationssäkerheten. Till detta hör att det ska finnas interna regler för informationssäkerhetsarbetet.

Enligt Finansinspektionens allmänna råd till FFFS 2014:5 bör de interna reglerna ange krav på bl.a. fysisk säkerhet, skydd av datakommunikation och drift, spårbarhet i it-system, produktionsmiljön för it-system, styrning av åtkomst till information, rapportering och hantering av incidenter, och en regelbunden kontroll av företagets it-system. Reglerna ska särskilt ange hur företaget ska tilldela, ändra och ta bort åtkomstbehörigheter till it-system. Företaget ska även regelbundet, dock minst årligen, kontrollera att befintliga åtkomstbehörigheter är begränsade till behov.[262]

Därtill måste informationen i verksamheten klassificeras, för att på så vis kunna säkerställa en adekvat skyddsnivå, och informationssäkerhetsrelaterade risker analyseras och dokumenteras. Detta ska ske årligen, eller vid större förändringar av betydelse för informationssäkerheten, och göras utifrån kriterierna konfidentialitet, riktighet och tillgänglighet.[263]

I sammanhanget är det även relevant att nämna Datainspektionens

---

258 Med kreditinstitut och värdepappersbolag avses bankaktiebolag, sparbanker, medlemsbanker, kreditmarknadsbolag, kreditmarknadsföreningar, och värdepappersbolag. För definitioner, se BFL och lagen (2007:528) om värdepappersmarknaden.

259 2 kap. 2 § FFFS 2014:1.

260 3 och 5 kap. FFFS 2014:4.

261 2 kap. FFFS 2014:5.

262 1 kap. 8 § FFFS 2014:5.

263 2 kap. 5 § FFFS 2014:5.

tillsynsärenden i fråga om bankappar, där inspektionen uttalade att de integritetskänsliga uppgifter som är åtkomliga genom bankappar innebär att det måste ställas högre krav på autentisering, t.ex. genom att autentiseringen sker med två faktorer, t.ex. en PIN-kod och telefonen till vilken applikationen är knuten.[264]

Utöver Finansinspektionens krav bör även den Europeiska bankmyndigheten (”**EBA**”) nämnas. EBA har som uppgift att skapa enhetlig reglering och tillsyn av banksektorn inom EU-länderna, vilket bl.a. innefattar att utfärda riktlinjer. Syftet med riktlinjerna är att skapa en effektiv och öppen marknad för bankprodukter i EU.[265]

EBA:s riktlinjer för utkontraktering[266] innehåller detaljerade krav avseende utkontrakteringsprinciper, där de mest relevanta utifrån ett informationssäkerhetsperspektiv blir de som rör skyddet av data.[267] Enligt riktlinjerna ska banker identifiera säkerhetskrav som ställs på data och datasystem inom utkontrakteringsavtalet samt säkerställa att tjänsteleverantörer uppfyller lämpliga krav på it-säkerhet. I detta ligger att banken ska kontrollera att kraven efterföljs.

Ifall utkontrakteringen involverar behandling av personuppgifter eller uppgifter som omfattas av banksekretess, måste banken vara särskilt riskmedveten och säkerställa att tjänsteleverantören skyddar sådan information.

Slutligen ska något sägas om EBA:s riktlinjer för IKT (informations- och kommunikationsteknologi).[268] I riktlinjerna ställs ett antal krav på såväl informationssäkerhetsåtgärder som informationssäkerhetsarbetet, som bör vidtas av banker. Kraven tar bl.a. sikte på loggning, ansvarsutkrävande, tillgänglighet, autenticitet och konfidentialitet, dvs. majoriteten av de aspekter vi lyft fram i avsnitten 2–4.[269]

5.5.2 FINANSINSPEKTIONENS TILLSYN

I tillägg till de föreskrifter och riktlinjer som nämnts ovan, finns det anledning att framhålla Finansinspektionens tillsynsrapport om bankers arbete med informations- och cybersäkerhet.[270] I rapporten pekar Finansinspektionen ut ett antal punkter där myndigheten identi-

---

264 Datainspektionen, *Tillsyn enligt personuppgiftslagen (1998:204) – bankers användning av s.k. appar,* 11 september 2013, bl.a. dnr. 1612-2011.

265 EBA:s riktlinjer är främst riktade till de nationella tillsynsmyndigheterna, som i sin tur har en skyldighet att ”följa eller förklara” (Engelska: *comply or explain*). Finansinspektionen har en tydlig tendens att följa EBA:s riktlinjer utan reservationer. Detta innebär i sin tur att EBA:s riktlinjer, om än inte direkt tillämpliga för bankerna, blir relevanta i relation till Finansinspektionens tillsyn.

266 Kallas även *uppdragsavtal* eller *utlagd verksamhet*. Vad som avses är, i korthet, att banken uppdrar åt en leverantör att utföra en verksamhet eller tillhandahålla en funktion som är viktig för själva bankverksamhet och annars hade utförts av banken själv.

267 Se avsnitt 13.2 i EBA:s *Riktlinjer för utkontraktering*.

268 EBA *Guidelines on ICT and security risk management*, 28 November 2019, EBA/GL/2019/04.

269 Se särskilt punkten 31, men även 32-49.

270 Finansinspektionens tillsynsrapport *Bankernas arbete med information- och cybersäkerhet,* FI-tillsyn nr 9 av den 7 december 2018.

fierar ett särskilt behov för bankernas ledning att agera. Det är inte otänkbart att synpunkterna och åtgärderna *som sådana* kan vara relevanta också för försäkringsföretag. I korthet rekommenderas att bankernas respektive ledningar ska:

- Säkerställa att ledningssystemet för informationssäkerheten även införs i praktiken;

- Analysera och bedöma aktuella cyberhot för att kunna anpassa riskhanteringen genom en kontinuerlig riskanalys; och

- Prioritera utbildning av personalen för att öka medvetenheten kring informations- och cybersäkerhet.[271]

Givet detta, kan det misstänkas att Finansinspektionen ser ett behov av dels en ökad medvetenhet avseende informationssäkerhet, dels fler faktiska åtgärder som syftar till just informationssäkerhet. Bland dessa åtgärder framhålls särskilt följande:

- Kryptering och övervakning av data som ett sätt att skydda data som lagras eller transporteras;[272]

- En begränsning av riskerna för obehörig åtkomst i form av nätverkssegmentering;[273]

- Upprättandet av en standard för säkerhetskonfiguration för hård- och mjukvara, som bl.a. reglerar vilka tjänster och nätverksportar som tillåts vara öppna. Detta syftar till att löpande kunna uppdatera standardkonfigurationer i takt med att nya hot och sårbarheter identifieras; och

- Skyddsåtgärder mot externa hot, genom t.ex. brandväggar, system för upptäckt av intrång, förhindrande av intrång och anti-virusskydd.

271 Finansinspektionens tillsynsrapport *Bankernas arbete med information- och cybersäkerhet*, s. 3 och 13-14.

272 Även benämnt *data at rest* och *data in transit*.

273 Del av ett nätverk med minsta möjliga kontakt med övriga delar av nätverket. Genom att dela upp ett nätverk i flera segment kan it-attacker begränsas till ett visst segment istället för att påverka hela nätverket.

5.6 Identitetstjänster

TILLSYN OCH TILLÄMPLIGA FÖRFATTNINGAR

Tillsynsmyndighet	Post- och telestyrelsen
eIDAS-förordningen	Förordningen är tillämplig på system för elektronisk identifiering som har anmälts av en medlemsstat samt på tillhandahållare av betrodda tjänster som är etablerade inom EU. Syftet med förordningen är att uppnå en lämplig säkerhetsnivå för medel för elektronisk identifiering och betrodda tjänster så att informationssäkerheten kan bevaras. Förordningen ställer bland annat krav på: • Tekniska och organisatoriska åtgärder • Rapportering av säkerhetsincidenter • Registrering av information • Formen på elektroniska underskrifter och stämplar

5.6.1 KRAV FÖR ELEKTRONISK IDENTIFIERING

Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden (”**eIDAS-förordningen**”) reglerar elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på EU:s inre marknad. Förordningen innebär att det numer är obligatoriskt för offentliga organ, och frivilligt inom den privata sektorn, att tillåta inloggning med utländska e-legitimationer.[274]

Förordningen är tillämplig på system för elektronisk identifiering som har anmälts av en medlemsstat samt på tillhandahållare av betrodda tjänster som är etablerade inom EU.[275] Syftet med förordningen är att säkerställa en välfungerande inre marknad och att uppnå en lämplig säkerhetsnivå vad avser medel för elektronisk identifiering och betrodda tjänster så att informationssäkerheten kan bevaras. Vidare syftar förordningen till att öka förtroendet för elektroniska transaktioner på den inre marknaden genom en gemensam grund för ett säkert samarbete mellan privatpersoner, företag och offentliga myndigheter.[276]

Reglerna är bindande och direkt tillämpliga i Sverige. Det finns dock kompletterande nationella bestämmelser om ackreditering, certifiering,

274 Artikel 6 eIDAS-förordningen.

275 Artikel 2 eIDAS-förordningen.

276 Skäl 2 eIDAS-förordningen.

tillsyn, avgifter och processuella frågor.[277] Ansvaret för tillsyn över regelefterlevnaden ligger hos PTS.[278]

Förordningen utgör ett ramverk och saknar således detaljregler. Bestämmelser på mer detaljerad nivå ska istället tas fram i samarbete mellan kommissionen och medlemsstaterna själva i så kallade genomförandeakter.[279] I väntan på dessa regler har PTS uttalat att det är lämpligt att använda de standarder som standardiseringsorganisationerna European Committee for Standardization (CEN) och European Telecommunications Standards Issue (ETSI) har beslutat på området. Dessa standarder är utformade utifrån förordningen och avses utgöra grunden för kommande genomförandeakter i vilka närmare säkerhetskrav kommer återfinnas.[280]

5.6.2 INFORMATIONSSÄKERHET

Förordningen ställer flera krav på tillhandahållare av betrodda tjänster. Bland dessa krav kan det, ur ett informationssäkerhetsperspektiv, särskilt framhållas att tillhandahållaren ska vidta lämpliga tekniska och organisatoriska åtgärder för att hantera riskerna för säkerheten hos de betrodda tjänster som tillhandahålls. Åtgärderna ska säkerställa att säkerhetsnivån står i proportion till graden av risk med beaktande av teknikutvecklingen.[281]

Tillhandahållaren ska under en lämplig tidsperiod registrera och hålla tillgänglig all relevant information om uppgifter som tillhandahållaren utfärdat och tagit emot (jfr tillgänglighet). Med ”*relevant information*” avses bl.a. avtal och dokumentation som ligger till grund för utfärdande av enskilda certifikat. I denna fråga har PTS bedömt att en lämplig tidsperiod är minst tio år från det att giltighetstiden har upphört (för det certifikat uppgifterna är knutna till).[282]

I fråga om incidenter ska tillhandahållaren, inom 24 timmar, anmäla alla säkerhetsincidenter eller integritetsförluster till PTS, vilka i betydande omfattning påverkar den betrodda tjänst som tillhandahålls. Om det är troligt att incidenten kommer ha en negativ påverkan på en fysisk eller juridisk person till vilken tjänsten tillhandahållits ska denne också underrättas utan onödigt dröjsmål av tillhandahållaren.[283]

---

277 Lag (2016:561) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering.

278 4 § förordningen (2016:576) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering.

279 Bemyndiganden att utfärda genomförandeakter finns i artiklarna 8.3, 9.5, 12.7. 12.8, 17.8, 19.4, 20.4, 21.4, 22.5, 23.3, 24.4, 27.4, 27.5 , 28.6, 29.2, 30.3, 31.3, 32.3, 33.2, 34.2, 37.4, 37.5, 38.6, 42.2, 44.2 samt 45.2 eIDAS-förordningen.

280 Se PTS rapport *Vägledning för betrodda tjänster i Sverige enligt eIDAS- utgåva 2*, Diarienummer 17-4465, s. 11.

281 Artikel 19 eIDAS-förordningen.

282 Se Post-och telestyrelsens rapport *Vägledning för betrodda tjänster i Sverige enligt eIDAS-utgåva 2*, s. 29.

283 Artikel 19.2 eIDAS-förordningen.

Flera konkreta krav ställs även på underskrifter, stämplar, tidsstämplingar samt överföring av information (elektroniska tjänster för rekommenderade leveranser).[284] Dessa krav tar framför allt sikte på spårbarhet och riktighet.

Vad avser spårbarhet finns det exempelvis krav på att en elektronisk underskrift ska vara unikt kopplad till undertecknaren och att det inte ska vara möjligt att ändra uppgifter om en tidsstämpel i efterhand.[285]

Riktigheten tillvaratas i sin tur exempelvis genom att såväl avsändaren som mottagaren av uppgifter i elektroniska tjänster för rekommenderade leveranser ska vara identifierade vid informationsöverföring, och att det inte ska vara möjligt att ändra uppgifterna under överföringen.

5.7 Bokföring

TILLÄMPLIGA FÖRFATTNINGAR

Bokföringslagen (1999:1078)	Är tillämplig på fysiska eller juridiska personer som är bokföringsskyldiga enligt bokföringslagen. Innehåller bestämmelser om bokföringsskyldighet, vilket bland annat innebär krav på att information ska bevaras på visst sätt och under viss tid.

Bokföringslagen (1999:1078) innehåller bestämmelser om bokföringsskyldighet för vissa fysiska och juridiska personer. Lagen omfattar även de skyldigheter som uppkommer när räkenskapsinformation ska arkiveras och bevaras.

I sjunde kapitlet framgår de åtgärder som måste vidtas för att informationen ska bevaras på ett informationssäkert sätt. I kapitlets inledande bestämmelser fastställs formen för bevarandet samt tid och plats för förvaringen. Dessa bestämmelser hänförs främst till kraven på *tillgänglighet, riktighet* samt *spårbarhet*. I korthet innebär bestämmelserna att:

- Informationen ska bevaras på ett lättåtkomligt och tillgängligt sätt. Detta innebär att den kan bevaras antingen i vanlig läsbar form eller i en form som gör att informationen kan utläsas med ett hjälpmedel. Ett sådant hjälpmedel kan vara både ett förstoringshjälpmedel för mikroskrift eller ett tekniskt hjälpmedel som gör att materialet kan läsas, avlyssnas eller på annat sätt uppfattas.[286]

- Information som företaget har fått från någon annan ska bevaras

284 Exempelvis artikel 26, 36, 42 och 44 eIDAS-förordningen.

285 Artikel 26 eIDAS-förordningen.

286 7 kap. 1-2 §§ bokföringslagen.

i det skick materialet hade när det kom till företaget. Har företaget självt upprättat informationen ska det bevaras i det skick det fick när informationen sammanställdes. Som grundkrav gäller dock att informationen ska bevaras i ett ordnat skick och på ett betryggande och överskådligt sätt.[287]

- Informationen ska bevaras fram till och med det sjunde året efter utgången av det kalenderår då räkenskapsåret avslutades. Detta gäller även den utrustning som behövs för att presentera informationen.[288]

- Informationen och eventuell hjälpmedelsutrustning ska bevaras i Sverige. Det finns dock vissa undantag till denna bestämmelse där företag kan få tillåtelse att i vissa fall förvara information och utrustning utomlands.[289]

7 kap. bokföringslagen innehåller även bestämmelser om överföring av räkenskapsinformation och när räkenskapsinformation får förstöras. Vad avser överföring av informationen får ett företag förstöra material för bevarande av informationen endast i de fall informationen på ett betryggande sätt överförs till något annat sådant material.[290] Bestämmelsen uppfyller informationssäkerhetskravet på att informationen ska vara *tillgänglig*, det vill säga att den inte ska förstöras i samband med materialet.

5.8 Cybersäkerhet

TILLSYN OCH TILLÄMPLIGA FÖRFATTNINGAR

Cybersäkerhetsakten	EU-förordning om Enisa och om cybersäkerhetscertifiering av informations- och kommunikationsteknik. Syftar till att höja cybersäkerheten inom EU genom bland annat krav på certifiering.

I fråga om cybersäkerhetsområdet är värt att uppmärksamma att rättsläget kan komma att förändras genom en ny förordning om cybersäkerhetscertifiering som ska stärka cybersäkerheten för nät- och informationssystem.

Förordningen, även kallad cybersäkerhetsakten[291], innebär inrättandet av ett EU-omfattande certifieringssystem som ska säkerställa att produkter, processer och tjänster som säljs inom EU uppfyller standarderna

287 7 kap. 1 § 2 st. bokföringslagen.

288 7 kap. 2 § bokföringslagen.

289 För en uttömmande lista på dessa situationer hänvisas till 7 kap. 3-5 §§ bokföringslagen.

290 7 kap. 6 § bokföringslagen.

291 Europaparlamentets och rådets förordning (EU) 2019/881 av den 17 april 2019 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik och om upphävande av förordning (EU) nr 526/2013.

för cybersäkerhet. Systemet ger ett permanent mandat och ökade resurser till EU:s cybersäkerhetsbyrå, Enisa. Kraven på certifiering har som syfte att öka cybersäkerheten inom EU, vilket ska bidra till ett mer informationssäkert samhälle.[292]

Förordningen trädde i kraft den 27 juni 2019 och började tillämpas direkt med undantag för vissa artiklar som kräver kompletterande bestämmelser på nationell nivå. Dessa ska därför börja tillämpas först den 28 juni 2021. Arbetet pågår därför nu med att ta fram den kompletterande nationella regleringen och att säkerställa att den finns på plats när resterande artiklar i cybersäkerhetsakten ska börja tillämpas.

5.9 Offentlighet och sekretess

TILLÄMPLIGA FÖRFATTNINGAR

Tryckfrihetsförordningen (1949:105), TF	Avgränsar vilka uppgifter i myndigheters verksamhet som utgör allmänna handlingar.
Offentlighets- och sekretesslagen (2009:400), OSL	Reglerar vilka allmänna handlingar som är och inte är offentliga.
Arkivlagen (1980:782)	Ytterligare krav på hur information i allmänna handlingar ska hanteras.
Riksarkivets föreskrifter och allmänna råd om elektroniska handlingar (upptagningar för automatiserad behandling), RA-FS 2009:1	Innehåller krav på informationssäkerhet för arkivering av elektroniska handlingar.

För verksamheter som tillämpar TF och OSL ställs särskilda krav på informationshantering vilka kan leda till särskilda utmaningar utifrån ett informationssäkerhetsperspektiv. Huvudregeln vad gäller främst myndigheter är att alla handlingar hos en myndighet är allmänna, d.v.s. tillgängliga för var och en. Från denna utgångspunkt finns två inskränkande faktorer; dels är alla uppgifter som en myndighet har tillgång till inte del av någon handling i TF:s mening, dels kan uppgifterna vara föremål för någon av de många sekretessregleringar som finns i OSL.

De sekretessregleringar som finns i OSL kan i grova drag delas upp i sådana med rakt skaderekvisit (även kallat svag sekretess), omvänt skaderekvisit (stark sekretess) och absolut sekretess. Bedömningen görs utifrån det intresse som sekretessregeln avser att skydda och om ett

292 Cybersäkerhetsaktens motivering, s. 3.

utlämnande kan anses leda till skada på detta intresse (med undantag för absolut sekretess, där man inte gör någon bedömning av en eventuell skada). Detta utgör också en form av reglerad informationsklassificering där uppgifter ska ha olika grad av skydd mot det röjande som ett utlämnande av en allmän handling innebär.

Utöver detta finns bestämmelser i arkivlagen om hur handlingar i arkiv ska hanteras (arkivvård) vilka har betydelse för informationssäkerheten. I arkivlagen 6 § tredje punkten anges att myndigheten ska skydda arkivet mot förstörelse, skada, tillgrepp och obehörig åtkomst, vilket även är ett grundläggande informationssäkerhetskrav. Mer detaljerade krav på informationssäkerhet finns i 6 kap. RA-FS 2009:1 och innefattar bl.a. krav på rutiner med utgångspunkt från ISO/IEC 27001 och 27002, upprättande av plan för informationssäkerhet samt riskanalys och vissa konkreta krav på skyddsåtgärder.

Vi vill i detta sammanhang understryka att de krav som följer av TF, OSL och arkivlagen är betydligt mer omfattande än de grundläggande regler som har betydelse för informationssäkerheten och som vi har nämnt här.[293]

5.10 Avslutande synpunkter

Mot bakgrund av vad som redogjorts för i detta kapitel kan noteras att det finns flera gemensamma drag som utmärker informationssäkerhetsarbetet inom de sektorspecifika bestämmelserna. Dessa är främst:

- En begränsad behörighet till uppgifter;
- Loggning av alla åtgärder i ett system;
- Utförandet av en riskanalys som omfattar en klassning av den information som behandlas;
- Incidentrapportering till ansvarig tillsynsmyndighet;
- Utvecklandet av ett ledningssystem; samt
- Utvecklandet av en god säkerhetskultur inom verksamheten vilket omfattar utbildningar för personalen.

Att dessa krav kan återfinnas inom flera av de olika sektorerna tyder på att de tillsammans utgör en typ av gemensam verksamhetsstandard för hur ett informationssäkert arbete ska bedrivas, särskilt som dessa åtgärder och krav är genomgående för säkerhetsskyddslagen, NIS-lagen, dataskyddsförordningen och ISO 27000-serien.

293 För en grundläggande genomgång av framförallt TF och OSL, se Bohlin, Alf, *Offentlighetsprincipen*, 9 uppl., Norstedts Juridik (2015).

6. Jämförelse mellan regelsystemen

För att kunna skapa sig en förståelse för vilka eventuella beröringspunkter som finns mellan de olika regelsystemen, måste dessa naturligtvis jämföras. Detta görs inledningsvis genom tabellen nedan.

Sammanställningen ger även en övergripande bild av och förståelse för respektive regelsystem. Förhoppningsvis kan den även användas som ett hjälpmedel för att navigera i denna rapport.

	Dataskydds-förordningen	**NIS-lagen**	**Säkerhetsskyddslagen**
Tillämpnings-område	Behandling av person-uppgifter, se avsnitt 4.2.1	Samhällsviktiga tjänster och digitala tjänster, se avsnitt 3.2.1	Säkerhetskänslig verksamhet, se avsnitt 2.2.1
Skyddsintresse	Enskildas fri- och rättig-heter, se avsnitt 4.2.2	Samhällsfunktioners tillförlitlighet och säker-het, se avsnitt 3.2.2	Sveriges säkerhet, se avsnitt 2.2.2
Hotbild	Kränkning av enskildas rättigheter genom felaktig behandling av personuppgifter, se avsnitt 4.2.3	Omständigheter och händelser med negativ inverkan på säker-heten i nätverk och informationssystem, se avsnitt 3.2.3	Antagonistiska hot mot Sverige och grunderna för stats-skicket, se avsnitt 2.2.3
Identifiering	Register över behand-lingen, se avsnitt 4.3.2	Identifiera samhälls-viktiga tjänster, se avsnitt 3.3.2	Identifiera skyddsvärden, se avsnitt 2.3.2
Analys	Konsekvensbedömning, se avsnitt 4.3.3	Riskanalys med åtgärds-plan, se avsnitt 3.3.3	Säkerhetsskyddsanalys Gradera skada från antagonistisk verksam-het, se avsnitt 2.3.3
Utformning av skydd	Säkerställ lämplig säkerhetsnivå Planera åtgärder, se avsnitt 4.3.4	Vidta ändamålsenliga och proportionella åtgärder för att hantera risker Minimera verkningar av ev. incidenter Beakta accepterade standarder, se avsnitt 3.3.4	Upprätta säkerhets-skyddsplan med skyddsdimensione-ring, se avsnitt 2.3.4

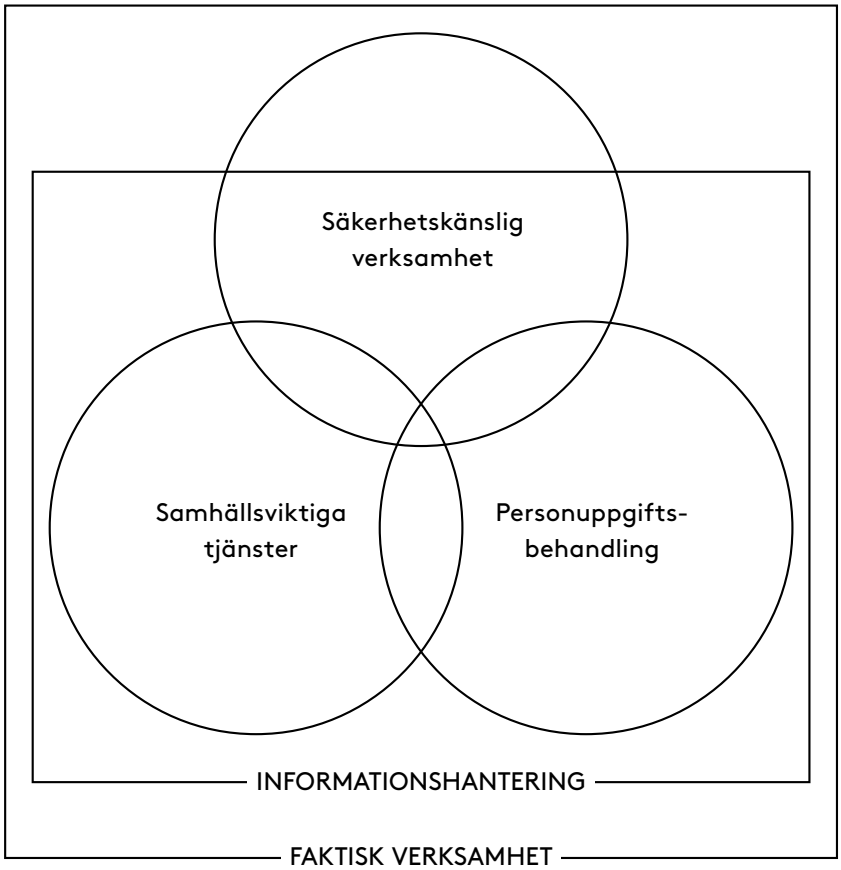
	Dataskydds-förordningen	NIS-lagen	Säkerhetsskyddslagen
Tillämpa/ följa upp	Hantera incidenter Genomför översyn, se avsnitt 4.3.5	Hantera incidenter Riskanalys ska uppdateras årligen Förhindra liknande incidenter, se avsnitt 3.3.5 och 3.3.6	Inrätta funktioner Dokumentera regelverk för upprätthållande av säkerhetsskyddet Säkerhetsskyddsanalysen ska hållas uppdaterad, se avsnitt 2.3.5 och 2.3.6
Tillsyns-myndighet	Datainspektionen, se avsnitt 4.6.1	Beroende på tjänstens typ, se avsnitt 3.6.1	Beroende på verksamhetens art, se avsnitt 2.6.1
Incident	Incident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter, se avsnitt 4.6.2	Incidenter med betydande inverkan på kontinuiteten, se avsnitt 3.6.2	Säkerhetsskyddsklassificerad uppgift kan ha röjts It-incident som allvarligt kan påverka ett system av betydelse för säkerhetskänslig verksamhet Kännedom eller misstanke om allvarlig säkerhetshotande verksamhet, se avsnitt 2.6.2
Incident-rapportering	Inom 72 timmar, anmäla till behörig tillsynsmyndighet I förekommande fall, informera de registrerade, se avsnitt 4.6.2	Inom sex timmar, underrätta CERT-SE om incidenten Inom 24 timmar, lämna skriftlig rapport till CERT-SE Inom fyra veckor, lämna skriftlig rapport med utvärdering och förebyggande åtgärder till CERT-SE, se avsnitt 3.6.2	Skyndsamt anmäla incidenten till Säkerhetspolisen eller Försvarsmakten I förekommande fall, underrätta andra berörda verksamhetsutövare, se avsnitt 2.6.2
Samråd	Inför riskfylld behandling, se avsnitt 4.6.3	N/A	Inför driftsättning av ett it-system för uppgifter i säkerhetsskyddsklass konfidentiell eller högre, eller vid vissa upphandlingar av statliga myndigheter, se avsnitt 2.6.3
Sanktioner	Upp till 10 miljoner EUR eller 2 % av årsomsättning, eller Upp till 20 miljoner EUR eller 4 % av årsomsättning, se avsnitt 4.6.4	Mellan 5 000 kr och 10 miljoner kr, se avsnitt 3.6.4	N/A

7. Konflikt och samordning mellan regelsystemen

7.1 Utgångspunkter

Detta avsnitt syftar till att belysa hur de olika regelsystemen kan tillämpas på ett samordnat sätt och vilka potentiella konflikter som finns.

I en verksamhet kan i ”värsta” fall samtliga regleringar bli tillämpliga på en viss del av verksamheten. Nedanstående bild illustrerar de tre stora regelsystemens tillämpningsområden på ett generellt sätt. Det är bara när cirklarna överlappar som det finns en potential för konflikt.



En utgångspunkt är att informationssäkerhetsarbete har ett värde utöver regelefterlevnaden som sådan, och hade behövt göras även om inget regelverk på området existerade. Det bör inte finnas en direkt konflikt mellan organisationens eget behov av informationssäkerhet och lagstiftningens krav på detsamma, även om lagstiftningen kan kräva att organisationen går längre i arbetet än vad organisationen annars hade gjort. Detta gäller även mellan de olika regelsystemen, dvs. de krav på informationssäkerhetsarbete som ställs bör inte vara

inbördes oförenliga, även om en viss lagstiftning kan ställa mer långtgående krav än en annan.

Det är därför rimligt att sträva efter att samordna informationssäkerhetsarbetet efter dels de olika regelsystemens krav, dels verksamhetens eget behov av informationssäkerhet. Men det sker inte av sig självt. Regelsystemen har i många fall ett annat skyddsintresse än verksamheten i sig, vilket i sig kan resultera i att en konflikt uppstår. Regelsystemens olika syften och utformning medför även potentiella konflikter vid gränsdragningen mellan systemens tillämpningsområden, gränssnitt och rapporteringsskyldigheter mot myndigheter samt specifika krav på processer för informationssäkerhetsarbete. Vi går därför i detta kapitel igenom de konflikter som finns mellan regelsystemen för att sedan ge ett förslag på hur ett samordnat informationssäkerhetsarbete kan utformas.

7.2 Konflikt

7.2.1 INLEDNING

Som inledningsvis påpekades i detta avsnitt bör de krav på informationssäkerhetsarbete som ställs i regelverken inte vara inbördes oförenliga. Det är ofta liknande skyddsåtgärder som krävs för att uppnå en adekvat nivå av informationssäkerhet, trots att regelverkens skyddsobjekt samt tillvägagångssätt skiljer sig åt. Kraven kan också vara olika långtgående vad gäller vilken säkerhetsnivå som ska uppnås.

Det är dock inte möjligt att rakt av tillämpa informationssäkerhetsprocesser utformade för ett visst regelverk på skyddsintressen som omfattas av ett annat regelverk. Det finns vissa grundläggande skillnader avseende bl.a. vad som utgör ett skyddsintresse, som i sin tur påverkar informationsklassificering och hotbilder.

Med andra ord, dessa grundläggande olikheter kan innebära att det ena regelverket kräver att en viss skyddsåtgärd vidtas, samtidigt som denna skyddsåtgärd innebär att ett skyddsobjekt enligt ett annat regelverk äventyras. Ett typiskt exempel är om säkerhetsskyddslagen ställer krav på omfattande och/eller integritetskänslig behandling av personuppgifter. Det ska dock förtydligas att detta inte är en regelkonflikt, utan snarare att betrakta som en intressekonflikt mellan respektive regelverks skyddsobjekt som lösts genom lagstiftning.

Det är således viktigt att komma ihåg att regelverken tagits fram för olika syften och med olika skyddsobjekt. Dessa grundläggande skillnader, menar vi, ger upphov till de huvudsakliga konflikterna mellan regelverken. I denna del belyser vi vissa konfliktytor mellan regelverken vilka vi identifierat.[294]

294 Naturligtvis kan det finnas ytterligare tänkbara konflikter mellan regelverken med informationssäkerhet som den gemensamma nämnaren. Detta avsnitt syftar inte till att uttömmande beskriva konflikterna mellan regelverken, utan snarare att belysa att det finns en konfliktyta mellan regelverken.

7.2.2 TILLÄMPNINGSOMRÅDE OCH SUBSIDIARITET

Genom bestämmelser om subsidiaritet och tillämpningsområde har de olika regelverken samordnats för att undvika konflikter. Dataskyddsförordningen gäller för personuppgiftsbehandling inom områden som faller inom EU:s kompetens. Genom dataskyddslagen har tillämpningsområdet dock utvidgats till att omfatta även områden som faller utanför förordningens område, förutom i den utsträckning andra lagar innehåller avvikande bestämmelser. På motsvarande sätt gäller NIS-lagen endast för samhällsviktiga tjänster och är subsidiär till säkerhetsskyddslagen.

Trots dessa samordningsinsatser kan det uppstå svåra gränsdragningsproblem mellan de olika regelsystemen, vilket riskerar att leda till konflikter, eller att i vart fall ge sken av konflikter. Ett exempel är vad vi kallar viktighetsparadoxen för samhällsviktiga tjänster.

Samhällsviktiga tjänster anses nödvändiga för den inre marknadens funktion och måste därför ha en hög grad av tillförlitlighet. Av denna anledning ligger det inom EU:s kompetens att reglera samhällsviktiga tjänster, vilket för svenskt vidkommande genomförts i NIS-lagen.

Om en samhällsviktig tjänst är så viktig att en antagonistisk handling skulle kunna medföra skadekonsekvenser på nationell nivå, blir det istället en fråga om Sveriges säkerhet.[295] Nationell säkerhet faller utanför EU:s kompetens och kan därför, utan regelkonflikt, regleras av säkerhetsskyddslagen. Detsamma gäller i fråga om mindre viktiga tjänster, som inte har någon större betydelse för den inre marknadens funktion och därför ligger utanför EU:s kompetens.

Det sagda innebär att om en tjänst eller verksamhet är lite viktig, regleras den på nationell nivå. Om den är samhällsviktig, utan att vara så viktig att den är relevant för Sveriges säkerhet, regleras den av NIS-lagen. Om tjänsten eller verksamheten är så viktig att den har betydelse för Sveriges säkerhet ur ett nationellt perspektiv, regleras den istället av säkerhetsskyddslagen.

Det svåra är inte att navigera mellan olika regelsystem, eftersom NIS-lagen är subsidiär till säkerhetsskyddslagen. Utmaningen ligger istället i att avgöra *verksamhetens betydelse för samhället*. Är den tillräckligt viktig för NIS-lagen? Är den för viktig för NIS-lagen?

7.2.3 SKYDDSOBJEKT OCH SKYDDSINTRESSEN

Som vi redogjort för, har säkerhetsskyddslagen, NIS-lagen och dataskyddsförordningen olika skyddsobjekt och skyddsintressen. Detta kan leda till att regelverken krockar i de delar de är parallellt tillämpliga.

Ett sådant exempel är loggning av användare i it-system. Många gånger

295 Prop. 2017/18:89 s. 44.

finns en önskan om, och ett behov av, att på en mycket detaljerad nivå kunna logga vad användare i it-systemet gör, och att spara dessa loggar för framtida utredningar. En alltför omfattande loggning (och inte minst en för väl tilltagen lagringstid för sådana loggar) är dock svår att förena med dataskyddsförordningens krav på hur personuppgifter ska behandlas. Två olika skyddsintressen, it-systemens integritet och användarnas personliga integritet, ställs därför mot varandra, utan att en ”lösning” erbjuds i lagstiftningen.

Detta ställer höga krav på den som utformar loggningen. Syftet med loggningen måste vara tydligt fastställt på förhand och loggningen ska bara avse sådant som faktiskt är nödvändigt för att uppnå detta syfte. En organisation kan inte logga information som förvisso inte behövs för skydda it-systemen, men som kan vara användbar i andra sammanhang. Sådan tillkommande insamling av personuppgifter måste i så fall vila på ett självständigt, tydligt avgränsat ändamål. Med andra ord, det går inte att passa på att logga ytterligare information än den nödvändiga för det aktuella ändamålet.

Ett liknande exempel är säkerhetsprövningar enligt säkerhetsskyddslagen, som kan kräva att integritetskänsliga personuppgifter samlas in i relativt stor omfattning. Här ställs Sveriges säkerhet mot den enskildes personliga integritet. I exemplet hamnar regelverkens respektive skyddsintresse i konflikt med varandra, där en omfattande utredning i den enskildes personliga integritet anses vara nödvändig för att säkerställa Sveriges säkerhet. Konflikten mellan regelverkens skyddsintressen hanteras genom att Säkerhetsskyddslagen innehåller vissa bestämmelser om personuppgiftsbehandling för säkerhetsprövningar samt har kompletterats med lag (2019:1182) om Säkerhetspolisens behandling av personuppgifter. Detta visar ändå på vikten av att vara medveten om personuppgiftsbehandlingen även i fråga om säkerhetsskydd, eftersom möjligheten att genomföra säkerhetsprövningar varierar beroende på den aktuella säkerhetsklassen.

7.2.4 PROCESSER FÖR INFORMATIONSSÄKERHETSARBETE

I den utsträckning de olika regelverken innehåller detaljerade bestämmelser avseende en process för informationssäkerhetsarbete uppstår risken för regelkonflikter, exempelvis vad gäller vilka nivåer som ska användas för informationsklassificering eller hur en riskanalys ska göras.

Här bör särskilt nämnas säkerhetsskyddsregleringens detaljerade bestämmelser för hur en säkerhetsskyddsanalys ska genomföras, som begränsar utrymmet att göra analysen på något annat sätt. Särskilt bör uppmärksammas att det i säkerhetsskyddsanalysen används ett konsekvensperspektiv för att hantera identifierade risker, vilket innebär att man mer ensidigt fokuserar på konsekvensen av en eventuell skada och inte på samma sätt beaktar sannolikheten för att skadan inträffar.[296] Det är inte heller möjligt att väga sannolikheten för skada

296 Säkerhetspolisen, *Vägledning i säkerhetsskydd – Säkerhetsskyddsanalys*, s 5.

mot kostnaden för åtgärder och välja att avstå från vissa åtgärder, eftersom skyddet för en säkerhetskänslig verksamhet ska vara detsamma oavsett vem som är verksamhetsutövare – utrymmet för att själv välja vad som är en lämplig skyddsnivå är, med andra ord, begränsat.[297] Även vilka skyddsåtgärder som ska tillämpas är fastslaget i lagstiftningen i högre grad en för andra regleringar, vilket också minskar utrymmet för verksamhetsutövaren att själv utforma skyddet (se vidare avsnitt 7.3.5 nedan).

7.2.5 GRÄNSSNITTET MOT MYNDIGHETER

Det finns en större risk för en direkt konflikt mellan regelsystemen i de delar regelverken reglerar gränssnittet mot myndigheter. Dessa problem drabbar aktörer som bedriver verksamhet som inte enbart faller under ett enda regelverk. Detta blir särskilt problematiskt om t.ex. ett visst incidentrapporterings- eller samrådsförfarande ska användas, framför allt när det förekommer bestämmelser om tystnadsplikt i samband med incidenter.[298] Ett sådant exempel är situationer där säkerhetsskyddslagens bestämmelser om tystnadsplikt förhindrar en aktör att genomföra ett samråd eller en konsekvensbedömning enligt dataskyddsförordningen.

I sammanhanget är det även relevant att återkomma till SOU 2018:82, där det föreslås sanktionsavgifter i säkerhetsskyddslagen. Enligt utredningen finns det ett behov av att komplettera tillsynsmyndigheternas beslut om sanktionsavgifter med en möjlighet att jämka och/eller efterge sanktionsavgifterna. Anledningen till detta, menar utredningen, är att det kan uppstå situationer där en verksamhetsutövare riskerar att *"drabbas av sanktionsavgift enligt något annat regelverk för i princip samma brist. Bestämmelser om säkerhetsåtgärder och sanktionsavgifter för den som bryter mot dessa bestämmelser finns t.ex. i [...] dataskyddsförordningen och dataskyddslagen, NIS-lagen samt i speciallagstiftning i de olika sektorerna"*. Till förtydligande kan nämnas att dessa situationer inte faller in under subsidiaritetsbestämmelserna, eftersom det i så fall inte hade behövts någon jämknings- eller eftergiftsmöjlighet för tillsynsmyndigheten.

En och samma brist kan i så fall leda till beslut om sanktionsavgift enligt såväl säkerhetsskyddslagen som dataskyddsförordningen eller NIS-lagen. En sådan ordning innebär även att det kan pågå parallella tillsynsärenden utan någon skyldighet för tillsynsmyndigheterna (för det fallet det är olika) att samordna tillsynen. I vissa situationer kan det dock vara motiverat med parallella tillsynsärenden, särskilt när det är fråga om olika skyddsobjekt och/eller skyddsintressen, t.ex. personuppgiftsbehandling och säkerhetsskydd.

297 Säkerhetspolisen, *Vägledning i säkerhetsskydd – Introduktion till säkerhetsskydd*, s. 10.

298 Det ska noteras att 1 kap. 4 § dataskyddslagen inte ger säkerhetsskyddslagen företräde i fråga om konsekvensbedömningar och samrådsskyldigheten.

7.3 En modell för samordnad juridisk informationssäkerhet

7.3.1 ALLMÄNT

Under de senaste åren har många organisationer haft anledning att se över sina respektive organisationers hantering av särskilt personuppgifter. Detta har ofta resulterat i någon form av ”GDPR-projekt” där befintlig och planerad personuppgiftsbehandling har inventerats och stämts av mot dataskyddsförordningens krav, vilket i många fall krävt att även it-säkerhetsaspekterna av personuppgiftsbehandlingen har bedömts utifrån de krav som dataskyddsförordningen ställer.

Den nya säkerhetsskyddslagen, NIS-regleringen och sektorsspecifik lagstiftning har lett till att organisationer i ökad utsträckning ställs inför frågor hur man kan bäst kan säkerställa sin regelefterlevnad även på dessa områden.

Vidare har många, särskilt större organisationer, även infört någon typ av ledningssystem för informationssäkerhet (LIS) – ibland vid sidan av andra ledningssystem för exempelvis kvalitet och arbetsmiljö. Detta arbete drivs vanligtvis inte från juristavdelningen, även om juridisk kompetens förhoppningsvis finns representerad i de arbetsgrupper som ansvarar för ledningssystemet.

Det finns därför ett behov av att samordna arbetet med att säkerställa att alla tillämpliga lagar följs tillsammans med organisationens eget informationssäkerhetsarbete på ett sådant sätt att ett helhetsperspektiv uppnås.

7.3.2 LEDNINGSSYSTEM OCH REGLERADE INFORMATIONSSÄKERHETSPROCESSER

Som vi har varit inne på i tidigare avsnitt innehåller de olika regelsystemen inte bara lösa krav på säkerhetsåtgärder. I större eller mindre utsträckning krävs även att man arbetar med informationssäkerheten på vissa sätt (reglerade informationssäkerhetsprocesser).

I ett LIS (se avsnitt 1.5 ovan) ingår att man beaktar vilka rättsliga krav som finns på verksamheten. Exempelvis framgår av de krav som ISO/IEC 27001 ställer att organisationen ska bestämma vilka intressenter som är relevanta för det LIS man utformar, och vilka av dessa intressenters krav som är relevanta för informationssäkerhet. Som en anmärkning anges att berörda parters krav kan inkludera rättsliga och regelmässiga krav och avtalsförpliktelser.[299] Enligt MSB:s metodstöd ska en organisation i analysfasens omvärldsanalys bl.a. identifiera vilka rättsliga krav som är viktiga för informationen och beakta dessa vid

299 Avsnitt 4.2 i SS-EN ISO/IEC 27001:2017.

utformningen.[300] Det går därför att argumentera för att det juridiska arbetet med informationssäkerhet kan och ska utföras som en del i ett större ledningssystem.

För en jurist kan det dock vara naturligare att börja med lagstiftningens egen systematik, eftersom lagstiftningen sällan är strukturerad i form av fristående och välavgränsade krav som kan lyftas in i en omvärldsanalys. Detta gäller särskilt för sådana regleringar som har reglerade informationssäkerhetsprocesser. Vi har beskrivit de tre centrala regleringarnas bestämmelser på detta område under den återkommande rubriken Process (med underrubrikerna Identifiering, Analys, Utformning, Tillämpning och Uppföljning) i avsnitt 2–4 och i viss mån i avsnitt 5 ovan.

Vad gäller NIS-regleringen har av avsnitt 3.3 ovan framgått att denna endast innehåller generella krav hur informationssäkerhetsarbetet ska bedrivas, där det huvudsakliga kravet är att det ska finnas ett strukturerat och riskbaserat informationssäkerhetsarbete. De mer detaljerade kraven som ställs (framförallt i MSB:s föreskriver om informationssäkerhet för leverantörer av samhällsviktiga tjänster, MSBFS 2018:9) harmonierar i stor utsträckning med ISO 27000-serien. Att arbeta med informationssäkerhet enligt NIS-regleringen är därmed att arbeta med ett LIS.

Dataskyddslagstiftningen och säkerhetsskyddslagen har däremot mer detaljerad reglering av hur informationssäkerhetsarbetet ska bedrivas. Det är därför lämpligt att man i ett inledande steg försöker tillämpa dessa krav på verksamhetens informationshantering i sin helhet. Detta kan medföra att man får behandla vissa informationssystem eller informationsmängder flera gånger – en gång ur personuppgiftsperspektiv, en gång ur säkerhetsskyddsperspektiv och kanske även ur ett generellt informationssäkerhetsperspektiv.

Det är värt att understryka att det inte finns någon konflikt mellan detta synsätt (att utgå från lagstiftningen) och synsättet i ett traditionellt LIS (att utgå från verksamhetens processer och informationstillgångar). Införande av ledningssystem kräver inte att man följer en viss standard. Det metodstöd för systematiskt informationssäkerhetsarbete som MSB tagit fram (se avsnitt 1.5.1 ovan) kan i många sammanhang vara ett fullgott stöd för att införa ett LIS som också beaktar lagstiftningens reglerade informationssäkerhetsprocesser. Om man istället använder ISO 27000-serien bör man särskilt uppmärksammas att denna standard är utformad för att göra det möjligt att i ett sammanhållet ledningssystem kunna lägga till sektorsspecifika krav. Det finns också en tilläggsstandard (ISO/IEC 27701:2019) för att även hantera personuppgiftsfrågor och på så sätt utöka ett LIS till ett LISD (ledningssystem för informationssäkerhet och dataskydd). Även andra former av ledningssystem kan anpassas för att tillgodose de externa och föränderliga krav som följer av lagstiftning.

---

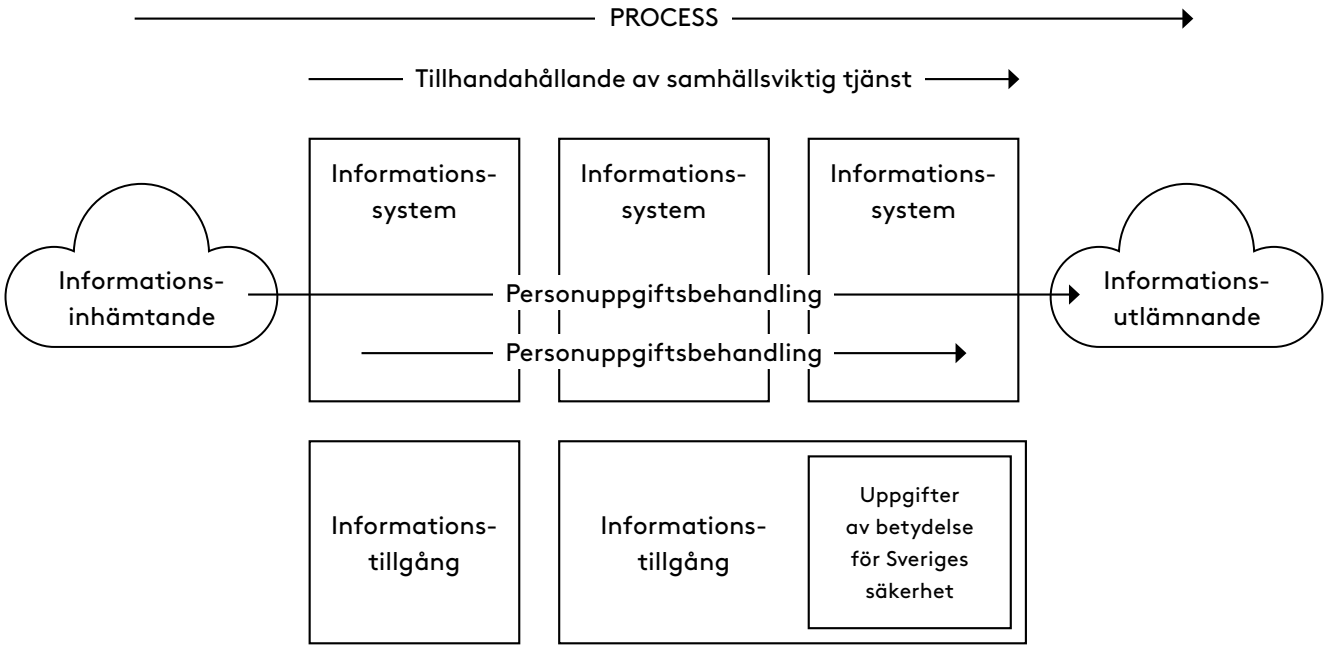
300 Se Informationssäkerhet.se, *Metodstödet – Analysera*, publicerad den 9 februari 2018, senast reviderad den 28 februari 2018, https://www.informationssakerhet.se/metodstodet/analysera/. Läst den 24 februari 2020.

7.3.3 AVGRÄNSNINGAR OCH INLEDANDE ANALYS

Identifieringssteget i de olika modellerna för ledningssystem handlar om att hitta och avgränsa de system, informationsmängder m.m. som ska skyddas (skyddsintressen). Redan i identifieringssteget måste det göras en bedömning av vilken reglering som kan komma att bli tillämplig. Det handlar helt enkelt om att utöver den informations- eller processinventering som måste göras, även analysera dataskyddsförordningens, NIS-lagstiftningens och säkerhetsskyddslagstiftningens tillämpningsområden, och i vilken mån dessa träffar den verksamhet som bedrivs. Om verksamheten faller in under något av de områden som omfattas av sektorspecifik reglering får man naturligtvis göra en bedömning av även sådan reglering.

Det är inte ovanligt att fler än endast en lag är tillämplig på en viss verksamhet. Som exempel kan nämnas att det, utifrån vår erfarenhet, är mer regel än undantag att säkerhetskänslig verksamhet eller samhällsviktiga tjänster på ett eller annat sätt även behandlar personuppgifter.

De olika regleringarnas tillämpningsområden låter sig inte alltid inordnas i verksamhetens processer, informationstillgångar eller informationssystem. Nedanstående bild illustrerar en komplex verksamsamhet där en viss verksamhetsprocess, som syftar till att leverera en samhällsviktig tjänst, använder sig av flera olika informationssystem som i sin tur använder olika informationstillgångar i form av exempelvis kund- och ärendedatabaser. Inom ramen för verksamhetsprocessen förekommer även flera olika personuppgiftsbehandlingar med olika ändamål. Slutligen förkommer det i en av databaserna ett fåtal poster som innehåller uppgifter av betydelse för Sveriges säkerhet.



Om man i den inledande analysen endast utgår från verksamhetsprocesser eller informationstillgångar uppstår en risk för att hela bilden av den personuppgiftsbehandling eller säkerhetskänsliga verksamhet som förekommer skyms bakom de enskilda processerna eller informationstillgångarna.

7.3.4 REGLERADE INFORMATIONSKLASSIFICERINGAR

I analysfasen ingår ett steg som vanligtvis kallas för informationsklassning. I tre av de regleringar som vi gått igenom i denna rapport finns det inbyggda modeller för informationsklassificering.

Dataskyddsförordningen tillsammans med den svenska dataskyddslagen gör skillnad på anonym information, ordinära personuppgifter samt känsliga personuppgifter (eller ”särskilda kategorier av personuppgifter”, som benämningen lyder i dataskyddsförordningen). Utöver detta har Datainspektionen i praxis och vägledning även definierat en kategori benämnt ”integritetskänsliga personuppgifter” för uppgifter som är extra skyddsvärda.[301]

Säkerhetsskyddslagen (som benämner detta steg ”säkerhetsskyddsklassificering”) kräver i sin tur att uppgifter klassificeras som antingen kvalificerat hemliga, hemliga, konfidentiella eller begränsat hemliga, utifrån vilken skada ett röjande av uppgifterna kan medföra på Sveriges säkerhet (se vidare avsnitt 2.3.2 ovan).

För verksamheter som tillämpar TF och OSL (se avsnitt 5.9 ovan) tillkommer utmaningen att allmänna handlingar, och den information som finns i dessa, ska lämnas ut till den som begär det, såvida inte någon sekretessreglering är tillämplig i den specifika situationen. De sekretessregleringar som finns i OSL kan i grova drag delas upp i sådana med rakt skaderekvisit (även kallat svag sekretess), omvänt skaderekvisit (stark sekretess) och absolut sekretess. Bedömningen görs utifrån det intresse som sekretessregeln avser att skydda (exempelvis den enskildes personliga integritet, en näringsverksamhets ekonomiska intresse, eller Sveriges säkerhet) och huruvida ett utlämnande kan anses leda till skada på detta intresse (med undantag för absolut sekretess, där man inte gör någon bedömning av en eventuell skada). Detta utgör också en form av reglerad informationsklassificering där uppgifter ska ha olika grad av skydd mot det röjande som ett utlämnande av en allmän handling innebär.

För NIS-lagstiftningen finns dock inte några sådana fasta kategorier. Istället finns regerat att en leverantör som omfattas av lagstiftningen ska klassa informationen med utgångspunkt i vilka konsekvenser som kan uppkomma vid brister i konfidentialitet, riktighet och tillgänglighet, där ”informationsklassning” är definierat som att genom

301 Datainspektionen, Dataskyddsförordningen – Detta är känsliga personuppgifter, under rubriken ”Andra personuppgifter kan också vara skyddsvärda”, https://www.datainspektionen.se/lagar-regler/dataskyddsforordningen/kansliga-personuppgifter/detta-ar-kansliga-personuppgifter/. Läst den 24 februari 2020.

konsekvensanalys identifiera skyddsbehovet för en viss typ av information.[302] Lagstiftningen kräver alltså att man använder en generell informationsklassificeringsmodell. I MSB:s metodstöd för ett strukturerat och riskbaserat informationsarbete finns en sådan modell som kan användas (se avsnitt 3.3.2 ovan för en närmre redogörelse).

Vi vill även tillägga att oavsett om man använder en generell informationsklassificeringsmodell för att det krävs enligt NIS-regleringen, eller för att den tillämpas i ett LIS av andra orsaker, så är det möjligt och ofta lämpligt att låta den reglerade informationsklassificeringen enligt dataskyddsregleringen och säkerhetsskyddslagstiftningen påverka denna informationsklassificering. Om MSB:s modell för informationsklassning används, kan det övervägas att alltid låta en känslig personuppgift omfattas av en högre skyddsnivå för konfidentialitet. En generell informationsklassificeringsmodell kan dock aldrig ersätta en lagreglerad, och framförallt inte en sådan modells koppling till lagreglerade skyddsåtgärder (se avsnitt 7.3.5 nedan). Detta är särskilt viktigt för säkerhetsskyddsklassificerade uppgifter.

7.3.5 MINIMIÅTGÄRDER

Syftet med alla typer av informationsklassificeringar är att, tillsammans med riskanalys, utgöra underlag för beslut om vilka säkerhetsåtgärder som ska vidtas. För dataskydd och säkerhetsskydd har lagstiftaren i viss utsträckning redan på förhand tagit beslut om vissa av sådana åtgärder (genom bemyndigande till de olika tillsynsmyndigheterna).

Vi har kallat dessa reglerade säkerhetsåtgärder för minimiåtgärder, eftersom lagstiftningen vanligtvis inte hindrar att man utöver de reglerade åtgärderna även vidtar ytterligare säkerhetsåtgärder. Dessa åtgärder framgår av de avsnitt som har rubriken Informationssäkerhetskrav i avsnitt 2–4 ovan. För dataskyddsförordningen bör även här uppmärksammas att det är svårt att fastställa minimiåtgärder i betydelsen ”åtgärder som måste vidtas” eftersom det i slutändan är den personuppgiftsansvarige som utifrån de risker som följer av behandlingen – inte bara vilka typer av uppgifter som ingår i behandlingen – bestämmer vilka tekniska och organisatoriska skyddsåtgärder som är lämpliga.

När en reglering föreskriver att en viss säkerhetsåtgärd ska vidtas är det vanligast att åtgärden ska vidtas för verksamheten som helhet eller i vart fall för all informationshantering som faller inom lagstiftningens tillämpningsområde. Ett exempel är dataskyddsförordningens krav på att säkerställa att varje person som får tillgång till personuppgifter, endast behandlar dessa på instruktion från den personuppgiftsansvarige (artikel 34.4) – det finns ingen avgränsning till bara en viss typ av personuppgifter, utan kravet på säkerhetsåtgärd gäller generellt.

302 4 och 8 §§ MSBFS 2018:8.

I vissa fall har det dock ställts krav på säkerhetsåtgärder utifrån vilken klassning som gjorts. Ett tydligt exempel är 4 kap. 21 § 1 st. PMFS 2019:2 som bara gäller uppgifter som klassificerats som hemliga eller kvalificerat hemliga (de två högsta säkerhetsskyddsklasserna). När ett informationssystem hanterar sådana uppgifter krävs en säkerhetsåtgärd i form av fysisk separation från informationssystem eller nätverk som inte omfattas av motsvarande krav.

Ytterligare ett exempel, som inte utgör ett författningsreglerat krav i formell bemärkelse, är Datainspektionens riktlinjer om att, när man måste använda e-post för integritetskänsliga eller känsliga personuppgifter (se ovan om möjliga klassificeringar av personuppgifter), använda kryptering så att endast den avsedda mottagaren kan ta del av uppgifterna.[303]

7.3.6 SAMORDNADE ÅTGÄRDER

I nedanstående figur ger vi ett exempel på hur man kan samordna olika regleringars informationsklassificeringar för att ta reda på minimiåtgärder. I exemplet går vi igenom den information som behandlas för att kunna lämna ut en lönespecifikation till en anställd. Av en sådan framgår typiskt sett den anställdes inkomst, eventuell sjukfrånvaro, utbetalade traktamenten och den anställdes namn.

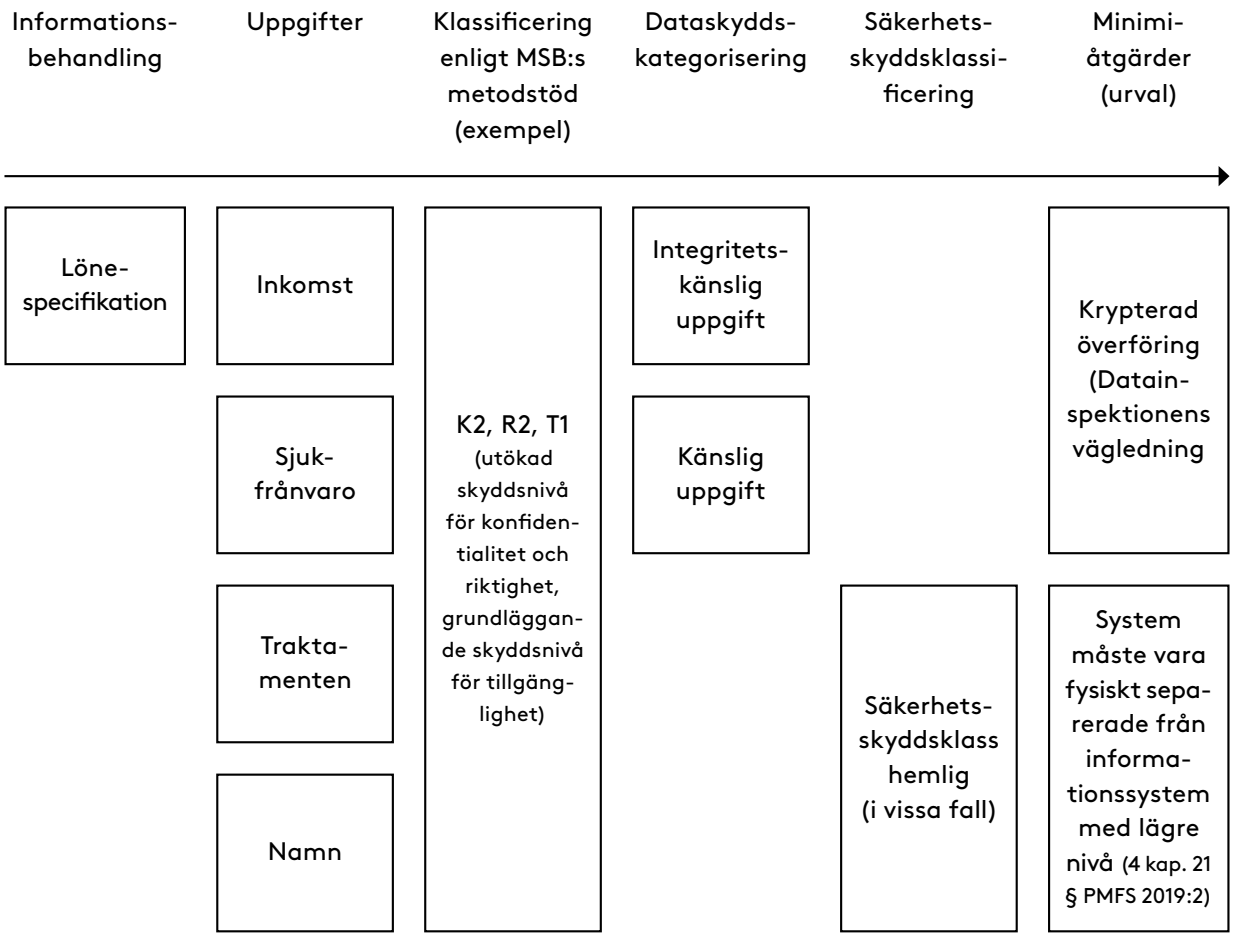
Utifrån ett generellt informationssäkerhetsperspektiv är det uppgifter där konfidentialiteten och riktigheten typiskt sett är av stor vikt, och förlust av desamma skulle, enligt en bedömning, kunna innebära betydande negativ påverkan för den enskilde. Förlust av tillgänglighet (främst i form av att informationen förmedlas till den anställde i rätt tid) är kanske inte av samma betydelse och medför endast måttlig negativ påverkan för den enskilde. Enligt den informationsklassningsmodell som ingår i MSB:s metodstöd ska då informationen ha en grundläggande skyddsnivå vad gäller tillgänglighet, men en utökad skyddsnivå vad gäller konfidentialitet och riktighet. Vi vill understryka att detta är ett exempel på en bedömning och att man mycket väl kan komma att vikta betydelsen av de olika skyddsegenskaperna annorlunda i sin egen verksamhet.

Från dataskyddsperspektiv utgör uppgifter om sjukfrånvaro känsliga personuppgifter. Uppgifter om inkomst har, som vi nämnt ovan, ofta betraktats som en form av integritetskänsliga uppgifter.

Från säkerhetsskyddsperspektiv är normalt sett uppgifter i en lönespecifikation inte alls av betydelse för Sveriges säkerhet. Den kan dock under vissa mycket specifika omständigheter avslöja sådan information. Om vi tänker oss att identiteten på vissa personer inom ett spe-

303 Detta krav framgår alltså inte direkt av dataskyddsförordningen eller svensk lagstiftning som antagits i anslutning till denna. Vägledningen får istället anses fylla ut och precisera kraven på att vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken (artikel 32.1). Det torde finnas utrymme att välja en annan säkerhetsåtgärd än just kryptering så länge som åtgärden i samma utsträckning säkerställer att endast den avsedda mottagaren kan ta del av uppgifterna.

cialförband omfattas av försvarssekretess (15 kap. 2 § OSL), men det är känt att förbandet utfört en operation inom ett visst lands territorium under en viss tidpunkt, kan en lönespecifikation som anger traktamente för vistelse inom det territoriet under samma tidpunkt avslöja identiteten på personerna som ingår i förbandet. Vidare så antar vi att röjande av dessa identiteter bedöms kunna medföra betydande negativa konsekvenser för den nationella förmågan inom avgränsade funktioner som är svårt att återställa. Enligt säkerhetspolisens vägledning skulle detta tala för att just dessa uppgifter är i säkerhetsskyddsklassen hemlig.[304]



Genom de förteckningar över reglerade minimiåtgärder som finns under rubriken Säkerhetsåtgärder i avsnitt 2–4 ovan kan man sedan ta fram en sammanlagt lista på säkerhetsåtgärder som måste tillämpas.

De olika reglerade säkerhetsåtgärder som vi benämnt minimiåtgärder har visst överlapp med varandra och även med säkerhetsåtgärder som framgår av olika skyddsåtgärdskataloger (bl.a. bilaga A till ISO/IEC 27002). Exempelvis förekommer i en eller annan form krav på kryptering

304 Säkerhetspolisen, *Vägledning i säkerhetsskydd – informationssäkerhet*, s. 9.

eller behörighetsstyrning i flera regleringar. Kraven är dock inte samordnade och skiljer sig mycket i detaljeringsgrad och tillämpningsområde. Det finns till exempel ett allmänt dataskyddsrättsligt krav på kryptering vid överföring av vissa uppgifter, medan det finns säkerhetsskyddsreglerade krav som även omfattar kryptering av lagrade uppgifter – men som är begränsade till att verksamheten själv ska analysera behovet av sådan kryptering.

De säkerhetsåtgärder som är reglerade i säkerhetsskyddsslagstiftningen är, särskilt för uppgifter i de högre säkerhetsklasserna, väldigt krävande. Om man har en verksamhet där bara vissa uppgifter omfattas av säkerhetsskyddet (exempelvis tio poster i en databas där de övriga tusentals uppgifterna inte är säkerhetsskyddsklassificerade) kan dessa rättsliga krav ibland göra det nödvändigt att lyfta ut uppgifterna från det större systemet och hantera dessa separat. Vid en sådan åtgärd bör man dock analysera om frånvaron av vissa uppgifter i systemet i sig kan avslöja uppgifter som i sig är säkerhetsskyddsklassificerade.

Slutligen ska sägas att det finns ett mellanting mellan de skyddsåtgärder som man måste vidta enligt lagstiftningen, och de skyddsåtgärder som man självständigt vidtar efter en informationsklassificering efter egna kriterier, nämligen sådana skyddsåtgärder som följer av branschpraxis (inklusive best practices och uppförandekoder).

7.3.7 ÖVRIGA REGLERADE INFORMATIONSSÄKERHETSPROCESSER

Utöver de reglerade kraven på informationsklassning och sammanhängande krav på skyddsåtgärder finns även reglerade krav på andra delar av processen. I sammanhanget ska understrykas att säkerhetsskyddslagstiftningen har relativt detaljreglerade krav på processen, inom begreppet säkerhetsskyddsanalys. Detta begrepp är brett och innefattar såväl identifierings av skyddsobjekt som utformning av skyddsåtgärder.

Vår bedömning är att så länge en aktör beaktar de enskilda krav som följer av säkerhetsskyddsregelverket finns inga hinder mot att göra en säkerhetsskyddsanalys inom ramen för ett kombinerat ledningssystem för informationssäkerhet. Man bör dock vara medveten redan vid införandet (av ledningssystemet) att säkerhetsskyddsanalysen är en relativt detaljreglerad process. För en verksamhet som hanterar både säkerhetskänslig verksamhet och annan verksamhet, innebär detta att vissa delar av analysen måste dokumenteras och fastställas i särskild ordning.

Vi bedömer inte att det är lämpligt att tillämpa metodiken för säkerhetsskyddsanalys på information och verksamhet som i sig inte faller under säkerhetsskyddslagen, inte heller för de ingående delarna informationsklassificering och riskanalys. Säkerhetsskyddslagen har sitt eget system med fasta kategorier för säkerhetsskyddsklassificering och konsekvensnivåer som är utformade efter vilken skada som kan

ske på Sveriges säkerhet, vilket inte är lämpligt att använda för sådan verksamhet som inte har betydelse för Sveriges säkerhet.

Även dataskyddsregleringen har vissa krav ytterligare på hur processen ska gå till. Vi har nämnt dessa i avsnitt 4.3 ovan och vill här bara uppmärksamma kraven på att en personuppgiftsansvarig ska föra ett register över personuppgiftsbehandlingar som sker under dennes ansvar (artikel 30 dataskyddsförordningen), och att för vissa behandlingar som typiskt sett medför en stor risk för de registrerade utföra en konsekvensbedömning (artikel 35 dataskyddsförordningen). Även dessa krav är utformade utifrån dataskyddsregleringen.

8. Slutkommentar

8.1 Allmänt

Såväl den svenska som den europeiska lagstiftaren har hanterat majoriteten av de frågor och områden där regelverkens olika skyddsintressen och -objekt potentiellt kunnat leda till direkta regelkonflikter. Det är tydligt att säkerhetsskyddslagen ska ha företräde framför NIS-lagen, och dataskyddslagen anger att avvikande bestämmelser om personuppgiftshantering i andra lagar ska ha företräde.

Det finns dock vissa situationer där samtliga tre regelverk är tillämpliga på en viss verksamhet inom en organisation. Det kan röra informationssystem för leverans av samhällsviktiga tjänster som innehåller personuppgifter och där vissa uppgifter även har betydelse för Sveriges säkerhet. I större utsträckning, fortfarande som ett tydligt undantag, förekommer det att två regelverk är tillämpliga samtidigt och står i konflikt med varandra. Den vanligaste situationen är att dataskyddsförordningen är tillämplig tillsammans med antingen säkerhetsskyddslagen eller NIS-lagen, och att någon av de sistnämnda ställer krav på personuppgiftsbehandling som inte är helt förenlig med dataskyddsförordningen.

Vi menar dock att det många gånger är möjligt att hantera de konflikter som faktiskt kan uppstå. Att säkerhetsskyddslagen ställer krav på integritetskänslig och omfattande personuppgiftsbehandling kan vid en första anblick stå i konflikt med dataskyddsförordningens skyddsintresse, men samtidigt är behandlingen nödvändig och reglerad i lag. Om den personuppgiftsansvarige därtill vidtar ytterligare säkerhetsåtgärder för att minimera intrånget i den enskildes personliga integritet blir det särskilt tydligt att de olika skydden går att förena. Många gånger ter det sig till och med naturligt. Det ligger i säkerhetsskyddslagens anda att begränsa tillgången till de personuppgifter som samlas in, eftersom det finns ett intresse av att så få som möjligt ska känna till vilka som arbetar inom säkerhetskänsliga verksamheter. Det skapar incitament till tillgångsbegränsning, som i sin tur kan utgöra en skyddsåtgärd för personuppgiftsbehandlingen utifrån dataskyddsförordningens perspektiv.

Sammanfattningsvis anser vi att konfliktytor förekommer, men att de som regel går att hantera genom en medvetenhet om dels regelverken som sådana, dels om verksamheten. Med det sagt, är det ingen enkel uppgift att navigera mellan olika skyddsintressen, särskilt som skiljelinjerna mellan de olika regelverken kan vara svåra att se.

8.2 Principen om den mest krävande lagstiftningen

Som vi varit inne på är de informationssäkerhetsåtgärder som lagstiftningen ställer krav på sällan i konflikt, även om viss lagstiftning kan gå längre än annan. Som grundprincip, både när man identifierar krav på säkerhetsåtgärder, men även närliggande frågor om process, dokumentation, eller annat, bör man kunna utgå från den lagstiftning som ställer de mest långtgående och/eller detaljerade kraven. Den modell för en samordnad juridisk informationssäkerhet som vi beskriver i föregående avsnitt kan hjälpa med att hitta dessa krav och framförallt samordna de reglerade skyddsåtgärderna.

8.3 Helhetsperspektiv på verksamhetens informationssäkerhet

Vi har i denna rapport återkommit till att regleringen av informationssäkerhet kommer från många håll, tar sikte på olika skyddsintressen och är olika konstruerad vad gäller exempelvis vilka tillsynsmyndigheter som är ansvariga och deras respektive mandat. Detta leder till att mycket information och vägledningar är skrivna utifrån ett visst regelsystem och bara i undantagsfall hanterar verksamhet som hamnar inom flera olika regelsystems tillämpningsområde.

Oavsett vilka regelsystem som är tillämplig på en verksamhet anser vi att det är nödvändigt med ett helhetsperspektiv på regleringen av informationssäkerhet, och att arbetet med regelefterlevnad på informationssäkerhetsområdet inte bara utgår från ett av regelsystemen om flera är tillämpliga. Ett sådant helhetsperspektiv är också en nödvändig grund för ett mer heltäckande strukturerat informationssäkerhetsarbete som kan hantera såväl lagstiftningens som verksamhetens egna krav.

Vi hoppas att denna rapport kan vara ett steg på vägen till ett sådant helhetsperspektiv.

Om Advokatfirman Kahn Pedersen

Kahn Pedersen är en advokatbyrå helt inriktad på specialiserad affärsjuridik. Vi åtar oss uppdrag enbart inom våra två verksamhetsområden Digital och Public. Se www.kahnpedersen.se för mer information om vår verksamhet.

Författarna till denna rapport är:

Karolina Kjellberg, Associate.

Lisa Lindeberg Sandahl, Associate.

Staffan Malmgren, Legal Technology Officer.

Albin Svensson, Associate.

Vi vill varmt tacka André Catry, Fia Ewald och Kim Hakkarainen[305] för deras ovärderliga insatser med att granska och kommentera ett utkast till denna rapport. Eventuella kvarvarande misstag är våra egna.

305 Kim Hakkarainen i egenskap av privatperson.

www.kahnpedersen.se

ISBN 978-91-983215-8-6