STORSTHLM

Stockholms läns landsting

Principer för digital samverkan
KSL/17/0096
2017

Principer för digital samverkan i Stockholms län

Tillgänglighetsanpassad version oktober 2020

Innehåll

1. Inledning

Digital samverkan och utbyte av elektronisk information ger förutsättningar att både förenkla och effektivisera för invånaren, brukaren och patienten.
För att möjliggöra detta har gemensamma principer för informationsutbyte, samt hur den ska ske säkert och effektivt, antagits av samtliga kommuner i regionen och landstinget.

I stockholmsregionen utgör principerna för samverkan grunden för all digital samverkan. Målet är att bygga den tillit som behövs för att möjliggöra ett säkert informationsutbyte över internet.

Den första versionen av principer, *16 principer för samverkan*, utarbetades 2009. Där redovisade kommunerna och landstinget sin gemensamma syn på vad som utgör grunden för säker och effektiv digital kommunikation.

Samtidigt etablerades ett arbetssätt där alla parter enades om att ta hänsyn till principerna vid kravställning av nya digitala tjänster. Under 2012 moderniserades principerna för att omfatta all informationshantering.

Under 2017 har en översyn av principerna genomförts. I denna bearbetning, *Principer för digital samverkan i Stockholms län,* har hänsyn bland annat tagits till E-delegationens *Principer för digital samverkan* och Sveriges Kommuner och Landstings *Handlingsplan 2017–2025: Förutsättningar för digital utveckling i kommuner, landsting och regioner*. Ambitionen är att på sikt enbart tillämpa gemensamma och nationella principer.

2. Syfte och målgrupp

Principerna för digital samverkan syftar till att få regional samsyn kring digital samverkan, uttrycka vilka som är prioriterade principer i Stockholms län och även att underlätta utbyte av information mellan aktörerna vilket skapar förutsättningar att både förenkla och effektivisera för både invånare och verksamhet.

Principerna har indelats i grund- och arkitekturprinciper för digital samverkan. Grundprinciperna vänder sig till högre tjänstemän/chefer och arkitekturprinciperna vänder sig till IT-beslutsfattare i kommuner eller landstinget. De områden som är mest prioriterade för digital samverkan i Stockholms län är informationsdelning, federation och tillit. Våra arkitekturprinciper har därför extra tyngdvikt på dessa områden.

3. Grundprinciper för digital samverkan

3.1 Utgå ifrån invånarnas behov

Invånarnas behov och perspektiv ska stå i centrum och vara den överordnade drivkraften i utvecklingen av gemensamma produkter, tjänster och metoder. Detta innebär en digital samverkan som leder till organisationsöverskridande kontakter som även kan inkludera privata företag.

Motiv: Invånarna ställer allt högre krav på offentligt finansierade verksamheter. Invånarna förväntar sig att offentliga och andra aktörer vill och kan samverka på ett effektivt sätt. Stockholmregionen är komplex med många aktörer, varav en stor andel är privata utförare. Den starka tillväxten i regionen och en ökad rörlighet över kommungränserna kräver samverkan på

ett strukturerat sätt. Samverkande processer och tjänster måste därför utvecklas för att möta invånaren i olika kanaler, på dennes villkor och i aktuella situationer.

Konsekvens: Aktuella tjänster och processer behöver tydliggöras och beskrivas på en nivå så att samverkan möjliggörs. Det innebär i praktiken att de samverkande aktörerna måste vara överens om hur invånaren ska mötas, vad som startar och avslutar en samverkande process, vilken information som ska flöda mellan aktörerna och vilka tjänster som behövs för att invånaren ska möta en sammanhållen service. Detta gäller också verksamhetsstödjande tjänster som inte direkt påverkar invånare.

3.2 Låt digitala möten ske på användarnas villkor

Användarnas behov ska beaktas när man bestämmer vilka offentliga tjänster som ska tillhandahållas och hur detta ska ske. Därför ska användarnas behov och krav så långt som möjligt vägleda utformningen och utvecklingen av offentliga tjänster.

Motiv: Digitala möten som är anpassade till invånarens behov ger ökad tillgänglighet, större enkelhet, bättre effektivitet, högre informationskvalitet samt större transparens och delaktighet. Invånarens vardag blir enklare när deras processer stöds tvärs över myndighetsgränserna. Informationskvaliteten höjs när användarnas initiala registreringar sker digitalt, vilket minskar risken för felregistrering och feltolkning av inkomna handlingar.

Konsekvens: Det ska finnas alternativa kanaler, både fysiska och digitala, för att få tillgång till en tjänst, eftersom användarna kan föredra olika kanaler beroende på omständigheterna och sina behov.

3.3 Upprätthåll rätt nivå på informationssäkerhet och integritet

I sina kontakter med offentliga myndigheter och privata företag måste alla kunna lita på att allt sker i en säker och pålitlig miljö och i enlighet med gällande bestämmelser, t.ex. förordningen om dataskydd (GDPR) och förordningen om elektronisk identifiering och betrodda tjänster (eIDAS).

Motiv: När offentliga aktörers uppdrag utförs via digitala tjänster ställs krav på en mer samverkande utformning, då information från flera aktörer ska vidareutnyttjas och förädlas. Detta leder till ett behov av samordning även av informationssäkerheten. Samordningen är nödvändig både för att effektivisera, öka kvaliteten, skapa interoperabilitet och för att reducera kostnader, men är också viktig för att kunna möta invånare och andra intressenters förväntan på likvärdig säkerhet och integritet i myndigheternas informationshantering.

Konsekvens: Säkerhet och respekt för privatlivet är grundläggande frågor vid tillhandahållandet av offentliga tjänster. Kommuner och landsting bör se till att de följer principerna om inbyggt integritetsskydd och inbyggd säkerhet. Detta för att skydda hela sin infrastruktur samt tillse att tjänsterna inte är sårbara för angrepp som kan störa driften, leda till datastöld eller dataskador. De måste också tillse att de uppfyller rättsliga krav och skyldigheter avseende dataskydd och respekt för privatlivet och medger de risker för integriteten som avancerad databehandling och dataanalys innebär. Vid informationsutbyte över huvudmannagränser ska rättsliga förutsättningar och regelverk beaktas.

3.4 Delegerat mandat och ansvar

EU:s princip för subsidiaritet innebär att beslut ska fattas så nära de samverkande parterna som möjligt eller av enskild part om endast en part är involverad.

Motiv: För att vi ska kunna samverka behövs en ständig dialog om vad som är det egna ansvaret respektive vad som är det gemensamma ansvaret.

Konsekvens: Tillse att den egna organisationen upprättar ramar och strategier för interoperabilitet och att dessa är i linje med EIF (European Interoperability Framework). Utifrån regionala sammanhang och behov kan dessa behöva utökas och anpassas. För detta kan olika samverkansgrupper behöva etableras av de parter som ska samverka, allt från samverkan mellan två parter till federationssamverkan.

3.5 Låt behov och nytta vara styrande

Utveckling och förvaltning av tjänster som inkluderar fler samverkande organisationer ska baseras på en så fullständig analys som möjligt.
Analysen ska omfatta det verkliga behovet och invånarnyttan samt på hur verksamhetsnyttor och kostnader fördelar sig mellan deltagande aktörer och berörda intressenter.

Motiv: Nyttan måste vara styrande och måste vara tydlig innan en gemensam lösning utvecklas. Fördelningen av kostnader och nyttor mellan deltagande aktörer är nödvändig att ta fram för att skapa acceptans och förståelse för lösningens hela livscykel. Viktigt är att detta primärt inte ska ske för att effektivisera organisationens egen handläggning och verksamhet, utan för att ge ökad nytta utifrån ett invånarperspektiv.

Konsekvens: Utvärdering av olika lösningars ändamålsenlighet och effektivitet måste ske i samverkan och med hänsyn till användarnas behov, proportionalitet samt kostnads-och nyttobalans.

4. Arkitekturprinciper för digital samverkan

4.1 Säkerställ ledning och styrning av informationssäkerhetsarbetet

En förutsättning för digital samverkan är att informationen hanteras korrekt och säkert så att inte informationssäkerheten i någon av de samverkande organisationerna riskeras (en kedja är inte starkare än sin svagaste länk). Grundelementet i arbetet med informationssäkerhet är ledning och styrning. För att en organisationsledning ska kunna styra informationssäkerhetsarbetet så att det motsvarar de behov som organisationen och dess samverkande parter har, krävs förutom ledningens engagemang, ett ledningssystem för informationssäkerhet (LIS).
Ledningssystemet omfattar bland annat:

- Policy, riktlinjer och styrdokument
- Metoder för informationsklassning, risk- och sårbarhetsanalys
- Process för hantering och uppföljning av inträffade incidenter

Motiv: Syftet med att respektive organisation har ett LIS är att genom ledningens delaktighet

och engagemang i informationssäkerhetsarbetet tillse att informationssäkerheten är på rätt nivå, så att tillit mellan samverkande aktörer uppnås.

Konsekvens: Utse minst en person som ansvarar för att införa ett LIS, kontinuerligt leda informationssäkerhetsarbetet, och utifrån metoder, processer och styrande dokument vidta nödvändiga åtgärder för att upprätthålla rätt skyddsnivåer.

4.2 Aktivt arbeta med federation och tillit

För att underlätta digital samverkan mellan flera organisationer bör ett aktivt arbete med identitets- och behörighetsfederation bedrivas och fastställda tillitsramverk följas.

Motiv: Tilliten grundläggs genom att den enskilde federationsmedlemmen uppfyller nödvändiga gemensamma krav. Uppfylls kraven kan medlemmarna ha tillit till varandra. Med federation behöver användare endast ha en inloggning till samtliga anslutna tjänster. Gemensamma tjänster blir lättare att komma åt och användandet ger mindre administration, samtidigt som högre säkerhetskrav kan ställas. Dessutom blir det enklare för tjänsteleverantörer att ansluta användarorganisationer.

Konsekvens: En identitets- och behörighetsfederation ställer krav på federationsmedlemmar. Alla involverade parter/komponenter – organisationer, tjänster, processer, användare – ska vara tillitsgranskade och godkända. Aktuella standarder ska följas. Information ska säkerhetsklassas. Tjänster som ingår ska federationsanpassas och bl.a. ha förmåga att konsumera elektroniska identitetsintyg.

4.3 Tillämpa gemensamma begrepp och informationsstrukturer

Information som är ändamålsenlig, enhetligt beskriven, strukturerad och med bibehållen mening blir möjlig att utbyta. Informationen kan då användas för att skapa sammanhållen information, förenkla informationssäkerhetsarbete, möjliggöra kunskapsstyrning och utveckling av beslutstöd, för uppföljning, jämförelse och som underlag för kvalitet och verksamhetsstyrning.

Motiv: Syftet med att strukturera och standardisera information är att stödja en effektiv informationsförsörjning och underlätta informationsöverföring mellan olika aktörer. Detta behöver göras utifrån verksamhetsprocesser, vad olika intressenter behöver kommunicera och vilken typ av information de behöver i kommunikationen.

Konsekvens: Varje informationsmängd behöver ha följande: ägare, förvaltning, affärsregelverk, användningskartläggning och kvalitetsregelverk enligt vedertagna masterdataprinciper. För att informationshanteringen ska vara effektiv behövs ett livscykelperspektiv både på informationen i sig och på dess hantering. När samverkande aktörer har en gemensam beskrivning av verksamhetsområdet och dess informationsstrukturer, ökar möjligheterna till ett väl fungerande informationsutbyte.

4.4 Tillgängliggör information som öppna data

Information som skapas i den egna verksamheten och som ska användas av andra aktörer ska tillgängliggöras på ett enhetligt sätt samt enligt gällande regelverk, lagar och förordningar. Ett speciellt område är tillgängliggörandet av öppna data, när myndigheternas information ska tillgängliggöras för externa parter i så stor omfattning som möjligt, med beaktande av sekretess- och integritetsaspekter.

Motiv: För att skapa en effektiv informationshantering vid digital samverkan krävs att den information som ska utbytas är tillgänglig, kan förstås och hanteras på samma sätt av alla ingående aktörer så att tjänsteutveckling och innovation möjliggörs.

Konsekvens: Genom att tillgängliggöra information enligt denna princip kan informationen i tjänster återanvändas inom eller utanför de egna organisationsgränserna, vilket möjliggör nya tillämpningsområden. Förutom att data som är publik lätt kan kommas åt och användas av regionens kommuner och landsting, ger detta en enhetlighet som underlättar utformning av nya och mer effektiva lösningar, vilka kan baseras på andras tjänsteutbud.

4.5 Hämta information vid källan

Huvudprincipen är att alltid hämta information så nära källan som möjligt, hos den som producerar och tillhandahåller informationen.

Motiv: Genom att hämta information vid källan säkerställs att informationen är tillförlitlig och aktuell.

Konsekvens: Ansvar för begrepp och information måste vara utrett och klarlagt. Det finns situationer då flera aktörer tillhandahåller samma information. Det är då relevant att klargöra vilken aktör som är att anses som primär källa. Om informationen behöver uppdateras ska detta göras hos den primära källan.

4.6 Använd standarder

Vid informationsutbyte ska i första hand lämpliga standarder användas. Om lämpliga standarder saknas ska etablerade branschstandarder eller de facto standarder användas. Valet av standard ska vara teknikoberoende så att man undviker inlåsningseffekter och begränsar samverkande parters val av tekniska plattformar.

Motiv: Standardiserade gränssnitt sänker kostnader och bidrar till ökad återanvändning och en öppen marknad.

Konsekvens: Beställare måste följa utvecklingen och ha en löpande omvärldsbevakning inom området för att kunna kravställa kring relevanta standarder.

4.7 Säkerställ digitala tjänsters tillgänglighet

Säkerställ stabilitet och tillgänglighet för de digitala tjänsterna utifrån de samverkande verksamheternas eller invånarens krav och behov.

Motiv: En stabil IT-miljö är en grundförutsättning för att bedriva en säker och effektiv verksamhet. I takt med att verksamheterna och invånarna blir alltmer beroende av digitala tjänster minskar toleransen för avbrott och andra störningar. Samhälls- eller verksamhetskritiska processer ställer krav på tillgänglighet och kontinuitet.

Konsekvenser: Graden av tillgänglighet och kontinuitet ska baseras på verksamhetens krav i förhållande till kostnad och nytta. Genom att ta fram en kontinuitetsstrategi för IT samt återställningsplaner för IT-system baserade på verksamhetskrav, kan kraven mötas med en konsekvent och strukturerad metod. Vid vidareutnyttjande av digitala tjänster bör kvalitet, skalbarhet och tillgänglighet särskilt beaktas.