Fagersta KOMMUN

Datum
2024-04-09

Ert diarienummer
Fi2024/00259

Kommunstyrelsen

Finansdepartementet

Yttrande över remiss från Finansdepartementet – En reform för datadelning (SOU 2023:96), dnr. Fi2024/00259

Fagersta kommun välkomnar initiativet och utredningen. Det finns ett stort behov av samverkan inom offentlig sektor samtidigt som också vissa sakfrågor behöver högre grad av styrning och beslut på en nationell nivå för att vi på riktigt ska kunna ta tillvara på de nyttor och möjligheter som digitaliseringen erbjuder. Utredningen gör en gedigen genomgång av tillämpningen och identifierar både möjligheter och risker på ett förtjänstfullt sätt.

Utredningens förslag skapar förutsättningar för interoperabilitet på nationell nivå. Detta är en mycket viktig fråga som kräver en samlad lösning för att undvika fragmentering och ineffektivitet.

Samtidigt vill vi lyfta fram några frågor som vi anser behöver belysas ytterligare:

Finansiering av omställningskostnader bör tydliggöras ytterligare. En övergång till interoperabla lösningar kommer att innebära kostnader för kommunerna.

Utredningens förslag är i vissa fall mjukt formulerade och saknar konkretion. Begreppet stödjande istället för styrande förekommer, vilket kan få en direkt påverkan på anslutning och/eller genomförande.

Det är avgörande att det finns en tydlig plan för hur införandet av interoperabilitetslösningar ska följas upp och hur eventuella brister ska åtgärdas och vilka konsekvenser avsteg kan få. Detta bör konkretiseras.

Sammanfattningsvis anser Fagersta kommun att förslagen i utredningen om interoperabilitet i offentlig sektor är ett steg i rätt riktning. Vi ser fram emot en fortsatt dialog och konkreta åtgärder för att realisera visionen om en mer effektiv och samverkande offentlig sektor.

Viktigt att beakta:

1. Ökad medvetenhet: Utbildning och medvetenhet är nyckeln. Alla användare bör förstå riskerna och bästa praxis för att skydda information.
2. Starka autentiseringsmetoder: Implementera starka autentiseringsmetoder, inklusive tvåfaktorsautentisering (2FA) och biometriska identifieringar.
3. Kryptering: Använd kryptering för att skydda data i vila och under överföring. Detta minskar risken för obehörig åtkomst.

Postadress: 737 80 Fagersta
Besöksadress: Bangårdsgatan 1
0223 - 440 00 växel
e-post: info@fagersta.se
hemsida: fagersta.se
Plusgiro: 12 37 80-9
Bankgiro: 547-6890
Org. nr: 212000–2106

4. Säkerhetskopior: Regelbundna säkerhetskopior är avgörande. Om data går förlorade eller skadas kan du återställa från en säkerhetskopia.
5. Sårbarhetshantering: Identifiera och åtgärda sårbarheter i system och programvara. Uppdatera regelbundet för att stänga kända säkerhetsluckor.
6. Öppenhet och samarbete: Dela information om hot och attacker med andra organisationer. Samarbeta för att förbättra säkerheten gemensamt.
7. Regelbunden översyn: Utvärdera och uppdatera säkerhetspolicyer och procedurer regelbundet. Anpassa dem efter nya hot och teknologier.
8. Fokus på mänskliga faktorer: Människor är ofta den svagaste länken. Utbilda användare om social ingenjörskonst och hur man undviker bedrägerier.
9. Lagstiftning och reglering: Följ gällande lagar och regler för informationssäkerhet. Anpassa dig till förändringar i lagstiftningen.
10. Samarbete med myndigheter: Arbeta tillsammans med myndigheter och experter för att förstå hotbilden och utveckla lämpliga skyddsåtgärder.
11. Lagstiftning är en viktig grund, men det är inte tillräckligt för att säkerställa effektiv efterlevnad och skydd av information. Det behövs ytterligare åtgärder som kan komplettera lagstiftningen:
    a) Utbilda användare om informationssäkerhet, risker och bästa praxis. Genom att öka medvetenheten minskar vi risken för oavsiktliga överträdelser.
    b) Tydliga riktlinjer för informationssäkerhet är avgörande. Användare bör veta hur de ska agera och vad som förväntas av dem.
    c) Säkerhetsmedveten kultur: Skapa en organisation där säkerhet prioriteras.
    d) Tekniska verktyg: Implementera tekniska lösningar som intrångsdetekteringssystem, kryptering, brandväggar och säkerhetsuppdateringar.
    e) Övervaka systemaktivitet för att upptäcka avvikelser. Regelbundna revisioner hjälper till att identifiera brister.
    f) Incidenthantering: Ha en plan för incidenthantering. Om en incident inträffar bör organisationen veta hur man agerar och vem som ansvarar.
    g) Sanktioner: Konsekvenser för överträdelser bör vara tydliga. Det kan innebära disciplinära åtgärder eller rättsliga påföljder.
    h) Samverkan med andra aktörer: Samarbeta med andra organisationer, myndigheter och experter. Erfarenhetsutbyte och gemensamma insatser är värdefulla.
    i) Uppföljning och utvärdering: Mät efterlevnad och effektivitet av säkerhetsåtgärder. Justera strategin vid behov.
    j) Kontinuerlig förbättring: Informationssäkerhet är en kontinuerlig process. Lär av misstag och utveckla ständigt.

Att kombinera lagstiftning med dessa åtgärder skapar en stark grund för att skydda information på ett effektivt sätt.

1. Utmaningar och åtgärder

- Standardisering: Offentliga verksamheter bör arbeta för att standardisera sina processer och metoder. Detta underlättar samarbete och effektivitet.

- Utbildning och medvetenhet: Anställda behöver utbildning om säkerhets principer och bästa praxis. Medvetenhet om risker är avgörande.
- Digitalt ledarskap: Ledare måste driva digital transformation och skapa en kultur där digitalisering prioriteras.
- Samverkan: Offentliga organisationer bör samarbeta för att dela erfarenheter och bästa praxis.

2. Ekonomiska förutsättningar

För att hantera kompetensutmaningar och skapa mer värde för invånarna krävs investeringar i digitalisering. Det är en långsiktig satsning, men den är nödvändig för att möta framtidens behov.

Sammanfattningsvis är det viktigt att offentliga verksamheter fortsätter att arbeta målinriktat med digitalisering och skapar förutsättningar för att öka nyttan. Genom samarbete, utbildning och forskning kan vi stärka den digitala mognaden och möta framtidens utmaningar.

Digitalisering är en avgörande faktor för samhällsutvecklingen, och det är viktigt att ha en nationell strategi för att hantera utmaningarna. Här är några aspekter att beakta:

1. *Nationell digitaliseringsstrategi:*
   - Sverige har nyligen tagit fram sin första nationella strategi mot organiserad brottslighet.
   - Det är också viktigt att ha en liknande strategi för digitalisering.
   - Lagstiftning är en viktig del av digitaliseringen. Den måste dock vara flexibel och anpassas till den snabba teknologiska utvecklingen.
   - Att ta bort hinder och skapa nya möjligheter genom lagstiftning är avgörande. Det handlar om att balansera skydd och innovation.
   - Samverkan mellan myndigheter, privata aktörer och forskning är nödvändig för att utveckla lämplig lagstiftning.

2. *Organiserad brottslighet:*
   - Den organiserade brottsligheten är ett allvarligt hot mot samhället. Strategier som fokuserar på att stoppa kriminella karriärer, minska tillgången på vapen och explosiva varor samt slå sönder den kriminella ekonomin är viktiga.
   - Det är också viktigt att identifiera kopplingar mellan organiserad brottslighet och andra hot, såsom våldsbejakande extremism och terrorism.

Sammanfattningsvis behöver vi en helhetsstrategi som integrerar digitalisering, lagstiftning och bekämpning av organiserad brottslighet för att skapa ett tryggare och mer effektivt samhälle.

3. Framtida hot och utmaningar

Att fundera över framtiden och hur hot kan utvecklas. När det gäller hot och utmaningar inom datadelning och informationssäkerhet finns det flera aspekter att beakta:

1. Teknologisk utveckling:
   - Ökad digitalisering kommer sannolikt att leda till fler möjligheter att dela data, men också till ökade risker för oavsiktlig eller avsiktlig exponering av känslig information.
   - Åtgärder: Fortsatt forskning och utveckling av säkerhetslösningar, inklusive kryptering, autentisering och intrångsdetektering, är avgörande.

2. Cyberhot:
   - Cyberattacker blir alltmer sofistikerade och riktade. Hotaktörer kan vara statliga aktörer, kriminella grupper eller enskilda hackare.
   - Åtgärder: Investera i cybersäkerhet, utbilda användare om säkerhetsmedvetenhet, och ha en incidenthanteringsplan på plats.

3. Lagstiftning och reglering:
   - Lagstiftning måste utvecklas för att hålla jämna steg med teknologin. Det bör vara flexibelt och anpassningsbart.
   - Åtgärder: Regelbundna översyner av lagstiftningen, samarbete med experter och myndigheter, och snabb anpassning vid nya hot.

4. Globala utmaningar:
   - Internationella hot som cyberkrigföring, spionage och desinformation påverkar alla länder.
   - Ökat samarbete mellan länder, delning av hotinformation och gemensamma strategier.

5. Mänskliga faktorer:
   - Social ingenjörskonst och insiderhot är allvarliga hot. Användare kan vara den svagaste länken.
   - Åtgärder: Utbildning, medvetenhet och tydliga riktlinjer för användare.

6. Framtidsbild:
   - En framtidsbild bör inkludera scenarioanalyser för olika hotutvecklingar.
   - Åtgärder: Skapa en anpassningsbar organisation som kan hantera olika hotscenarier.

Sammanfattningsvis krävs en holistisk strategi som kombinerar tekniska, juridiska, mänskliga och globala aspekter för att möta framtidens hot inom datadelning och informationssäkerhet.

4. Skydd av demokratiska värderingar och informationsdelning

Skyddet av demokratiska värderingar och informationsdelningar kräver mer än enbart lagstiftning. Här är några överväganden för att bemöta hot och säkerställa en trygg informationsdelning:

1. Nationell digitaliseringsstrategi:
   - En nationell digitaliseringsstrategi är avgörande för att skapa en gemensam riktning och förutsättningar för att skydda information.
   - Strategin bör inkludera utbildningsinsatser, säkerhetsmekanismer och kontinuerlig uppföljning.

2. Utbildning och medvetenhet:
   - Utbilda användare om informationssäkerhet, risker och bästa praxis.
   - Medvetenhet om hot och hur man agerar är avgörande för att minska sårbarheter.

3. Ständig uppföljning:
   - Uppföljningsmekanismer bör vara en integrerad del av informationsdelningen.
   - Regelbundna revisioner, riskbedömningar och anpassningar är nödvändiga.

4. Tekniska åtgärder:
   - Implementera tekniska lösningar som kryptering, autentisering och intrångsdetektering.
   - Skydda noderna där information delas.

5. Samverkan och delning av erfarenheter:
   - Samarbeta med andra aktörer, både nationellt och internationellt.
   - Dela erfarenheter och bästa praxis för att stärka skyddet.

6. Framtidsbild:
   - En framtidsbild bör inkludera scenarioanalyser för olika hotutvecklingar.
   - Anpassa strategin efter nya hot och teknologier.

Sammanfattningsvis krävs en holistisk strategi som kombinerar lagstiftning, utbildning, tekniska åtgärder och samverkan för att skydda information och demokratiska värderingar.

5. Demokrati

I en demokrati är det viktigt att skydda känslig information och värna om demokratiska värderingar. Här är några aspekter att beakta:

1. Demokratins kännetecken:
   - Fria val: Fria och rättvisa val är centralt i demokratier. I Sverige har vi regelbundna val till riksdagen, kommuner och landsting.
   - Flera partier: För att ett val ska vara demokratiskt måste det finnas flera olika partier att välja mellan. I Sveriges riksdag finns åtta politiska partier representerade.

- Politiska rättigheter: Människor måste vara garanterade politiska rättigheter, inklusive rösträtt, yttrandefrihet och mötesfrihet.
- Rättssäkerhet och likhet inför lagen: Alla ska vara lika inför lagen, och domstolar ska agera rättssäkert och opartiskt.
- Respekt för de mänskliga rättigheterna: Alla människor ska räknas som jämlika, oavsett personliga egenskaper.

2. Skydd av känslig information:
   - För att skydda känslig information behövs säkerhetsåtgärder. Det handlar om att balansera öppenhet och skydd.
   - Lagstiftning är en grund, men det krävs också utbildning, mevetenhet och kontinuerlig uppföljning.

3. Nationell digitaliseringsstrategi:
   - En nationell strategi för digitalisering kan skapa förutsättningar för att skydda information bättre.
   - Strategin bör inkludera utbildningsinsatser, säkerhetsmekanismer och kontinuerlig uppföljning.

6. Standardisering

Standardisering är avgörande för att underlätta effektiv datadelning och skapa en mer sammanhållen IT-verksamhet. Här är några aspekter att beakta:

1. Standardisering inom vårdinformationssystem:
   - Inom vårdsektorn är det viktigt att använda standarder och gemensam struktur i vårdinformationssystemen.
   - Detta är en förutsättning för att information som används i olika system ska fungera effektivt tillsammans, så kallad interoperabilitet.
   - Genom att använda standarder kan vi skapa ordning och reda i vårdsystemen och därmed ge en bättre arbetsmiljö för personalen och säkrare vård och omsorg för patienten.

2. Nationell digitaliseringsstrategi:
   - En nationell strategi för digitalisering är avgörande för att skapa en gemensam riktning och förutsättningar för att standardisera och effektivisera IT-verksamheten.
   - Strategin bör inkludera utbildningsinsatser, säkerhetsmekanismer och kontinuerlig uppföljning.

3. Förskolan, skolan och vuxenutbildningen:
   - I Sverige har Skolverket tagit fram en nationell digitaliseringsstrategi för skolväsendet.
   - Strategin fokuserar på barns och elevers digitala kompetens samt användningen av digitaliseringens möjligheter i undervisning och lärande.

4. Effektiv informationsförsörjning:
   - Inom hälso- och sjukvården pågår arbete med att ta fram en effektivare informationsförsörjning mellan vårdinformationssystem och Nationella Kvalitetsregister.
   - Automatiserad informationsförsörjning är ett sätt att praktiskt genomföra strategin för informationsförsörjning.

Sammanfattningsvis är standardisering och en nationell strategi avgörande för att skapa en mer sammanhållen och effektiv IT-verksamhet som underlättar datadelning och informationsutbyte.

7. Dataklassificering

Dataklassificering är en central del av att skydda känslig information och minimera risken för obehörig åtkomst.

1. Genom att klassificera data kan vi tillämpa effektiva säkerhetsåtgärder på den information som faktiskt är viktig och skyddsvärd.

2. Skyddet av känslig information är avgörande för att undvika oavsiktlig eller avsiktlig exponering.

3. Dataklassificering hjälper till att:
   - Förhindra obehörig åtkomst till känslig information.
   - Säkerställa fullständig efterlevnad med branschregler och standarder.
   - Skydda organisationens rykte genom att undvika dataintrång.
   - Identifiera känslig data: Utvärdera vilken information som är mest känslig för din organisation (t.ex. personuppgifter, affärshemligheter, finansiella data).
   - Skapa klassificeringskategorier: Definiera olika nivåer av känslighet (t.ex. offentlig, intern, konfidentiell, hemlig).
   - Tilldela klassificering: Klassificera varje dataobjekt baserat på dess innehåll och användningsändamål.
   - Implementera åtkomstkontroller: Använd klassificeringen för att tillämpa lämpliga åtkomstkontroller (t.ex. behörighetsgrupper, kryptering).

Sammanfattningsvis är dataklassificering en central del av att skydda information från obehörig åtkomst. Genom att använda tydliga kategorier och effektiva säkerhetsåtgärder kan vi minimera riskerna och säkerställa att endast auktoriserade användare får tillgång till känslig data.