IAM Strategi

Med kommunernas behov i fokus

Bilaga 1 – Regulatoriska krav

inera

Innehåll

1. Regulatoriska åtkomstkrav ur ett kommunalt perspektiv

De regulatoriska kraven med avseende på IAM har sammanställts nedan. Det är inte uttömmande förteckning utan syftar till att ge en bild av utmaningen att hantera IAM i en kommun även ur regulatoriskt perspektiv.

1.1 Dataskyddsförordningen (EU 2016/679)

Artikel 2 - Materiellt tillämpningsområde

Artikel 4 - Definitioner

Artikel 32 - Säkerhet i samband med behandlingen

Dataskyddsförordningen är tillämplig på sådan behandling av personuppgifter som helt eller delvis företas på automatisk väg (artikel 2). Den är även tillämplig på annan behandling än automatisk behandling av personuppgifter, om dessa uppgifter ingår i eller kommer att ingå i ett register. Med ett register avses en strukturerad samling av personuppgifter som är tillgänglig enligt särskilda kriterier, oavsett om samlingen är centraliserad, decentraliserad eller spridd på grundval av funktionella eller geografiska förhållanden (artikel 4). Förordningens text har skrivits med en medvetet bred tillämpningsgrad, både vad gäller legala och tekniska krav, för att undvika att förordningen kan kringgås.

Vid alla slags personuppgiftsbehandlingar som träffas av förordningen enligt artikel 2 ovan, ska lämpliga tekniska och organisatoriska åtgärder vidtas för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken (artikel 32).

Då de flesta kommunala verksamheter får sägas behandla personuppgifter i någon mån enligt ovan, så berörs alla dessa av dataskyddsförordningens krav på att upprätthålla en säkerhetsnivå som är lämplig i förhållande till risken.

1.2 Kompletterande svensk dataskyddslagstiftning till dataskyddsförordningen

Lagen om kompletterande bestämmelser till EU:S dataskyddsförordning 2018:218 (Dataskyddslagen)

Förordning med kompletterande bestämmelser till EU:s dataskyddsförordning 2018:219

Dataskyddslagen är kompletterande reglering till dataskyddsförordningen (1 kap. 1 §). Lagen är subsidiär i förhållande till avvikande bestämmelser i annan lag eller förordning som reglerar behandling av personuppgifter. Det finns ett antal sådana avvikande bestämmelser i sektorsspecifika författningar, främst avseende hur olika myndigheter får behandla personuppgifter. En sådan lag eller förordning har dock företräde endast om den är förenlig med dataskyddsförordningen och avser en fråga som enligt dataskyddsförordningen får särregleras eller specificeras genom nationell rätt (1 kap. 6 §).

Den kompletterande svenska lagstiftningen innehåller inte ytterligare krav på autentisering utöver de krav som dataskyddsförordningen ställer.

1.3 Säkerhetsskyddslagstiftningen

Säkerhetsskyddslag (2018:585)

Säkerhetsskyddsförordning (2018:658)

Säkerhetsskyddslagen är tillämplig på alla utövare av säkerhetskänslig verksamhet, däribland även kommunala myndigheter och bolag (1 kap. 1§). Exempel på kommunala verksamheter som omfattas är energi- och/eller vattenförsörjning. Kommunala bolag och myndigheter har även till uppgift att skydda uppgifter som rör säkerhetskänslig verksamhet och som därför omfattas av sekretess enligt offentlighets- och sekretesslagen, eller som skulle ha omfattats av den lagen om den varit tillämplig.

För de kommunala bolag och myndigheter som omfattas av reglerna i säkerhetsskyddslagen och säkerhetsskyddsförordning, är även Säkerhetspolisens föreskrifter tillämpliga.

Säkerhetspolisens föreskrifter om säkerhetsskydd PMFS 2019:2, 4 kap 12 -17 §§

Alla utställda identiteter i ett informationssystem som har betydelse för säkerhetskänslig verksamhet ska vara unika över tid. Åtkomsten ska vara spårbar till individ, system eller resurs.

Verksamhetsutövaren ska tilldela sådana behörigheter som ger systemadministrativ åtkomst eller annan särskild tillgång till informationssystem som har betydelse för säkerhetskänslig verksamhet restriktivt. Behörigheterna ska vara tidsbegränsade och följas upp särskilt.

Tilldelning av behörigheter enligt första stycket som inte direkt kan kopplas till någon fysisk individ ska ske särskilt restriktivt och beslutas av säkerhetsskyddschefen eller den han eller hon bestämmer.

Verksamhetsutövaren ska se till att autentisering vid åtkomst till informationssystem som har betydelse för säkerhetskänslig verksamhet baseras på flera faktorer (flerfaktorsautentisering).

Verksamhetsutövaren ska fastställa tekniska eller administrativa regler för utformning, byte och hantering av lösenord, om sådana används för att ge tillgång till informationssystem som har betydelse för säkerhetskänslig verksamhet. Reglerna ska bl.a. innehålla bestämmelser om återanvändning av lösenord samt lösenordens längd och komplexitet.

Verksamhetsutövaren ska ge kod eller lösenord som ger tillgång till informationssystem som har betydelse för säkerhetskänslig verksamhet ett säkerhetsskydd som motsvarar det säkerhetsskydd som informationssystemet ska ha enligt skyddsdimensioneringen.

Vid användning av central funktion för identifiering eller behörighetskontroll, ska verksamhetsutövaren se till att denna funktion ges ett säkerhetsskydd som motsvarar det högsta säkerhetsskydd som de anslutna informationssystemen ska ha enligt skyddsdimensioneringen.

1.4 Lag om informationssäkerhet för vissa tillhandahållare av samhällsviktiga och digitala tjänster (NIS-direktivet)

Kommuner kan beröras av NIS-regleringen som leverantörer av samhällsviktiga tjänster, se 1 § lagen om informationssäkerhet för samhällsviktiga och digitala tjänster. Vanliga områden där kommuner levererar sådana tjänster är inom dricksvattenförsörjning, energi samt hälso- och sjukvård.

Enligt 11-12 §§ lagen om informationssäkerhet för samhällsviktiga och digitala tjänster, ska leverantörer av samhällsviktiga tjänster ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete avseende nätverk och informationssystem som de använder för att tillhandahålla samhällsviktiga tjänster.

Leverantörer av samhällsviktiga tjänster ska vidta ändamålsenliga och proportionella tekniska och organisatoriska åtgärder för att hantera risker som hotar säkerheten i nätverk och informationssystem som de använder för att tillhandahålla samhällsviktiga tjänster. Åtgärderna ska säkerställa en nivå på säkerheten i nätverken och informationssystemen som är lämplig i förhållande till risken.

Enligt 6 § förordning om informationssäkerhet för samhällsviktiga och digitala tjänster ska, vid bedömningen av om säkerhetsåtgärder enligt 15 § lagen om informationssäkerhet för samhällsviktiga och digitala tjänster säkerställer en nivå på säkerheten i nätverk och informationssystem som är lämplig i förhållande till risken, följande beaktas:

1. säkerheten i system och anläggningar,
2. incidenthantering,
3. hantering av driftskontinuitet,
4. övervakning, revision och testning, och
5. efterlevnad av internationella standarder.

1.5 MSBFS 2018:8 5-6 §§, 8 §, 10 - 11 §§ (Kompletterande föreskrift till lag om informationssäkerhet för vissa tillhandahållare av samhällsviktiga och digitala tjänster ovan)

Varje leverantör ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete med stöd av standarderna SS-EN ISO/IEC 27001:2017 och SS-EN ISO/IEC 27002:2017 om ledningssystem för informationssäkerhet eller motsvarande.

Det systematiska och riskbaserade informationssäkerhetsarbetet ska utformas och samordnas utifrån organisationens behov. Det ska vara styrande avseende informationshantering i nätverk och informationssystem som används för att tillhandahålla samhällsviktiga tjänster.

En leverantör ska ha ett dokumenterat arbetssätt för sitt informationssäkerhetsarbete som stöd för att

1. klassa information med utgångspunkt i vilka konsekvenser som kan uppkomma vid brister i konfidentialitet, riktighet och tillgänglighet,
2. identifiera, analysera och värdera risker för organisationens information, nätverk och informationssystem,
3. utifrån genomförd informationsklassning och riskbedömning införa ändamålsenliga och proportionella säkerhetsåtgärder,
4. följa upp och utvärdera säkerhetsåtgärder i syfte att vid behov anpassa skyddet av informationen, samt
5. fortlöpande dokumentera vidtagna åtgärder enligt punkt 1–4.

En leverantör ska ha interna regler och arbetssätt som säkerställer att samtliga nätverk och informationssystem för samhällsviktiga tjänster uppfyller identifierade behov av informationssäkerhet. Drift och förvaltning över tid, arkitektur samt sammankoppling mot andra nätverk och informationssystem ska särskilt beaktas. Arbetet ska dokumenteras.

En leverantör ska ha interna regler och arbetssätt för att upptäcka och vidta åtgärder för att minimera konsekvenserna av incidenter och avvikelser avseende informationshanteringen i nätverk och informationssystem som används för att tillhandahålla samhällsviktiga tjänster.

Myndigheten för samhällsskydd och beredskaps allmänna råd om informationssäkerhet för leverantörer av samhällsviktiga tjänster till 8 § om systematiskt arbetssätt:

Verksamhetens behov av spårbarhet samt äkthet och ursprung (autenticitet) hos informationen bör särskilt beaktas.

1.6 Riksarkivets föreskrifter och allmänna råd (RA-FS 2009:1) om elektroniska handlingar (upptagningar för automatiserad behandling)

Enligt Riksarkivets föreskrifter ska bevarade elektroniska handlingar skyddas från obehörig åtkomst. Skyddsåtgärder ska tas fram i enlighet med SS-ISO/IEC 27001:2006 och SS-ISO/IEC 27002:2005.

RA-FS 2009:1 6 kap. 1 §

Myndigheten ska för att säkerställa ett bevarande av de elektroniska handlingarna skapa och upprätthålla rutiner för samt vidta åtgärder för att skydda handlingarna från skada, manipulation, obehörig åtkomst och stöld. Det ska ske med utgångspunkt ur SS-ISO/IEC 27001:2006, Informationsteknik – Säkerhetstekniker – Ledningssystem för informationssäkerhet (LIS), och med stöd av riktlinjerna i SS-ISO/IEC 27002:2005, Informationsteknik – Säkerhetstekniker – Riktlinjer för styrning av informationssäkerhet.

1.7 Patientdatalag (2008:355) och kompletterande föreskrifter (HSLF-FS 2016:40, SOSFS 2008:14)

Patientdatalagen tillämpas vid vårdgivares behandling av personuppgifter inom hälso- och sjukvården, såsom exempelvis inom äldrevården i kommunen. Dessa krav omfattar t.ex. att överföring av patientuppgifter görs på ett sådant sätt att ingen obehörig kan ta del av uppgifterna, och att åtkomst till patientuppgifter föregås av stark autentisering.

PDL 4 kap. 1 §

Den som arbetar hos en vårdgivare får ta del av dokumenterade uppgifter om en patient endast om han eller hon deltar i vården av patienten eller av annat skäl behöver uppgifterna för sitt arbete inom hälso- och sjukvården.

HSLF-FS 2016:40 3 kap. 15 §

Om vårdgivaren använder öppna nät vid behandling av personuppgifter, ska denne ansvara för att 1. överföring av uppgifterna görs på ett sådant sätt att inte obehöriga kan ta del av dem, och 2. elektronisk åtkomst eller direktåtkomst till uppgifterna föregås av stark autentisering.

SOSFS 2 kap. 5 §

Om vårdgivaren använder öppna nät för att hantera patientuppgifter, ska denne ansvara för att det i ledningssystemet finns rutiner som säkerställer att 1. överföring av patientuppgifter görs på ett sådant sätt att ingen obehörig kan ta del av uppgifterna, och 2. åtkomst till patientuppgifter föregås av stark autentisering.

Socialtjänst- och LSS-lagstiftningen

De uppräknade lagarna nedan uttrycker inte några specifika, tekniska krav på autentiseringsåtgärder. Däremot hänvisar Inspektionen för vård och omsorg (IVO), tillsynsansvarig myndighet för vårdgivare i de här omnämnda lagarna, att det är Datainspektionen som har tillsyn över hur vårdgivarna tillämpar dataskyddsbestämmelser. Detta betyder att Datainspektionen kan tillsyna att en vårdgivare har vidtagit tekniska säkerhetsåtgärder, exempelvis i form av autentisering, för att skydda de personuppgifter som vårdgivaren behandlar i enlighet med dataskyddsförordningen (https://div.socialstyrelsen.se/juridiskt-stod/personuppgiftsbehandling-inom-halso-och-sjukvarden-och-socialtjansten).

Socialtjänstlag 2001:453 (SoL) och Lagen om stöd och service till vissa funktionshindrade 1993.387 (LSS)

I 1 kap. 1 § SoL och i 6 § LSS finns bestämmelser om att verksamheten ska vara grundad på respekt för den enskildes självbestämmanderätt och integritet.

11 kap. 5 § andra stycket SoL anges att handlingar ska förvaras så att obehöriga inte kan ta del av dem.

12 kap. SoL reglerar behandling av uppgifter inom Socialtjänsten. Kapitlet har ingen uttrycklig bestämmelse som rör autentisering.

Lagen om behandling av personuppgifter inom socialtjänsten 2001:454 (SoLPuL)

SoLPuL, reglerar vissa specifika förhållanden som gäller för den personuppgiftsbehandling som är nödvändig för socialtjänstens verksamheter. Lagen är en sektorsspecifik lagstiftning, som är kompletterar dataskyddsförordningen och är underordnad densamma, men den är överordnad den svenska dataskyddslagstiftningen - 4 § SoLPuL.

Enligt 11 § får regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om vilka som är personuppgiftsansvariga och om begränsning tillåtna behandlingar av personuppgifter enligt 6 § samma lag. Detsamma gäller föreskrifter om sökbegrepp, direktåtkomst och samkörning av personuppgifter. Regeringen får även meddela föreskrifter om när personuppgifter får föras över till tredje land.

Lagen har i övrigt ingen uttrycklig bestämmelse som rör autentisering.

Förordning om behandling av personuppgifter inom socialtjänsten

Lagen hänvisar i 2 § om att det existerar särskilda bestämmelser om behandling av personuppgifter i SoLPuL, i 12 kap. SoL och i LSS. Lagen har i övrigt ingen uttrycklig bestämmelse som rör autentisering.

Av 11 § framgår att en kommunal myndighet är personuppgiftsansvarig för den behandling av personuppgifter inom socialtjänsten som myndigheten utför, vilket betyder att det är denna myndighet som har skyldighet att tillse att dataskyddsförordningen följs.

1.8 eIDAS-förordningen (EU 910/2014)

En kommun kan behöva ta hänsyn till eIDAS i de fall att en kommuninvånare saknar svensk e-legitimation, men där invånaren ändå har rätt att ta del av vissa kommunala tjänster där säker identifiering krävs.

Artikel 6

När det enligt nationell rätt eller enligt nationella administrativa förfaranden krävs en elektronisk identifiering där medel för elektronisk identifiering och autentisering används för att få åtkomst till en nättjänst som tillhandahålls av ett offentligt organ i en medlemsstat, ska de medel för elektronisk identifiering som utfärdats i en annan medlemsstat erkännas i den första medlemsstaten för gränsöverskridande autentisering för den tjänsten via internet.

1.9 Offentlighets- och sekretesslag (2009:400)

OSL saknar uttryckliga bestämmelser om autentisering - men då lagen reglerar vad som utgör sekretesskyddad information inom offentlig verksamhet, får krav på någon form av autentisering anses följa sekretessen per automatik i tysthet, i det fallet att en offentlig utövare arbetar digitalt med sådan sekretesskyddad information. För att nämna några exempel på när en autentiseringslösning kan vara behövlig nämnas:

Enligt 8 kap. 2 § OSL gäller sekretess mellan olika verksamhetsgrenar inom en myndighet när de är att betrakta som självständiga i förhållande till varandra - för exempelvis myndighetsgemensamma system kan det därför behövas åtkomstbegränsningar även för internt bruk. Ett exempel på detta kan vara när en kommun har ett kommungemensamt omvårdnadssystem som delas av en social- och äldrevårdsnämnd.

Enl. OSL 15-20 kap. råder sekretess till skydd för allmänna intressen, däribland för kommunala bolag och myndigheter som har till uppgift att skydda uppgifter som rör säkerhetskänslig verksamhet (se styckena om säkerhetsskyddslagstiftningen ovan). Genom hänvisningen till säkerhetsskyddslagstiftningen ställer här OSL har indirekta krav på autentisering.

Enligt 26 kap. 1 § OSL, gäller sekretess inom socialtjänsten för en uppgift om enskilds personliga förhållanden om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon närstående till denne lider men.