Vägledande principer för digital samverkan

Version 1.3

Med syfte att stödja en öppen, enkel och innovativ offentlig förvaltning

E-delegationen

Dokumentets ursprung

Datum	Namn/Författare	Organisation
2013-01-11	Lars Wahlund Ulf Palmgren Lars-Åke Johansson	Pensionsmyndigheten Sveriges Kommuner och Landsting Arbetsförmedlingen

Godkännande och fastställande

Datum	Version	Namn	Organisation
2013-08-28	1.0	E-delegationens Arbetsgrupp	E-delegationen
2015-05-28	1.3	Annika Bränström	Ordförande E-delegationen

Ändringshistorik

Datum	Version	Namn	Förändringar
2014-10-31	1.1	Lars Wahlund Lars-Åke Johansson	Lagt till jämförelse med EU:s European Interoperability Framework Placerat referenslistan i bilaga Nytt namn: Tjänste- och processamverkan Nytt namn: Säkerhet och juridik Ny grundprincip G1: Livsituationer och livshändelser Förändrad grundprincip G4: Delegera mandat och ansvar Ändrat placering av princip D4: Externa innovatörer Döpt om princip D5: Återanvänd inlämnad information Lagt in princip om Öppna data i T2: Bygg tjänstebaserat Slagit ihop ett antal säkerhetsprinciper Ändrat princip S4: Analysera rättsliga förutsättningar Gjort mindre textändringar i hela dokumentet
2014-12-02	1.2	Lars Wahlund Lars-Åke Johansson	Inarbetat remissvar inlämnade senast den 21 nov 2014 Lagt till en ny princip G3 om informationssäkerhet och integritet Flyttat tidigare princip G3 om tillgängliggörande till ny T2 Ändrat numrering på övriga principer
2015-05-27	1.3	Lars Wahlund	Omarbetat avsnitten om informationssäkerhet (G3, S1-S3) efter dialog med Arbetsutskottet för informationssäkerhet. Döpt om dokumentet till Vägledande principer för digital samverkan.

Dokumentreferenser

Referensnr	Dok.bet.	Dokumentnamn
Se bilaga 1	Referenser	

Bild på förstasidan: http://en.wikipedia.org/wiki/File:Selfridges_BIrmingham.jpg

Innehållsförteckning

1 Inledning 4

1.1 Syfte 4
1.2 Omfattning 4
1.3 Målgrupper 4
1.4 Tillämpning av vägledande principer för digital samverkan 4
1.5 Initiativ på EU-nivå 5

2 Vägledande principer för digital samverkan 6

3 Grundprinciper 7

3.1 Utgå från medborgarnas livshändelser 7
3.2 Låt digitala möten ske på användarnas villkor 8
3.3 Upprätthåll rätt nivå på informationssäkerhet och integritet 9
3.4 Delegera mandat och ansvar 10
3.5 Låt behov och nytta vara styrande 10

4 Arkitekturprinciper 11

4.1 Digitala möten 11
4.1.1 Låt digitala kanaler vara det primära alternativet 11
4.1.2 Anpassa till olika gruppers och individers behov 12
4.1.3 Öka medborgarnas insyn och möjligheter att påverka 13
4.1.4 Öppna upp för externa innovatörer 13
4.1.5 Återanvänd redan inlämnad information 14
4.2 Tjänste- och processamverkan 15
4.2.1 Bestäm och tillämpa gemensamma begrepp, modeller och mönster 15
4.2.2 Tillgängliggör och återanvänd information och tjänster på ett enhetligt sätt 16
4.2.3 Bygg tjänstebaserat 18
4.2.4 Hämta information vid källan 19
4.2.5 Använd öppna standarder 19
4.3 Informationssäkerhet och juridik 20
4.3.1 Bedriv ett riskbaserat informationssäkerhetsarbete 20
4.3.2 Skydda den personliga integriteten 21
4.3.3 Beakta informationens skyddsvärde i hela kedjan 22
4.3.4 Analysera rättsliga förutsättningar 23

Bilaga 1, Referenser 24

Bilaga 2, Jämförelse European Interoperability Framework 24

1 Inledning

Som en del i realiseringen av regeringens vision och målbild – ”Med medborgaren i centrum” – har en arbetsgrupp under dåvarande E-delegationen haft i uppdrag att fokusera på samverkan kring myndighetsgemensamma lösningar och verksamhetsöverskridande processer, där det på ett naturligt sätt inte finns någon aktör som ensam kan ta ansvaret för tjänsten, processen eller resultatet. Utifrån detta perspektiv har det vuxit fram ett behov av en Vägledning för digital samverkan. Ett fundament i denna vägledning är principerna för digital samverkan.

1.1 Syfte

Syftet med detta dokument är att stödja utveckling av en samverkande e-förvaltning.

1.2 Omfattning

Principerna berör samverkanslösningar som stöder medborgarnas livssituationer. Det avser både lösningar som riktar sig direkt till medborgare samt sådana som underlättar samverkan genom ett IT-baserat informationsutbyte.

Principerna möjliggör digital samverkan **mellan olika aktörer,** exempelvis tillhandahållande av folkbokföringsuppgifter, webbplatser för olika livshändelser, t.ex. verksamt.se, eller arkitektur för hantering av e-legitimationer.

Principerna ger stöd för utveckling och förvaltning av olika typer av **tjänster**[1] (inom kommunal sektor används även begreppet ”service”). Principerna ska även underlätta utveckling och förvaltning av **samverkansprocesser** som berör flera myndigheter och organisationer.

Principerna anger hur samverkan bör ske mellan olika myndigheter och andra aktörer, principerna kan dock även användas internt hos enskilda aktörer.

1.3 Målgrupper

Dokumentets primära målgrupper är beslutsfattare, verksamhets-, IT- och samverkansarkitekter och verksamhetsutvecklare som är involverade i samverkansprojekt. Sekundära målgrupper är planeringsansvariga, beslutsfattare, jurister och informationssäkerhetsansvariga med anknytning till sådana projekt.

1.4 Tillämpning av vägledande principer för digital samverkan

Genom tillämpning av grundprinciper och arkitekturprinciper skapas bättre förutsättningar för att nå en bra samverkan, samt för att möjliggöra återanvändning av redan tillgängliga funktioner och information.
Principerna tillämpas vid utveckling och förvaltning av:

- samverkanslösningar som inbegriper myndigheter och andra aktörer
- förvaltningsgemensamma tjänster, som utvecklas av utsedda myndigheter eller externa aktörer.

---

[1] **Bastjänster** där en myndighet antingen tillhandahåller information som kan vidareförädlas och presenteras av andra parter eller utför en tjänst. Exempel på sådana bastjänster är kungörelseinformation från Post- och Inrikes Tidningar och avställning av fordon. En bastjänst kännetecknas av att den saknar användargränssnitt, istället sker anrop till tjänsten från ett annat program för vidareförädling och presentation av andra parter.

Vidareförmedlingstjänster är en variant av detta, där någon part sammanställer information från flera bastjänster och presenterar denna information som en ny bastjänst.

E-tjänster, med vilket menas tjänster som tillhandahålls via ett digitalt användargränssnitt av myndigheter, privata företag eller andra organisationer. E-tjänsten kan t.ex. vara en funktion på en webbsida, visas i en smart telefon eller på en surfplatta. E-tjänster kan anropa bakomliggande bastjänster eller initiera verksamhetsprocesser hos en eller flera myndigheter. Exempel på sådana e-tjänster är anmälan om VAB på forsakringskassan.se, en app för väderprognoser på en smart telefon eller åtgärder när en närstående avlider.

Förvaltningsgemensamma tjänster, med vilket avses digitala tjänster som tas fram för specifika syften och som kan delas och återanvändas inom hela eller delar av den offentliga sektorn. En myndighet får ansvaret att utveckla och förvalta en referensinstallation, medan andra aktörer kan utveckla alternativa lösningar. Exempel på sådana förvaltningsgemensamma tjänster är Mina meddelanden eller en gemensam notifieringsfunktion.

Principerna bör tillämpas vid all utveckling och förvaltning av myndighetsöverskridande processer, bastjänster, e-tjänster och andra komponenter som ingår i eller utgör offentliga e-förvaltningstjänster.

Kraven på grundprinciper och arkitekturprinciper är att de ska vara långsiktiga, teknikoberoende och stabila, och därmed ligga på en relativt hög nivå, dvs. inte vara alltför detaljerade. Specifika krav ska istället hanteras i mer konkreta anvisningar.

Principerna är vägledande, dvs innehåller rekommendationer för hur myndigheter och andra bör utforma tjänster mot medborgarna, men är inte föreskrivande.

Principerna ska vara:

- **Förankrade** - grundprinciper ska beslutas på högsta ledningsnivå. Övriga principer beslutas på lämpliga undernivåer (så få som möjligt).
- **Begripliga** - principernas grundsatser (uttryck, logisk grund, slutsats) ska lätt kunna förstås.
- **Robusta** - principerna måste vara exakt formulerade för att kunna ge ett otvetydigt underlag för användning.
- **Kompletta och konsistenta** - principerna bör vara heltäckande, men får ändå inte vara motsägelsefulla.
- **Stabila** - principerna ska vara stabila över tid, men ändå kunna genomgå en ändrings- och livscykelhantering.
- **Spårbara** - principerna ska kunna härledas till uppsatta strategier och mål.

1.5 Initiativ på EU-nivå

På EU-nivå finns ett initiativ, European Interoperability Framework (EIF) for European public services, kring interoperabilitet vilket utgår från tolv arkitekturprinciper:

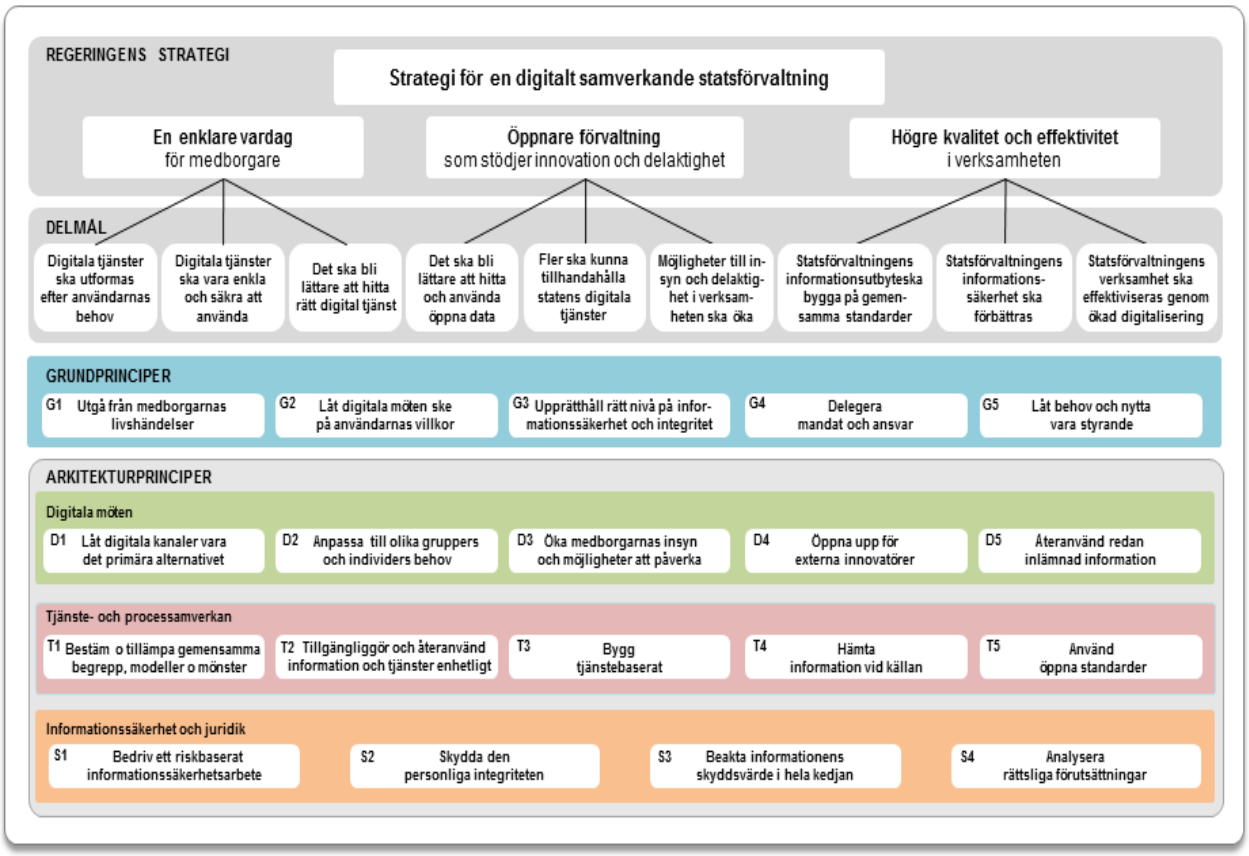
1. Subsidiarity and proportionality (subsidiaritet och proportionalitet)
2. User-centricity (användaren i fokus)
3. Inclusion and accessibility (delaktighet och tillgänglighet)
4. Security and privacy (säkerhet och personlig integritet)
5. Multilingualism (flerspråkighet)
6. Administrative simplification (administrativ förenkling)
7. Transparency (transparens)
8. Preservation of information (bevarande av information)
9. Openness (öppenhet)
10. Reusability (återanvändbarhet)
11. Technological neutrality and adaptability (teknikneutralitet och anpassningsbarhet)
12. Effectiveness and efficiency (effektivitet och ändamålsenlighet).

I Bilaga 2 görs en jämförelse mellan indelningen i detta dokument och EIF:s principer. Jämförelsen pekar på att de båda principindelningarna väl täcker in varandra, dock kräver principen om bevarande av information att arkivering enligt Riksarkivets anvisningar tillämpas. Vid en granskning från EU av en tidigare version av dokumentets principer var enda anmärkningen att EIF:s princip om transparens saknas. Detta har korrigerats i avsnitt 4.1.3.

Vi har trots jämförelsen valt att inte strukturera enligt ovanstående EIF-principer. Vi har istället utgått från regeringens strategi för en samverkande e-förvaltning, vilken bättre stämmer överens med visionen om Medborgaren i centrum utgående från dennes livshändelser, något som inte lika tydligt framhävs i European Interoperability Framework.

2 Vägledande principer för digital samverkan

Baserat på de huvudmål och delmål som definieras i regeringens Strategi för en digitalt samverkande statsförvaltning har fem grundprinciper formulerats och under dem har fjorton arkitekturprinciper utarbetats:[2]



Figur 1: Principer för digital samverkan

[2] Färgkodningen och numreringen i bilden överensstämmer med beskrivningarna i detta dokument.

Det finns i detta dokument ett antal referenser till dokument från regeringen, E-delegationen m.fl. Sådana dokument tenderar att vara versionsbundna och bli inaktuella. Vi har ändå valt att ta med referenserna, läsaren bör dock undersöka om mer aktuella versioner finns.

3 Grundprinciper

3.1 Utgå från medborgarnas livshändelser

G1 – Utgå från medborgarnas livshändelser	
Beskrivning	En livshändelse uppstår när en medborgare (privatperson eller företagare) ställs inför en händelse som påverkar och förändrar hans eller hennes livssituation. Den kundprocess som då startar kan ofta innebära ett antal myndighetsöverskridande kontakter och verksamhetsprocesser. Kundens agerande måste inte alltid vara ett resultat av att en livshändelse inträffat, utan kan vara resultatet av en rad andra faktorer, t.ex. baserat på en fastställd tidpunkt, exemplifierat av skattedeklarationen i början av maj varje år.
Motivering	Vissa livshändelser behöver särskilt stöd; om de kräver kontakter med olika myndigheter och aktörer, om de kräver flera återkommande kontakter eller om livshändelserna är nya och komplicerade för medborgaren att hantera. Samverkande processer och tjänster måste därför utvecklas för att möta medborgaren i olika kanaler, på dennes villkor och i aktuella situationer. Offentlig sektors kunder, både privatpersoner och företag, förväntar sig att offentliga aktörer vill och kan samverka på ett effektivt sätt. Kunden har istället idag ett stort och betungande ansvar att koordinera de offentliga aktörerna vilket inte skulle behövas om de offentliga aktörerna kunde samverka på ett strukturerat sätt. Flera studier lyfter fram att svensk offentlig förvaltning tappar sin ställning i internationella jämförelser, mycket på grund av oförmågan att skapa sammanhållna tjänster som hanterar livshändelser som spänner över statlig, regional och lokal nivå. Ett fortsatt fokus på utveckling av service och tjänster med utgångspunkt i sammanhållna livshändelser är en viktig förutsättning för att behålla och utveckla medborgarnas förtroende.
Konsekvens	De samverkande processerna i kundens livshändelse behöver alltså tydliggöras och beskrivas på en nivå så att samverkan möjliggörs. Det innebär i praktiken att de samverkande aktörerna måste vara överens om hur kunden ska mötas, vad som startar och avslutar en samverkande process, när agerandet i kundens livshändelse är fullgjort, vilken information som ska flöda mellan aktörerna och vilka tjänster som behövs i livshändelsen för att kunden ska möta en viss servicenivå. När medborgarnas livshändelser ska stödjas av flera olika myndigheter är det nödvändigt att de inblandade myndigheterna utser en ansvarig myndighet med ett tydligt utpekat och kvitterat huvudansvar. Utan en huvudansvarig myndighet är risken annars stor att avtal, funktionalitet, gränssnitt, samordning, testmöjligheter m.m., vilka är nödvändiga komponenter för leveransen, inte kommer på plats.

3.2 Låt digitala möten ske på användarnas villkor

G2 – Låt digitala möten[3] ske på användarnas villkor	
Beskrivning	I det nya e-samhället kommer medborgarna att avgöra när och hur digitala möten ska äga rum. Därigenom förändras perspektivet, från myndighetscentrerat till medborgarorienterat, från myndigheternas egna verksamhetsprocesser till medborgarnas processer. Sådana processer kan spänna över både offentlig och privat sektor. Digitala möten kommer i det nya e-samhället att ske via olika kanaler; i smarta telefoner, på pekplattor, i sociala medier, på privata och offentliga webbportaler, på myndighetsspecifika webbplatser, samt via framtida, i dag okända klient-plattformar. Det bör vara möjligt att nå tjänster vid tidpunkter på dygnet när medborgarna själva kan och vill.
Motivering	Digitala möten som är anpassade till medborgarnas behov ger ökad tillgänglighet, större enkelhet, bättre effektivitet, högre informationskvalitet samt större transparens och delaktighet. Genom att finnas i för medborgarna kända miljöer uppnås en ökad enkelhet och förståbarhet, vilket skapar förutsättningar för att minska det ”digitala utanför-skapet”. Medborgarnas vardag blir enklare när deras processer stöds tvärs över myndig-hetsgränserna. Informationskvaliteten höjs när användarnas initiala registreringar sker digitalt, vilket minskar risken för felregistrering och feltolkning av inkomna handlingar. Via digitala kanaler möjliggörs transparens, större insyn och delaktighet genom att medborgarna kan följa t.ex. handläggningsprocessen eller vårdkedjan och status för dem.
Konsekvens	För att möta medborgarnas behov måste myndigheter och annan offentlig verksamhet tillhandahålla tjänster så att de blir lätt tillgängliga i de digitala kanaler som föredras, i medborgarnas ”digitala rum” och miljöer. Samtidigt måste säkerställas att informationen presenteras på likvärdigt sätt, oberoende av i vilken kanal detta sker. Då en enskild myndighet inte ensam kan stödja medborgarens hela process, ger detta ett ökat behov av att samverka över organisationsgränserna, samt att utveckla tjänster som stödjer denna princip. Användarmönster förändras över tiden, nya kanaler och nya tekniska plattformar tillkommer, medan andra minskar i omfattning och betydelse, vilket ställer krav på resurser för omvärldsbevakning och trendspaning, både på nationell nivå och på myndighetsnivå. Tekniker som kan hantera flera, olika digitala kanaler bör användas för att slippa utveckla och anpassa e-tjänster för olika specifika, tekniska klientplattformar. Se även Riktlinjer för myndigheters användning av sociala medier. Möjligheten att växla mellan olika understödda digitala kanaler gör dock att uttestning av e-tjänster kompliceras. Vidare behöver informationssäkerhetskrav på nya och befintliga kanaler analyseras, värderas och beaktas, den personliga integriteten värnas samt kostnadsaspekter vägas in. Single sign on (SSO) bör övervägas för att koppla ihop användarnas identifiering så att de får tillgång till flera tjänster utan att inloggning behöver upprepas. Poli-cies för gemensam utloggning (Single Log Out) måste då även tas fram för olika situationer.

[3] Med digitala möten avses i detta dokument att användarna nyttjar tjänster via digitala kanaler

3.3 Upprätthåll rätt nivå på informationssäkerhet och integritet

G3 – Upprätthåll rätt nivå på informationssäkerhet och integritet	
Beskrivning	En ökad samverkan samt en koncentration av e-tjänster på nationell nivå skapar nya möjligheter, men också nya risker, som måste hanteras gemensamt för att viktiga samhällsfunktioner ska kunna upprätthållas. Informationssäkerhet är därför en nödvändig förutsättning för e-förvaltningen, vilket också framgår av den målbild som finns i Strategi för informationssäkerhet i e-förvaltning från Myndigheten för samhällsskydd och beredskap, MSB. Med detta avses en styrning av organisatoriska och tekniska åtgärder som skyddar information så att – utifrån analyserade risker – rätt nivå uppnås för: • konfidentialitet • riktighet • spårbarhet • tillgänglighet. Generellt ska de tjänster som tas fram vid digital samverkan utvecklas i linje med de krav som ställs på myndigheters arbete med informationssäkerhet, för att uppfylla målbilden i ovanstående strategi. Personuppgifter ingår i den absoluta majoriteten av tjänster, som hanterar information i offentlig verksamhets uppdrag, riktade mot enskilda. Därför är skyddet av den personliga integriteten en viktig aspekt som särskilt ska beaktas. Syftet med arbetet med informationssäkerhet är att reducera risker ur de fyra perspektiv som beskrivs ovan. Därför måste arbetet bygga på itererade riskanalyser som påverkar utveckling och sedermera förvaltning av de tjänster som är aktuella.
Motivering	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 därför till ett behov av samordning även av informations-säkerheten. Samordningen är nödvändig både för att effektivisera, öka kvaliteten, skapa inter-operabilitet och för att reducera kostnader, men är också viktig för att kunna möta medborgare och andra intressenters förväntan på likvärdig säkerhet och integritet i myndigheternas informationshantering. Informationssäkerhet – där skyddet av personlig integritet ingår som en av flera aspekter – är därför en grundläggande princip i all offentlig informationshantering och måste ingå som en styrande faktor redan initialt i projekt som baseras på digital samverkan. Det är viktigt att en säkerhetsarkitektur skapas integrerat med övrig arkitektur och alltså inte tvingas läggas till i slutskedet av ett utvecklingsinitiativ.
Konsekvens	Ansvar och roller som informationsägare och tjänsteproducent måste beskrivas och hanteras på likartat sätt i olika samverkanslösningar liksom styrning genom riskanalyser och informationsklassningar, samt definierade skyddsnivåer. De lös-ningar som tas fram ska uppfylla krav på funktion i normalläge, men ska även planeras för att hantera störningar på olika nivå. Stor vikt måste läggas vid att hantera lösningar där information från flera aktörer sammanförs, på annat sätt aggregeras, altenativt används på annat sätt än ursprungligen definierat. I sådana situationer riskeras både att ett oklart ansvar uppstår och att kraven på personlig integritet åsidosätts. Ytterligare en konsekvens är att det måste finnas funktioner som hanterar tillit då flera aktörer (offentliga och privata) samverkar, exempelvis genom efterlevnads-kontroller.

3.4 Delegera mandat och ansvar

G4 – Delegera mandat och ansvar	
Beskrivning	EU:s princip för subsidiaritet innebär i detta sammanhang att beslut ska fattas så nära de samverkande parterna som möjligt eller av enskild part om endast en part är involverad. EU:s princip för proportionalitet begränsar mängd och omfattning av åtgärder till det som är nödvändigt för att uppnå överenskomna mål, vilket lämnar största möjliga frihet för genomförandet till de samverkande parterna. Detta har bl.a. resulterat i att samverkansarkitekturen har begränsats till digital samverkan mellan olika parter. Hur en enskild aktör utformar sin interna arkitektur och sina egna processer, hur den hanterar sina begrepp, sin interna information och sin informationslagring är en intern angelägenhet.
Motivering	Det finns inget egenvärde i att samordna mer än vad som är nödvändigt för att kunna samverka kring det digitala mötet. Istället uppnås en större flexibilitet om medverkande parter själva kan bestämma och hantera sin interna verksamhet, det enda som är intressant är att parterna levererar avtalade tjänster och medverkar med sina delar.
Konsekvens	Detta påverkar arkitekturen som helhet samt relationer mellan samverkande parter med avseende på avtal, tillgänglighet m.m. För detta kan olika samverkansgrupper behöva etableras av de parter som ska samverka, allt från bilateral samverkan mellan två parter till stora nationella eller sektorsvisa federationer. Se även Vägledning för digital samverkan.

3.5 Låt behov och nytta vara styrande

G5 – Låt behov och nytta vara styrande	
Beskrivning	Utveckling och förvaltning av tjänster ska baseras på en så fullständig analys som möjligt av det verkliga behovet och kundnyttan, samt på hur kostnader och nyttor (ekonomiska och kvalitativa) fördelar sig mellan deltagande aktörer och berörda intressenter. Denna analys ska inte bara omfatta kostnader för IT-utveckling, utan – baserat på ett livscykelperspektiv – också omfatta drift- och förvaltningskostnader samt verksamhetens kostnader för att göra nödvändiga anpassningar, så att den eftersträvade nyttan kan realiseras.
Motivering	Nyttan måste vara styrande och måste vara tydlig innan en lösning utvecklas. Fördelningen av kostnader och nyttor mellan deltagande aktörer är nödvändig att ta fram för att skapa acceptans och förståelse för den förvaltningsgemensamma lösningens hela livscykel. Viktigt är att detta primärt inte ska ske för att effektivisera myndigheternas egen handläggning och verksamhet, utan för att ge ökad nytta utifrån ett medborgarperspektiv.
Konsekvens	Varje satsning kräver att man tar fram en behovs- och nyttoanalys för att tydliggöra både kostnader och nyttor, innan ett beslut tas om att utveckla en ny tjänst/process. Denna analys ska kontinuerligt följas upp och säkerställa att en positiv, förstådd och mätbar nettonytta verkligen realiseras. Utvecklingen av förvaltningsgemensamma lösningar kan innebära komplexa kostnads- och nyttomodeller, t.ex. kan de nyttor som realiseras av en gemensam lösning uppkomma hos andra myndigheter än den som gjorde investeringen, vilket påverkar såväl incitament att delta som finansierings- och förvaltningsmodeller. Vissa satsningar kommer således att bära sig själva, medan andra måste förstås som möjliggörare för utveckling av andra lösningar. Finansieringsmodeller bör utarbetas, där det tydligt framgår hur kostnader och intäkter fördelas. Se även Vägledningar för Nyttorealisering och Behovsdriven utveckling, samt Översikt över finansieringsformer för e-förvaltning.

4 Arkitekturprinciper

4.1 Digitala möten

4.1.1 Låt digitala kanaler vara det primära alternativet

D1 – Låt digitala kanaler vara det primära alternativet	
Beskrivning	Digitala kanaler bör vara det primära alternativet för medborgarnas möten med den offentliga förvaltningen. Vid framtagande av nya digitala tjänster måste en analys göras av om det är nödvändigt att över huvud taget utveckla en traditionell, pappersbaserad kanal för medborgaren. Principen bör gälla gentemot medborgarna under hela ärendekedjan; vid inregistrering av ett ärende, vid kompletteringar, beslut etc.
Motivering	Informationskvaliteten höjs när allt sker i en obruten, digital kedja (se grundprincip G1). Detta minskar risken för felregistreringar och feltolkningar, samt möjliggör ökad automatisering av myndigheternas verksamhetsprocesser, vilket i sin tur minskar förvaltningskostnader och förkortar handläggningstider. Genom att erbjuda medborgarna möjligheten att lämna information via digitala kanaler, istället för via formaliserade och standardiserade blanketter, minskar kostnaderna för att ta fram, skriva ut, skanna, ankomstregistrera, tolka och slutförvara sådana blanketter. Vidare är en övergång från analog, pappersbaserad ärendehantering till digital hantering mer miljövänlig.
Konsekvens	Myndigheter kan aldrig frånsäga sig medborgarens rätt att sända in pappersbaserade brev och ansökningar, rutiner måste därför finnas för att manuellt digitalisera sådana brevbaserade ansökningar. Funktioner behöver per myndighet tas fram för att digitalt sända ut kompletteringsönskemål, beslut etc, t.ex. via Mina meddelanden, inklusive notifieringsfunktioner. Juridiska aspekter behöver utredas. Se även Vägledning kring elektroniska original, kopior och avskrifter, samt Juridisk vägledning

4.1.2 Anpassa till olika gruppers och individers behov

D2 – Anpassa till olika gruppers och individers behov	
Beskrivning	Det digitala mötet måste utformas så att medborgarna kan styra sina processer utifrån egna preferenser och egna behov. Detta inkluderar perspektiven information, tjänster, processer samt individualisering. Exempelvis kan möjligheterna till individualisering förbättras genom fördefinierade mallar/mönster på webbplatser som täcker in olika livshändelser, t.ex. inför pensionering, vid barns födelse eller vid långvarig sjukdom. Sådana mallar ska tas fram av den myndighet som utses att ha huvudansvar att hantera en sådan händelse. En viktig aspekt är att e-tjänsterna måste utformas med hög användbarhet; med smidig inloggning, med bra hjälpfunktioner och då med enhetliga gränssnitt Offentlig sektor måste utnyttja teknikens möjligheter till att stötta, informera och utbilda i syfte att minska det "digitala utanförskapet". Webbplatser och e-tjänster ska utformas för att kunna inkludera personer med funktionsnedsättningar. Exempelvis ska användarna erbjudas möjligheter att ändra fontstorlek, få sidan uppläst eller få digital assistans. Vägledning för ökad tillgänglighet ska följas. Den övergripande rekommendationen i den vägledningen utgår från W3C:s Content Accessibility Guide. För den som inte själv kan genomföra sina digitala möten bör det finnas möjlighet att på sikt använda Mina fullmakter. Vidare kan det finnas behov inom en familj att kunna dela på information, stödja anhöriga och efterlevande etc.
Motivering	Det digitala mötet ska ske på medborgarnas villkor, medborgarna ska själva kunna anpassa sina egna digitala miljöer och sina egna processer. Dessa ska kunna optimeras för aktuell livssituation, med en mix av offentliga och privata tjänster. Ett exempel kan vara att vid tillfällig vård av sjukt barn kunna anmäla detta till Försäkringskassan, arbetsgivaren, förskolan och andra berörda, helst i ett enda arbetssteg. Avsikten är vidare att minska det ”digitala utanförskapet” så att det digitala mötet inte utvecklas till en angelägenhet enbart för datorvana personer med full funktionsförmåga. Istället har alla rätt att kunna delta utifrån sina förutsättningar. Som ett alternativ ska en medborgare via en fullmakt kunna delegera arbetet till personer som medborgaren utsett.
Konsekvens	Myndigheter måste i förlängningen förändra sina digitala kanaler så att de kan individanpassas. Hjälp och förklaringar ska finnas på de fem officiella minoritetsspråken, samt bör finnas på de mest vanliga invandrarspråken. En förvaltningsgemensam tjänst behöver etableras och göras åtkomlig i alla kanaler där användarna interagerar. Tjänsten kan lagra personliga uppgifter som telefonnummer eller lagra mina inställningar, exempelvis av önskad fontstorlek. Juridiska aspekter för att kunna realisera detta måste undersökas. Externa granskningar av tillgänglighet bör ske av fristående organisationer och företag.

4.1.3 Öka medborgarnas insyn och möjligheter att påverka

D3 – Öka medborgarnas insyn och möjligheter att påverka	
Beskrivning	Intresserade medborgare ska kunna vara delaktiga vid utveckling av gemensamma eller myndighetsspecifika processer och tjänster; vid planering, utformning av användargränssnitt, uttestning etc. Användarna ska kunna recensera och betygsätta e-tjänster. Även inom andra områden kan medborgarnas delaktighet öka, t.ex. i kommunalpolitiska frågor. Den enskilde medborgaren ska även få insyn i sina pågående och avslutade ärenden hos olika myndigheter och se hur dennes ärendeprocesser framskrider, t.ex. via Mina ärenden eller liknande sammanställningar.
Motivering	Ökad delaktighet ger större kundnytta genom att efterfrågade tjänster tas fram med högre kvalitet. Konsumentnyttan ökar genom att bättre och mer användbara tjänster kommer fram och omvänt att dåliga tjänster rensas ut eller förbättras. Kunskap om status för egna ärenden minskar trycket på myndigheternas kundtjänster med frågor om ärendestatus etc.
Konsekvens	Referensgrupper och fokusgrupper kan användas för att kvalitetssäkra och förbättra tjänsterna. Funktioner behövs för att recensera nya e-tjänster innan nedladdning från marknadsplatser, samt behövs möjligheter till betygssättning och kommentarsfält implementeras. Enhetlighet i utformning av Mina ärenden underlättar kundupplevelsen, men kräver gemensam vägledning i hur detta bör ske.

4.1.4 Öppna upp för externa innovatörer

D4 – Öppna upp för externa innovatörer	
Beskrivning	Arkitekturen ska underlätta nya lösningar som kan utvecklas av både myndigheter och marknadens aktörer. Fristående utveckling av externa innovatörer ska uppmuntras, inte minst för de digitala kanaler där användarna finns i vardagen. Offentlig sektor ska tillgängliggöra publik information, från vilken externa aktörer kan utveckla egna tjänster att erbjuda medborgarna. Sådana externa innovatörer måste få tillgång till utvecklingsplaner för tjänster och för utformning av gränssnitt etc.
Motivering	Med fristående utveckling skapas förutsättningar för att kunna driftsätta nya e-tjänster helt fristående från varandra och därmed öka leveranstakten av sådana e-tjänster, samt få bort oönskade beroenden dem emellan. Externa innovatörer ger dessutom möjligheter till nya infallsvinklar, idéer och lösningar som drar nytta av den potential som möjliggörs i nya digitala kanaler.
Konsekvens	En konsekvens blir att en offentlig aktör inte alltid kommer att äga det digitala mötet i sig, utan snarare vara informationslämnare. Istället kommer olika nätverk, ofta sektorsvisa, att samverka kring utveckling av nya tjänster. Tydligt definierade ”digitala ekosystem” kommer att involvera externa utvecklare som behöver ha tillgång till fastlagda utvecklingsplaner, kunna påverka gränssnitt etc. För att uppmuntra extern innovation kan det per samverkansområde behöva byggas upp utvecklingsforum, liknande vad som finns vid utveckling av system och infrastruktur baserade på öppen källkod.

För att möjliggöra nya innovativa lösningar krävs att:

- det finns ekonomiska modeller som uppmuntrar och underlättar extern tjänsteutveckling
- bastjänster med enhetliga gränssnitt tillgängliggörs för externa innovatörer, se även princip T4.
- det finns marknadsplatser för fristående appar och för komponenter som kan användas på befintliga webbplatser
- krav ställs på bakomliggande tjänster, bl.a. avseende tillgänglighet
- juridiska överväganden är klarlagda
- säkerhet och personlig integritet beaktas.

4.1.5 Återanvänd redan inlämnad information

D5 – Återanvänd redan inlämnad information	
Beskrivning	En uppgift ska endast behöva lämnas en gång till offentlig förvaltning. På samma sätt ska uppgifter som tagits fram av en myndighet kunna användas av andra aktörer i den offentliga förvaltningen. För att underlätta det digitala mötet bör uppgifter som redan finns registrerade kunna återanvändas och t.ex. förifyllas i e-tjänster. Det bör vidare gå att mellanlagra t.ex. ett elektroniskt formulär där ifyllnad pågår, för att fortsätta vid ett senare tillfälle.
Motivering	En privatperson eller ett företag ska bara behöva registrera sina uppgifter en gång, finns informationen inom offentlig förvaltning ska den inte behöva efterfrågas flera gånger vid ärendehandläggning. Samtidigt måste individer kunna lita på att uppgifter om dem endast används för direkt myndighetsutövning.
Konsekvens	Bastjänster måste finnas för att tillhandahålla befintliga grunduppgifter om framförallt fysisk person, juridisk person, fastighet, företag och fordon. Gemensamma begrepps- och informationsmodeller kan behöva tas fram, se T1. Medborgarens integritet och känsla av kontroll ska behållas. Detta innebär att medborgaren måste ha möjlighet att överblicka användningen av sin information så att denna inte återanvänds inom offentlig förvaltning eller bland kommersiella företag med ett syfte som medborgaren inte har kontroll över. Information bör endast lagras på ett enda ställe. E-tjänster behöver utformas för att kunna mellanlagra uppgifter som fylls i. Även myndigheternas verksamhetssystem behöver successivt anpassas för att erbjuda detta stöd. Affärsmässiga aspekter och juridiska aspekter kring gällande rätt behöver utredas, bl.a. i förhållande till Offentlighets- och Sekretesslagen (OSL). Se även Juridisk vägledning för verksamhetsutveckling inom e-förvaltning.

4.2 Tjänste- och processamverkan

4.2.1 Bestäm och tillämpa gemensamma begrepp, modeller och mönster

T1 – Bestäm och tillämpa gemensamma begrepp, modeller och mönster

För att kunna utveckla en samverkande e-förvaltning krävs att gemensamma begrepp, modeller och mönster [4] tillämpas för information som används över organisationsgränserna.

Fyra begreppsområden kan identifieras:

- **Grunddata**, t.ex. organisationsnummer och personnummer måste formatmässigt vara lika över alla e-tjänster.
- **Standardiserade informationsstrukturer,** t.ex. datum, metadata om ärenden eller arkivobjekt, kontaktinformation och kalenderuppgifter.
- **Sektorsvis information** inom t.ex. vård och omsorg, skolan, pensionsområdet eller fastighetssektorn.
- **Gemensamma koder och variabler,** t.ex. kommunkoder eller sjukvårdens HSA-katalog.

Grundläggande begrepp bestäms och ansvaras för av den myndighet som tillhandahåller respektive grunddata. Standardiserade informationsstrukturer bestäms och förvaltas på nationell nivå, medan sektorsvis information och gemensamma koder bestäms och förvaltas bäst av aktörer som är aktiva inom respektive verksamhetsområde.

Motivering

Väldefinierade begrepps- och informationsmodeller är en förutsättning för en samverkande e-förvaltning och för att tillhandahålla information för extern vidareförädling.

Det finns ofta ett stort behov av samverkan mellan aktörer som är verksamma inom samma sektor eller verksamhetsområde. En sammanhållen och kostnadseffektiv förvaltning av delade informationsresurser underlättas ofta om dessa hanteras som sektorsgemensamma tillgångar.

Konsekvens

Att upprätta och underhålla gemensamma begrepps- och informationsmodeller är ett stort arbete som kräver kontinuerliga insatser. Det är därför viktigt att aktörerna inom ramen för samverkan tar aktiva beslut kring vilka gemensamma beskrivningar som faktiskt behövs, och omfattningen av dessa.

I många fall kan en organisation utpekas som både begrepps- och informationsägare, men det kan också vara ett delat ansvar. Ett exempel på det senare kan vara att en nationell begreppsmodell för plan- och byggprocessen hanteras av en aktör (begreppsansvar) men ansvaret för informationen i sig fördelas på 290 kommuner. Se vidare Vägledning för digital samverkan.

Aktörerna som behöver samverka inom en sektor där samverkansorganisation saknas behöver dels komma överens om hur ansvaret ska fördelas mellan parterna, dels söka sektor- och situationsanpassade lösningar av finansieringsfrågorna.

Begrepps- och informationsägare behöver utses både för basinformation (person, fastighet etc.) och för sektorsvis information, t.ex. socialförsäkring, skola samt vård- och omsorg.

Uppgifter om begrepps- och informationsmodeller ska principiellt tillhandahållas fritt som öppet data.

[4] Med mönster avses att återanvända strukturer och arbetssätt.

4.2.2 Tillgängliggör och återanvänd information och tjänster på ett enhetligt sätt

T2 – Tillgängliggör och återanvänd information och tjänster på ett enhetligt sätt	
Beskrivning	Genom ett förskjutet fokus från myndighetscentrerat till digitala möten på medborgarnas villkor, ställs krav på att tjänster som utvecklas av myndigheter och andra aktörer använder enhetliga tjänstegränssnitt, begrepp och informationsmängder. För att möjliggöra detta behövs en samverkansarkitektur, som möjliggör informationsutbyte via tjänster. Se Vägledning för digital samverkan för en beskrivning av samverkansarkitektur. En viktig aspekt är här att myndigheternas information – i basal eller aggregerad form – ska kunna tillgängliggöras för externa aktörer, vilket en samverkansarkitektur måste stödja. Sektorsvis kommer en mer detaljerad samverkan att behövas, t.ex. inom vård och omsorg, socialförsäkrings-, geodata- eller pensionsområdena. Inom respektive sektor kan branschvisa standarder behöva tas fram och förvaltas. Ett speciellt område är tillgängliggörandet av Öppen data[5]/PSI[6], när myndigheternas information ska tillgängliggöras för externa parter i så stor omfattning som möjligt, med beaktande av sekretess- och integritetsaspekter.
Motivering	Genom att tillgängliggöra tjänster enligt denna grundprincip kan information i bastjänster återanvändas inom eller utanför de egna organisationsgränserna inom hela ”koncernen Sverige”, vilket möjliggör nya tillämpningsområden. Detta ger en enhetlighet som underlättar utformning av nya och mer effektiva lösningar, vilka kan baseras på andras tjänsteutbud. Det finns vidare en stor potential i att externa innovatörer kan utveckla och erbjuda nya tjänster baserade på offentlig information. Fördelarna med att återanvända verksamhetsprocesser, bastjänster, e-tjänster och förvaltningsgemensamma tjänster är att: • återanvändning ger minskade utvecklings- och förvaltningskostnader • det finns ett utpekat ansvar för utveckling och förvaltning • återanvändning ger kortare utvecklingstid • användarna känner igen sig genom att gränssnitten i olika e-tjänster kan ha liknande utformning och beteende • medborgarna får bättre stöd för sina kundprocesser som går tvärs över olika myndighetet • driftkostnaden för förvaltningsgemensamma tjänster kan bli lägre med gemensam drift Öppen data möjliggör innovation samt leder dessutom till större transparens, genom att felaktiga grunddata blir synliga, vilket i sin tur kan öka informationskvaliteten.
Konsekvens	Det finns idag fungerande processer och tjänster som tillhandahålls av enskilda myndigheter. Syftet är inte att bryta upp och bygga om dessa, nya tjänster kan dock behöva utvecklas så att återanvändning blir möjlig. En rekommendation är att om en myndighet utvecklar en ny, egen e-tjänst för sina kunder, bör denna internt anropa egna bastjänster för sin informationsförsörjning. Detta möjliggör att myndigheten framöver kan tillhandahålla information via sådana bastjänster för förädling av externa innovatörer. För varje sektor behöver de inblandade aktörerna utse en som är sektorsansvarig. I de flesta fall finns dock en naturlig färdledare. För att kunna samverka kring förvaltningsgemensamma tjänster (FGT) krävs

[5] Med Öppen data eller Publik information avses i detta dokument digital information som är fritt tillgänglig utan inskränkningar.
[6] Med PSI (Public Sector Information), avses i detta dokument uppfyllande av EU:s PSI-direktiv som genomförs i Sverige genom lagen (2010:566) om vidareutnyttjande av handlingar från den offentliga förvaltningen.

specifikt att:

- ansvar för och skyldighet att tillhandahålla tjänster fastställs
- det bildas samverkansgrupper/federationer kring sådana tjänster
- olika intressenter tar på sig att utveckla och förvalta sådana FGT
- detta samordnas och prioriteras på nationell nivå
- det finns en ekonomisk modell kring finansiering av utveckling, förvaltning och drift
- vägledningar tas fram för hur FGT på ett samordnat sätt ska möta användarna i olika digitala möten
- en gemensam supportfunktion kan behöva etableras
- anvisningar tas fram för hur FGT ska kunna interagera med myndigheternas egna kanallösningar
- drift av FGT, inklusive lagring av gemensamma uppgifter, sker på ett sätt som upprätthåller hög personlig integritet
- privata alternativ möjliggörs, både av konkurrensskäl och för att få nya impulser
- juridiska överväganden är hanterade.

Se även Vägledningar för Digital samverkan, Nyttorealisering och Behovsdriven utveckling.

Semantiska tekniker ska användas för att beskriva data och göra den fritt tillgänglig i ett format som är möjligt att söka och tolka via system. Tillhörande begrepps- och informationsmodeller samt utbytesformat ska fritt publiceras.

Beaktande av sekretess- och integritetsaspekter vid utlämning av publik information/PSI, innebär att möjligheterna att tillgängliggöra personuppgifter är begränsade.

Det ska öppet och fritt på en myndighets webbplats publiceras vilken information en myndighet innehar och hur den kan tillgängliggöras. Tjänster med publik information ska publiceras i tjänstekataloger.

Se vidare Vägledning för vidareutnyttjande av offentlig information.

4.2.3 Bygg tjänstebaserat

T3 – Bygg tjänstebaserat	
Beskrivning	Information och funktioner som ska göras tillgängliga för digital samverkan ska tillhandahållas som tjänster. En tydlig tjänstebaserad arkitektur (”Service Oriented Architecture”), bör därför införas tvärs myndigheterna för att kunna erbjuda sådana tjänster. Denna arkitektur ger lösa kopplingar samt gör beroenden explicita och synliga. Alla tjänster ska i sig vara versionshanterade. Flera versioner ska kunna användas samtidigt, för att möjliggöra successiva övergångar. Det ska även finnas testversioner av tjänsterna.
Motivering	Genom att exponera bastjänster uppnås en lös koppling mellan producenter och konsumenter, där gränssnitten för tjänsterna blir vad som avtalas och definieras, medan bakomliggande verksamhets- och IT-system döljs. Den lösa kopplingen gör vidare att tjänsterna bli mer okänsliga för förändringar, t.ex. när flera olika versioner kan tillhandahållas och samexistera parallellt. Tjänster utformade på dessa grunder är modulära, möjliga att distribuera, upptäckbara, utbytbara och återanvändbara samt bygger på upprättade gränssnittskontrakt/tjänstekontrakt, vilka måste versionshanteras och förvaltas. Tillgång till bastjänster ger möjlighet att kombinera och förädla exponerad information, här finns möjligheter för externa parter att ta fram innovativa lösningar. Återanvändning är också en stark drivkraft för tjänsteorientering av samverkans-arkitekturen.
Konsekvens	Teknisk kompetens inom tjänsteorientering krävs av de parter som samverkar och av dem som har ansvar för samverkansarkitekturen. Utvecklare av sådana tjänster är beroende av att test- och utvecklingsmiljöer samt testdata finns tillgängliga. Det bör finnas publicerade protokoll över vilka verifierande tester som har utförts vid utveckling av en tjänst. Inom specifika sektorer med känslig information bör en certifiering av godkända tjänster övervägas. Anvisningar behöver tas fram och förvaltas över vilka tekniska gränssnitt som ska stödjas över tiden. Gränssnittskontrakt/tjänstekontrakt behöver förvaltas. Det ska finnas tjänstekataloger som på ett enhetligt sätt förtecknar och beskriver de tjänster som kan erbjudas, med tydlig beskrivning av tjänstens innehåll och förutsättningar. Sökning ska kunna ske sömlöst i sådana kataloger, dvs. man ska inte behöva veta deras interna strukturer och relationer. Kataloger ska upplevas som globala vid sökning och lokala vid administration. Vidare behöver bestämmas vilket metadata som ska finnas i sådana kataloger. Över tid kommer lasten att variera och troligen öka, vilket ingående tjänster behöver kunna hantera. Tjänsternas skalbarhet behöver därför beaktas redan vid deras utformning så att de kan skalas upp vid behov, utan omfattande omkonstruktion. Tjänsteproducenter har också ett ansvar för att tillhandahålla testdata. Ansvaret för varje sådan tillgång kräver verksamhetskunskap och bör placeras hos en aktör som är centralt verksam inom sin sektor. På sikt bör nya verksamhetssystem byggas med tjänstegränssnitt från början, för att undvika efterföljande utveckling av extra lager av bastjänster.

4.2.4 Hämta information vid källan

T4 – Hämta information vid källan	
Beskrivning	Huvudprincipen är att alltid hämta information så nära källan som möjligt, hos den som producerar och tillhandahåller informationen.
Motivering	Genom att hämta information vid källan säkerställs att informationen är tillförlitlig och aktuell samt att utlämnande aktör kan identifiera och logga vem (vilken organisation) som får tillgång till informationsklassad information.
Konsekvens	Begrepps- och informationsägaransvaret måste vara utrett och klarlagt. Medborgaren bör ges möjlighet att i användargränssnittet överblicka var informationen har inhämtats om den har inhämtats från annan källa än den aktuella myndigheten. Källan till informationen behöver vara känd och tillgänglig. De organisationer som har information som efterfrågas av andra aktörer behöver tillgängliggöra den informationen. Det är den som ansvarar för källan som ska varsla om förändrade uppgifter och fatta beslut om uppdateringar. På grund av höga krav på prestanda och tillgänglighet kan information behöva mellanlagras högre upp i informationskedjan. När informationen av olika skäl behöver mellanlagras kan ansvaret för identifiering och loggning behöva överföras till mellanlagrande myndighet. Kopior och mellanlagring av information bör undvikas. I de fall kopior eller mellanlagring krävs, ska konsistens mot originalet eftersträvas.

4.2.5 Använd öppna standarder

T5 – Använd öppna standarder[7]	
Beskrivning	När gränssnitt för information och tjänster utformas ska i första hand öppna standarder användas. En standards mognad och etableringsgrad behöver även beaktas för att valet av standard inte ska utgöra ett hinder för samverkan. Om lämpliga öppna standarder saknas ska etablerade branschstandarder användas. Proprietära, slutna standarder ska så långt det är möjligt undvikas. Valet av standarder ska inte inkräkta på samverkande parters rätt att välja intern teknisk plattform för produktion eller konsumtion av tjänster.
Motivering	Standardiserade gränssnitt sänker kostnader och bidrar till ökad återanvändning och en öppen marknad (jämför med standardiserad spårbredd för järnväg, format på elektriska kontakter eller e-post). Öppna standarder är att föredra eftersom de kan användas fritt utan att ägaren av standarden sätter upp orimliga eller diskriminerande hinder, kostnader eller avtalsmässiga begränsningar. Proprietära lösningar medför inlåsningseffekter som kan få oönskade ekonomiska och praktiska konsekvenser för de samverkande parterna.
Konsekvens	Beställare av tjänster behöver ställa krav på att plattformsoberoendet säkerställs genom praktiska tester.

[7] En öppen standard är en standard som, i motsats till en proprietär teknisk specifikation, tillåter vem som helst att implementera den utan att ägaren av standarden sätter upp orimliga eller diskriminerande hinder

4.3 Informationssäkerhet och juridik

4.3.1 Bedriv ett riskbaserat informationssäkerhetsarbete

S1 – Bedriv ett riskbaserat informationssäkerhetsarbete	
Beskrivning	Informationshanteringen vid digital samverkan bör ses i ett livscykelperspektiv där roller och ansvar för informationssäkerheten ska vara fastställda från det att en tjänst initieras, utvecklas, driftssätts och förvaltas, fram till dess att den slutligen avvecklas. Två centrala roller i detta hänseende är informationsägare respektive tjänsteproducent, se även Vägledning för digital samverkan, fördjupning om roller. När en tjänst utvecklas ska informationsägarna identifieras och ges möjlighet att formulera relevanta och nödvändiga informationssäkerhetskrav. Kraven som ställs ska baseras på kunskap om den information som hanteras, samt vilka hot och risker som bedöms föreligga i och eller mot informationen och informationshanteringen. Kunskapen inhämtas genom riskanalys och informationsklassning. MSB har tagit fram modeller för informationsklassning respektive riskanalys som kan användas vid genomförandet.
Motivering	Informationssäkerhet i tjänster ska bygga på en bedömning av aktuella risker och hur dessa ska reduceras. Genom informationsklassning formulerar informationsägaren sin riskbedömning och överför den i form av säkerhetskrav till tjänsteproducenten. Genom att arbeta strukturerat med informationsklassning och riskanalys förenklas kravställningsproceduren vilket även innebär en ökad grad av effektivitet och möjlighet att höja kvaliteten i informationshanteringen. Därutöver kan det även leda till lägre kostnader då man tidigt kan planera för en balanserad säkerhetsnivå i form av krav på arkitektur och på design av lösningen.
Konsekvens	Säkerhetsåtgärderna ska omfatta skydd i lagring och i kommunikation samt gälla samtliga aspekter: konfidentialitet, riktighet, spårbarhet och tillgänglighet. Av särskild betydelse är att klarlägga ansvarsförhållanden då informationsmängder från flera informationsägare sammanförs i en och samma tjänst. Om tjänsten är av sådan art att störningar i tjänsten bedöms kunna få konsekvenser av nationell betydelse, ska detta särskilt beaktas och bedömas i riskanalysen. Den som ansvarar för hela tjänsten, tjänsteproducenten, svarar i sin tur för att det genomförs en riskanalys för lösningen som helhet och att särskild hänsyn tas till operationella och eller säkerhetsrelaterade risker i tjänsten. Tjänsteproducenten ska ha dokumenterade rutiner för att säkerställa att regelbundna interna och externa efterlevnadskontroller av säkerheten genomförs. I händelse av att tjänsten eller systemet ska avvecklas ansvarar tjänsteproducenten för att planera för och genomföra en avveckling på ett strukturerat sätt, så att informationssäkerhetskraven kan upprätthållas genom hela avvecklingsprocessen. En tjänsteproducent ska bedriva ett förebyggande och systematiskt arbete för att kunna hantera inträffade incidenter och för att säkerställa kontinuitet i leveransen, se även Vägledning för digital samverkan. Detta kräver att man har färdiga rutiner och metoder för att bl.a. anmäla, analysera, prioritera, eskalera, rapportera och utvärdera incidenter. Kontinuitetsplanering innebär i det här sammanhanget att ha rutiner och metoder för att prioritera samverkanstjänster, hantera störningar, reducera negativa konsekvenser av sådana, ha alternativa leveranssätt samt kommunicera respektive återställa till normalläge. Tjänster ska vara utvecklade och driftsatta för att kunna motstå olika typer av yttre och inre angrepp.

4.3.2 Skydda den personliga integriteten

S2 – Skydda den personliga integriteten

Beskrivning

Det är alltid den som bestämmer över hanteringen av personuppgifter som har ansvar för att personuppgiftslagen (PuL) följs. Ansvaret innebär att se till att de tjänster som används inte medför integritetsrisker och därför måste tydliga krav formuleras på dem som levererar tjänsterna. Vid utformning av en ny tjänst ska en analys göras av vilka personuppgifter som är relevanta att samla in och hantera.

Några grundläggande principer inom integritetsskydd är att inte samla in mer information än vad som behövs, inte ha kvar den längre än man behöver och inte använda den till något annat än vad man samlade in den för.

Motivering

Utveckling av digitala tjänster är ofta komplicerade processer där man måste ta hänsyn till många typer av krav, inte minst gäller det skydd av den personliga integriteten. För att undvika fallgropar som blir dyra att åtgärda i efterhand och som gör det svårt att följa lagen är det viktigt att ta hänsyn till integritetsaspekterna i ett tidigt skede av processen.

Att informera om hur uppgifterna ska behandlas, att begära samtycke och att tillåta insyn i den vidare hanteringen är också viktiga led i integritetsskyddet.

Om tjänsten ska hantera personuppgifter bör Datainspektionens Rekommendation för ”Privacy by design” (inbyggd integritet) tillämpas. Begreppet går ut på att låta integritetsfrågorna påverka systemets hela livscykel – från förstudie och kravställning via design och utveckling till användning och avveckling.

Konsekvens

Till skydd av integritetskänsliga uppgifter finns det vissa specifika åtgärder som bör beaktas. För att upprätthålla Privacy by design bör man eftersträva att:

- minimera mängden personuppgifter
- begränsa åtkomsten till uppgifterna
- skydda uppgifterna
- låta tjänsten styra användaren rätt.

Speciellt måste man beakta att sammansatt information från flera källor kan kräva en högre klassificering.

Möjligheten för systemadministrativ personal att arbeta med och ta del av personuppgifter ska begränsas till dem som behöver detta för att kunna utföra sina arbetsuppgifter. Kryptering av lagrad information kan vara ett ytterligare sätt att begränsa åtkomsten.

Vid uttestning av digitala samverkanslösningar bör testdata inte innehålla riktiga personuppgifter.

Loggar och säkerhetskopior kan i sig själva innebära en integritetsrisk. Loggar kan till exempel innehålla personuppgifter och måste därför hanteras på ett integritetssäkert sätt. Säkerhetskopior som sparas länge kan komma att innehålla personuppgifter som borde raderats tidigare etc.

4.3.3 Beakta informationens skyddsvärde i hela kedjan

S3 – Beakta informationens skyddsvärde i hela kedjan	
Beskrivning	Informationsägaren tillhandahåller information som ska förädlas och/eller exponeras i tjänster för medborgarna. Informationskedjan sträcker sig hela vägen från det att informationen skapas, via förmedling och förädling mellan olika aktörer till dess att informationen gallras ut och försvinner. Tjänsteproducenten ska upprätta och upprätthålla nödvändiga skyddsnivåer, baserade på informationens skyddsvärde och fastställda av informationsägaren. Informationens skyddsvärde ska baseras på gjord informationssäkerhets-klassning. Skyddsnivåerna ska utformas med hänsyn tagen till krav på konfiden-tialitet, riktighet, tillgänglighet och spårbarhet. Kraven på skydd ska uppfyllas även hos eventuella underleverantörer. Det kan vara nödvändigt med förnyad informationsklassning om nya kombina-tioner av information skapas vid digital samverkan. Skyddet ska bestå av en kombination av organisatoriska, tekniska och fysiska åtgärder, se nedan.
Motivering	Skyddsvärdet måste beaktas i hela kedjan för att säkerställa att informationen inte kommer i orätta händer eller att den förvanskas på vägen. Uppfylls inte detta kan det leda till svåra konsekvenser för den enskilde eller för de aktörer som direkt berörs av informationen. Det kan också innebära att den aktör som ska tillhanda-hålla informationen väljer att inte längre göra det och påverkar också tilliten negativt mellan de aktörer som berörs.
Konsekvens	Informationsägarens ansvar är att se till att hela informationskedjan förblir säker-hetsmässigt intakt, denne måste därför analysera vilka svaga delar som kan finnas och vilka skyddsåtgärder som krävs. **Organisatoriskt** skydd innefattar bl.a. roller och ansvar, policys, rutiner och instruktioner. Varje organisation som ansvarar för en del av informationskedjan måste säkerställa att roller och ansvar tydliggörs, samt att nödvändiga rutiner och instruktioner finns för att organisationens medarbetare ska kunna fullgöra sitt ansvar. **Tekniskt** skydd innefattar bl.a. behörighetssystem, identifiering, signering, logg-ning och spårning. Producerande aktörer måste säkerställa att loggning görs samt att mottagande aktörer har rätt behörighet att ta emot informationen. Detta behöver också fastställas i en överenskommelse. Ansvaret för behörighetskontroll på individnivå ligger däremot vanligtvis på den mottagande aktören, dvs. den part som begär åtkomst har ansvar för att administrera behörigheten för sina använ-dare. Varje aktör har ansvar för att upprätthålla informationens skyddsvärde inom den egna organisationen. För tjänster mot medborgare ska Svensk e-legitimation[8] tillämpas som grundalter-nativ för identifiering och signering. **Fysiskt** skydd innefattar bl.a. skalskydd och kryptering, vilka ska utformas utgående från gjord informationssäkerhetsklassning. Kryptering ska övervägas vid kommunikation över Internet, i databaser och av mobila enheter. Användning av det säkra myndighetsnätverket SGSI (Swedish Government Secure Intranet) bör övervägas.

[8] Svensk e-legitimation är en identitetsfederation baserad på intygshantering och har olika nivåer för identifiering

4.3.4 Analysera rättsliga förutsättningar

S4 – Analysera rättsliga förutsättningar

Beskrivning

Vid en utvecklingsinsats bör en analys göras i ett tidigt skede av vilka lagar och förordningar som påverkar önskad funktionalitet. Utgående från en sådan analys kan lämpliga lösningar värderas ut ett juridiskt perspektiv.

Arkitekturen ska då täcka balanserade avvägningar mellan berörda intressen avseende funktionalitet och effektivitet å ena sidan och informationssäkerhet, rättssäkerhet samt integritetsskydd å den andra.

Självklart ska funktioner och tjänster som tas fram vara förenliga med gällande rätt.

Flera olika aspekter behöver beaktas av informationsägaren, specifikt när information ska publiceras som Öppna data/PSI. Dokument som innehåller något av följande behöver inventeras och kan behöva undantas vid publicering:

- **Personuppgifter** - innehåller uppgifter som direkt eller indirekt kan hänföras till en fysisk person vilken är i livet. Uppgifterna kan dessutom vara känsliga enligt PuL
- **Sekretessreglerad information** - t.ex. omsorgs- och vårddokumentation som ej får lämnas ut utan menprövning.
- **Upphovsrätt och andra immateriella rättigheter** - t.ex. kring fotografier, litterära verk samt rättigheter till programvaror.

För att sekretess- och integritetsaspekterna ska tillgodoses när en ny datamängd görs tillgänglig behöver även konsekvenser beaktas av att denna information kan kombineras med andra tillgängliga datakällor.

Motivering

Det måste verifieras att planerade tjänster är genomförbara utifrån de förutsättningar som olika lagar och föreskrifter ger: tryckfrihetsförordningens bestämmelser om allmänna handling (offentlighetsprincipen m.m.), personuppgiftslagen, offentlighets- och sekretesslagen, patientdatalagen, socialtjänstlagen, arkivlagen m.fl.

Beroende på de juridiska förutsättningarna kan utformning av tjänster påverkas, alternativt visa att det saknas juridiska förutsättningar för att ta fram en sådan tjänst.

Konsekvens

Rättslig expertis bör involveras tidigt när en tjänst ska utvecklas. I arbetet bör också personuppgiftsombud delta, när sådant ombud finns.

Även rättsliga förutsättningar och regelverk vid informationsutbyte mellan myndigheter bör beaktas.

Se även vägledningen Direktåtkomst och utlämnande på medium för automatiserad behandling, Juridisk vägledning för verksamhetsutveckling inom e-förvaltning, Checklista för jurister samt SOU 2014:39, Så enkelt som möjligt för så många som möjligt - Bättre juridiska förutsättningar för samverkan och service.

Bilaga 1, Referenser

Ref	Objekt
1	European Interoperability Framework (EIF)
2	Med medborgaren i centrum
3	Riktlinjer för myndigheters användning av sociala medier
4	Vägledning i nyttorealisering
5	Vägledning för behovsdriven utveckling
6	Vägledning för vidareutnyttjande av offentlig information
7	Översikt över finansieringsformer för e-förvaltning
8	Vägledning kring elektroniska original, kopior och avskrifter
9	Juridisk vägledning för verksamhetsutveckling inom e-förvaltning
10	Vägledning för webbutveckling
11	Web Content Accessibility Guidelines (WCAG) 2.03C CAG
12	Direktåtkomst och utlämnande på medium för automatiserad behandling
13	Checklista för jurister
14	SOU 2014:39, Så enkelt som möjligt för så många som möjligt
15	Strategi för informationssäkerhet i e-förvaltning
16	MSB:s föreskrifter om statliga myndigheters informationssäkerhet
17	Datainspektionens rekommendation om ”privacy by design”
18	MSB:s modell för informationsklassning, bilaga E, sidan 22
19	MSB:s modell för riskanalys
20	Vägledning för digital samverkan
21	Vägledning för digital samverkan, fördjupning Roller och överenskommelser

Bilaga 2, Jämförelse European Interoperability Framework

EIF-Principer	Vägledande principer
1 - Subsidiarity and proportionality	G4 Delegera mandat och ansvar
2 - User-centricity	G1 Utgå från medborgarnas livshändelser G2 Låt digitala möten ske på användarnas villkor G5 Låt behov och nytta vara styrande D1 Låt digitala kanaler vara det primära alternativet D3 Öka medborgarens insyn och möjlighet att påverka
3 - Inclusion and accessibility	D4 Öppna upp för externa innovatörer D2 Anpassa till olika gruppers och individers behov D3 Öka medborgarnas insyn och möjligheter att påverka
4 - Security and privacy	G3 Upprätthåll rätt nivå på informationssäkerhet och integritet S1 Bedriv ett riskbaserat informationssäkerhets-arbete S2 Skydda den personliga integriteten S3 Beakta informationens skyddsvärde i hela kedjan S4 Analysera rättsliga förutsättningar
5 - Multilingualism	D2 Anpassa till olika gruppers och individers behov
6 - Administrative simplification	D5 Återanvänd redan inlämnad information
7 - Transparency	G2 Låt digitala möten ske på användarnas villkor D3 Öka medborgarnas insyn och möjligheter att påverka D5 Återanvänd redan inlämnad information
8 - Preservation of information	D5 Återanvänd redan inlämnad information S1 Bedriv ett riskbaserat informationssäkerhets-arbete

9 - Openness	D4 Öppna upp för externa innovatörer D3 Öka medborgarnas insyn och möjligheter att påverka T1 Bestäm och tillämpa gemensamma begrepp, modeller o mönster
10 - Reusability	T2 Tillgängliggör och återanvänd information och tjänster på ett enhetligt sätt D5 Återanvänd redan inlämnad information T1 Bestäm och tillämpa gemensamma begrepp, modeller och mönster T3 Bygg tjänstebaserat T4 Hämta informationen vid källan
11 - Technological neutrality and adaptability	T1 Bestäm och tillämpa gemensamma begrepp. modeller och mönster T2 Tillgängliggör och återanvänd information och tjänster på ett enhetligt sätt T4 Använd öppna standarder
12 - Effectiveness and efficiency	G2 Låt digitala möten ske på användarnas villkor T2 Tillgängliggör och återanvänd information och tjänster på ett enhetligt sätt G4 Delegera mandat och ansvar G5 Låt behov och nytta vara styrande D1 Låt digitala kanaler vara det primära alternativet D5 Återanvänd redan inlämnad information T1 Bestäm och tillämpa gemensamma begrepp. modeller och mönster T3 Bygg tjänstebaserat T4 Hämta information vid källan T5 Använd öppna standarder S2 Skydda den personliga integriteten

Vägledande principer	EIF-Principer
G1 - Utgå från medborgarnas livshändelser	**2**
G2 - Låt digitala möten ske på användarnas villkor	**2, 7, 12**
G3 - Upprätthåll rätt nivå på informationssäkerhet och integritet	**4**
G4 - Delegera mandat och ansvar	**1, 12**
G5 - Låt behov och nytta vara styrande	**2, 12**
D1 - Låt digitala kanaler vara det primära alternativet	**2, 12**
D2 - Anpassa till olika gruppers och individers behov	**3**
D3 - Öka medborgarens insyn och möjligheter att påverka	**2, 3, 5, 9**
D4 - Öppna upp för externa innovatörer	**3, 9**
D5 - Återanvänd redan inlämnad information	**7, 8, 10, 12**
T1 - Bestäm och tillämpa gemensamma begrepp, modeller o mönster	**9, 10, 11, 12**
T2 - Tillgängliggör och återanvänd information och tjänster på ett enhetligt sätt	**10, 11**
T3 - Bygg tjänstebaserat	**10, 12**
T4 - Hämta information vid källan	**12**
T5 - Använd öppna standarder	**11, 12**
S1 - Bedriv ett riskbaserat informationssäkerhetsarbete	**4, 8, 12**
S2 - Skydda den personliga integriteten	**4, 8, 12**
S3 - Beakta informationens skyddsvärde i hela kedjan	**4**
S4 - Analysera rättsliga förutsättningar	**4**