Granskning av regionens styrning och kontroll av användning av applikationer

Region Dalarna

Building a better working world

Innehåll

1. Sammanfattande bedömning och rekommendationer

På uppdrag av regionens förtroendevalda revisorer har EY genomfört en granskning av regionens styrning och kontroll med avseende på användning av applikationer.[1] Syftet med granskningen är att bedöma om regionens styrelse och nämnder har en ändamålsenlig styrning och kontroll över användningen av applikationer i verksamheten.

Användningen av molntjänster med tillhörande applikationer[2] är ett område som berörs av flera lagstiftningar inom olika områden, förordningar och regelverk, myndighetsföreskrifter och rekommendationer. Centrala perspektiv att beakta är intern styrning och kontroll, informationssäkerhet, patientsäkerhet, IT-säkerhet, juridiska samt tekniska risker. Denna granskning berör översiktligt väsentliga risker utifrån regionens styrning, kontroll och uppföljning. Vi vill betona att respektive riskområde är brett och bör granskas separat för att fånga samtliga perspektiv.

Vår sammanfattande bedömning är att regionen inte fullt ut säkerställer en tillräcklig styrning och kontroll avseende användningen av applikationer. Vi ser dock positivt på att det utifrån applikationsrådet finns en struktur för beredning och hantering av avvägningar rörande applikationer och dess användningsområden i verksamheterna. Vår bedömning grundar sig i följande iakttagelser:

- Användningen av applikationer berörs i ordinarie styrning och uppföljning, IT-portföljstyrningen samt hantering i applikationsrådet. Hur dessa strukturer förhåller sig till varandra är emellertid inte tydliggjort.
- Beslutsnivåerna avseende användning av molntjänster med tillhörande applikationer är otydligt, exempelvis när ett ärende ska beslutas av applikationsrådet, regiondirektör respektive regionstyrelsen.
- Det finns ett flertal styrande dokument, riktlinjer och rutiner som belyser väsentliga aspekter i hantering av regionens applikationer. I flera fall saknas det tydliga former för uppföljning och återrapportering.
- Det saknas former för återrapportering till regionstyrelsen avseende de väsentliga risker som är förknippade med användning av applikationer, såsom exempelvis informationssäkerhet.
- Det finns rutiner för genomförande av riskanalyser rörande informationssäkerhet inför behandling i applikationsrådet. Verksamheternas deltagande i dessa analyser varierar, vilket kan påverka analysernas resultat och värde.
- I det stickprov vi har genomfört rörande underlag för applikationer som behandlats av applikationsrådet noterar vi inga väsentliga avvikelser. Dock konstaterar vi att det finns ett mörkertal avseende hur många applikationer i regionen som inte hanterats av applikationsrådet.

Utifrån granskningens iakttagelser ger vi regionstyrelsen följande rekommendationer:

- Tydliggör applikationsrådets roll, mandat och när ärende ska lyftas för beslut av regiondirektör respektive regionstyrelse
- Säkerställ att alla applikationer som är tänkta att behandlas av applikationsrådet blir föremål för applikationsrådets kontroll
- Klargör förhållandet avseende mandat och funktion mellan applikationsrådet, portföljstyrningsmodellen och linjeorganisationen
- Ta fram en modell för uppföljning av applikationsanvändning och utvärdering av regelefterlevnad

[1] En ”app” är en förkortning för ”applikation” vilket i sammanhanget är ett mindre program som är enkelt förpackat utan särskilda installationsprocedurer. Applikationer laddas ner i en smartmobil eller en surfplatta, men kan också vara webbapplikationer som är åtkomliga via en webbrowser på en dator (e-Klient)

[2] Molntjänster är en övergripande benämning på tjänster som innebär att en leverantör tillhandahåller lagring, datorkapacitet, datorprogram, applikationer, funktioner, plattformar eller liknande utanför Region Dalarnas nätverk, oftast i tjänsteleverantörens/ hostingleverantörens egna datorhallar med stöd av elektroniska kommunikationsnät. En stark trend är att många applikationer levereras som molntjänst istället för som enskilda installationer i användarnas egna datorer.

- Säkerställ revidering av riktlinjen avseende molntjänster, för att spegla organisationens arbetssätt. Tydliggör hur riktlinjens efterlevnad ska följas upp och utvärderas.
- Klargör regionens förhållningssätt som vårdgivare avseende förskrivning och rekommendation av applikationer

2. Inledning

2.1 Bakgrund

En ”app” är en förkortning för ”applikation” vilket i sammanhanget är ett mindre program som är enkelt förpackat utan särskilda installationsprocedurer. Applikationer laddas ner i en smartmobil eller en surfplatta, men kan också vara webbapplikationer åtkomliga från en dator och dess webbläsare.

Användningen av applikationer, som är en del i samhällets digitalisering, har ökat dramatiskt under senare år. Inom t ex hälso- och sjukvården finns idag en stor mängd appar som en del i olika e-hälsolösningar. Applikationerna kan röra sig om allt från aviseringsappar inför kommande besök till vårdappar som samlar in och delar patientinformation med vårdgivarna. Även inom andra delar av regionens verksamhet utgör applikationer en del av utvecklingen, t ex inom kollektivtrafiken.

De nya möjligheter utvecklingen av olika applikationer innebär för verksamheten i form av t ex ökad effektivitet och inte minst förutsättningar för förbättringar av t.ex. hälsoläget i befolkningen kan inte underskattas. Samtidigt ska utvecklingen hanteras inom ramen för en komplex lagstiftning som i alla delar inte är anpassad till den rådande utvecklingen. Som ett närliggande exempel kan lyftas fram e-hälsomyndighetens uppdrag, på nationell nivå, om personliga hälsokonton som stoppats efter kritik från Datainspektionen. Men även för en region finns en rad utmaningar kring användningen av applikationer som måste hanteras. Detta gäller t.ex. frågor kring innehåll och lagring av patientuppgifter, ansvar för innehåll i appar om dessa rekommenderas till patienter, förhållandet i relation till LOU vid nyttjande av appar framtagna på kommersiella grunder, förhållandet till GDPR och PDL ur olika perspektiv o s v.

Region Dalarnas uppfattning är att det i skärningspunkten mellan digitaliseringens möjligheter och den komplexa lagstiftningen uppstår betydande risker för regionen. De förtroendevalda revisorerna ser därför starka skäl att granska regionens beredskap och rutiner för användningen av olika appar, såväl direkt som indirekt[3], särskilt utifrån ett juridiskt perspektiv inom hela verksamheten men med särskild inriktning mot hälso- och sjukvården där de bedömer riskerna som störst.

2.2 Syfte och revisionsfrågor

Syftet med granskningen är att bedöma om regionens styrelse och nämnder har en ändamålsenlig styrning och kontroll över användningen av appar i verksamheten. I granskningen besvaras följande revisionsfrågor:

- ☐I vilken utsträckning används appar i regionens verksamheter?
- Finns någon ändamålsenlig uppföljning/kontroll (centralt eller på nämndnivå) över vilka appar som används, såväl direkt som indirekt, i organisationen?
- Har regionen utarbetat, eller planeras, några övergripande styrdokument (ramverk, rekommendationer etc) för användning av appar i regionens verksamhet?
    - Har regionen klargjort olika ansvarsförhållanden vid t.ex. förskrivning, rekommendationer att använda appar, exempelvis för s.k. ”självmonitorering” inom vården?
- Finns några begränsningar, t.ex. tekniskt och juridiskt, för styrelser och nämnders möjlighet att använda appar inom verksamheten?
- Genomförs ändamålsenliga riskanalyser i samband med anskaffning/förskrivning etc. av appar eller en utrustning etc. till vilken en app kan kopplas?
- Har styrelse och nämnder säkerställt att patientuppgifter och andra förekommande personuppgifter hanteras på ett ändamålsenligt och tillräckligt sätt vid användning av appar?
    - Finns t.ex. i regionen någon organisation eller beredskap för att testa/godkänna appar som t.ex. kommer att användas i verksamheten? (t.ex. ur patientsäkerhetsperspektiv, risken för obehöriga att få del av information etc.?
- Finns det en tydlig koppling mellan överväganden rörande säkerhet för användning av appar och det regionövergripande säkerhetsarbetet?

[3] Indirekt användning avser t ex appar som en patient själv kan ladda ner

- Finns ett systematiskt arbete för att säkerställa en tillräcklig intern kontroll avseende behörigheter till den data som appar tillgängliggör?
- Genomförs analyser på verksamhetsnivå avseende vilka applikationer som skulle kunna gynna verksamheternas arbetssätt mot att nå sina verksamhetsmål?

2.3 Revisionskriterier

Med revisionskriterier avses de bedömningsgrunder som används i granskningen för analyser, slutsatser och bedömningar. Revisionskriterierna för denna granskning utgörs av:

- Kommunallagen
- Hälso- och sjukvårdslagen
- Patientlagen
- Dataskyddsförordningen (GDPR)
- Lagen om offentlig upphandling (LOU)
- Patientdatalagen
- Patientsäkerhetslagen
- Budget och regionplan 2021–2023
- Övriga centrala direktiv och styrning inom området
- EYs erfarenheter och kunskap kring införande av e-hälsolösningar

En översiktlig redogörelse för relevant lagstiftning ses i bilaga 1.

2.4 Metod och avgränsning

Granskningen har genomförts genom en dokumentstudie, intervjuer samt processgenomgång av aktuella appar. Samtliga intervjuade har getts möjlighet att faktakontrollera ett rapportutkast, för att säkerställa att uttalanden bygger på korrekta fakta och iakttagelser. Slutsatser och revisionsbedömningar svarar EY för.

3. Nationella utmaningar i arbetet med digitalisering och användning av molntjänster

Kommuner och regioner samt statliga myndigheter har under lång tid haft som mål att digitalisera, genom de olika satsningar, investeringar och mål som styr offentlig sektor.

Sveriges kommuner och regioner (SKR) beskriver att digitaliseringen inom kommuner och regioner har två grundläggande syften; att effektivisera tjänsteleveransen till invånaren både ur ett kostnadsperspektiv och ur perspektivet att förenkla invånarens dialog med parterna i offentlig sektor. Båda dessa syften kräver goda förutsättningar för innovation kopplat till informationshantering, dvs att organisationer radikalt ändrar hur de bearbetar och lagrar information. För många innebär det att flytta arbetssätten till publika eller privata molntjänster då det ger en större möjlighet att genomföra transformationen och samtidigt följa principen om det mest kostnadseffektiva alternativet. När nu grundlägganderättsliga förutsättningar för denna övergång ifrågasätts under pågående transformation uppstår en osäkerhet som medför en uppbromsning enligt SKR.

Trots rättslig osäkerhet när det gäller förutsättningar för användning av molntjänster, finns fortfarande ett stort behov av användning och alternativet att ”backa” eller ”ta hem” till egen drift är ofta inte möjligt att genomföra. Redan genomförda omställningar för att skapa förmåga att digitalisera verksamheten och gjorda investeringar för att möta de nationella målen om digitalisering medför att det saknas förmåga att hantera drift i egen regi, som det gjordes förr. En återgång till mer traditionell IT-drift medför konsekvenser i form av kostnader som måste vara mycket väl motiverade för att kunna vara i linje med god ekonomisk hushållning.

Kommuner och regioner använder i stor utsträckning olika typer av molntjänster. Nyttjandet varierar från användning av dedikerade lösningar för viss del av verksamheten till strategiska vägval för infrastruktur och centrala administrativa stödresurser.

SKR beskriver vidare att molntjänster, med rätt kravställning och införande, kan ge en högre nivå av IT-säkerhet än vad IT-drift i egenregi kan åstadkomma. Mot detta behöver ställas risker för informationshanteringen som uppstår av globala molntjänsteleverantörer med flera länders rättssystem att ta hänsyn till, komplexa affärsmodeller och omfattande avtalskonstruktioner.

När det gäller användning av publika molntjänster med standardiserade avtalsvillkor blir det däremot en annan process eftersom man istället måste granska tjänsten, vilka säkerhetsmekanismer som finns och analysera ifall tjänstens utformning och villkor lämpar sig för de behov verksamheten har och de krav på säkerhet som informationen kräver.[4]

[4] Molntjänster i verksamheter, SKR 2019

4. Styrning och begränsningar rörande användning av applikationer inom Region Dalarna

Enligt uppgift finns det totalt ca 830 applikationer och system inom regionen. Av dessa är ca 220 molntjänster (s.k. webbapplikationer) där flertalet även har mobilapplikationer. Inom regionen finns 50 beslutade molntjänster, varav 18 har en mobilapplikation.[5] Av de 50 system som är beslutade har 12 procent ej blivit godkända och 26 procent kan inte nyttjas på tänkt sätt då hinder föreligger, primärt kopplat till lagstiftning i form av dataskyddsförordningen (GDPR) och patientdatalagen (PDL). Vanligen kan då antingen systemen inte användas, alternativt används de med restriktioner, komplettering med manuella rutiner eller liknande.

Enligt intervjuade använder regionens verksamheter i begränsad utsträckning appar som samlar in data om patienter eller invånare. Det saknas dock en ändamålsenlig kontroll avseende samtliga applikationer som används i nuläget.

4.1 Styrande dokument och riktlinjer

4.1.1 Regionplan och digitaliseringsstrategi

Den övergripande styrningen avseende digitalisering inom regionen utgår från regionplan och budget 2021–2023 samt den regionala digitaliseringsstrategin 2021–2025. I regionplan och budget är ett av målområdena digitalisering, där det anges att det ska vara lätt av att vara digital såväl inom Region Dalarna som i länet.

I regionplan, budget och finansplan 2021–2023 anges att digitaliseringen av hälso- och sjukvården ska påskyndas genom utbyggnad av vårdappen Min vård. Alla verksamheter ska även erbjuda digital tidsbokning. Vidare har hälso- och sjukvårdsnämnden pågående uppdrag från regionplan 2019 och 2020 som bland annat innefattar att utveckla den digitala vårdcentralen Min vård med fler funktioner och tjänster, de ska möjliggöra bokning och ombokning via webben samt ha en fortsatt utveckling av e-hälsa, tidsbokning på nätet, distansbesök genom digitala hälsorum och videosamtal. Kollektivtrafiknämnden ska utveckla digitaliseringen av kallelser och bussbiljetter genom att möjliggöra QR-kodläsning samt möjligheten att boka färdtjänstresor digitalt.

Syftet med digitaliseringsstrategin är att den ska vara vägledande och stödjande för samtliga verksamhetsområden. Strategin har fem övergripande målområden:

1. Ökad invånarmedverkan och digital service
2. Ökad digital kompetens och smartare arbetssätt
3. Tydligare styrning, ledning och organisation
4. Ändamålsenlig digital infrastruktur och informationsförsörjning
5. Gemensamt ramverk för arkitektur och IT-/informationssäkerhet

I strategin anges att en fördjupning och konkretisering av digitala utvecklingsinsatser och uppdrag för regionen ska tas fram i samverkan med verksamheterna i en gemensam handlingsplan. Vidare definieras vad digitalisering innebär för regionens olika verksamhetsområden. Respektive verksamhet är sedan ytterst ansvarig för att konkretisera och omsätta strategi och handlingsplan i genomförandeprojekt och aktiviteter samt förankra detta i respektive nämnd. Uppföljning ska ske i enlighet med fastlagda principer i ordinarie uppföljningsprocess.

4.1.2 Informationssäkerhets- och dataskyddspolicy

Regionens informationssäkerhetspolicy är fastställd av fullmäktige och reviderad senast 2021. Målet med policyn är att ange den politiska ledningens inriktning och uppdrag för informationssäkerhetsarbetet.

Regionens informationssäkerhetsarbete ska skydda informationen inom verksamheten och vara anpassat till skyddsvärde, risk och lagkrav samt aktuell hotbild. Informationssäkerhets- och dataskyddsarbetet ska främja verksamheternas funktionalitet, kvalitet och effektivitet, invånarnas rättigheter och personliga integritet. Arbetet ska även säkerställa lagefterlevnad, stärka regionens förmåga att förebygga och hantera allvarliga störningar och kriser samt stärka förtroendet för regionens informations- och personuppgiftshantering. Policyn

[5] Beslutade molntjänster är kopplat till ett verkställighetsbeslut som infördes i november 2019 av regiondirektören. Molntjänster som implementerades innan november 2019 krävde inte applikationsrådets godkännande.

tydliggör ansvarsnivåer för informationssäkerhet och dataskydd samt hur dokumentet ska revideras. Former för uppföljning av policyns efterlevnad framgår ej.

Regionstyrelsen ansvarar dels för att informationssäkerhetspolicy samt riktlinjer utarbetas och uppdateras, dels för att samordna regionens informationssäkerhetsarbete.

Regionstyrelsen samt varje nämnd ansvarar sedan för informationssäkerheten inom respektive verksamhetsområde samt att planlägga och löpande följa upp informationssäkerheten och i övrigt vidta nödvändiga åtgärder för att upprätthålla tillräcklig intern kontroll. Området regleras ytterligare i ”*Riktlinjer för informationssäkerhet*”.

Ansvaret regleras dessutom i riktlinjer för informationssäkerhet och dataskydd. Dessa är under framtagande när granskningen genomförs.

4.1.3 Riktlinje för användning av molntjänster

Mot bakgrund av den tekniska utvecklingen och införandet av den amerikanska lagstiftningen Cloud Act[6] har regionen en riktlinje för upphandling och användning av molntjänster från 2019[7]. Cloud Act kan vara i strid med bestämmelserna i GDPR när datan berör personuppgifter och SKR betonar att svenska kommuner och regioner behöver beakta risken för informationsutlämning i sin bedömning inför användning av en molntjänst. Vid tidpunkten för granskningen är 59 % av regionens beslutade molntjänster kopplade till amerikanska aktörer, vilket är en väsentlig andel.

Riktlinjen innefattar bland annat att beslut om att nyttja molntjänster ska förankras i regionens applikationsråd[8] samt att behandling av sekretesskyddades uppgifter i molntjänster som omfattas av Cloud Act endast får ske efter särskilt godkännande.

Av riktlinjen framgår att en risk- och sårbarhetsanalys samt informationsklassning ska göras (kallad ISAK) avseende molntjänster.[9] Analyserna ska säkerställa att informationshanteringen inte strider mot lagar och förordningar samt ge en kravbild på införskaffande och användning av molntjänsten. Följande krav ska uppfyllas:

- Lagringens geografiska plats ska vara förenlig med gällande dataskyddslagstiftning
- IT-säkerhetskrav från informationsklassningen ska uppfyllas
- Informationens skyddsnivå ska vara lägre än ”Hemlig”
- Riskerna från riskanalysen ska vara accepterade av ansvarig
- Tillgänglighetskraven ska vara uppfyllda
- Datamigreringen ska vara möjlig vid avveckling
- Ett dokumenterat beslut om att nyttja molntjänsten ska finnas. Innan beslutet fastställs ska det beredas i applikationsrådet.

Trots att leverantören ansvarar för uppdatering och konfiguration så ska en förvaltning finnas och säkerställa tjänstens funktionalitet och en ändamålsenlig användning. Riktlinjen specificerar kontrollpunkter som ska finnas enligt regionens förvaltningsmodell.[10]

Enligt uppgift är riktlinjen i behov av revidering, då den inte fullt ut speglar hur regionen praktiskt arbetar med frågorna. Det framgår inte heller hur beslutsgång och mandat ser ut för applikationsrådet i förhållande till övrig styrning.

---

[6] Cloud Act (Clarifying Lawful Overseas Use of Data Act) är en amerikansk lag som möjliggör för amerikanska myndigheter att begära ut data som lagras utanför det amerikanska territoriet från tjänsteleverantörer som omfattas av USA:s jurisdiktion. Lagen syftar till att underlätta utredningsarbetet för brottsbekämpande myndigheter.

[7] RD19/05757

[8] Applikationsrådet presenteras närmre i avsnitt 5.1.

[9] Arbetet med riskanalyser presenteras vidare i avsnitt 6.

[10] PUB-avtal, Service och underhållsavtal, Budget och resurser för förvaltning finns, Löpande granskning av leverantören och underleverantörens informationssäkerhetsarbete, Löpande granskning av att tjänsten används på ett avsett sätt, Incidenthantering, Kontinuerlig risk- och sårbarhetsanalyser genomförs, Kvalitetssäkrad behörighetshantering.

4.2 Begränsningar för hur molntjänster får användas

Regionens användning av molntjänster påverkas av flertalet lagar och förordningar som begränsar och styr användandet av digital offentlig service.[11] Myndigheten för digital förvaltning (DIGG) har identifierat 12 områden där det finns behov av rättsligt stöd hos den offentliga förvaltningen i digitaliseringsfrågor. Av granskningen framkommer att Region Dalarna upplever liknande problematik som omnämns i dessa områden, i olika omfattning beroende på verksamhet. Flera utav dessa har direkt bäring på molntjänster med tillhörande applikationer, medan andra redogör för mer övergripande utmaningar avseende digitalisering och IT. Nedan fokuserar vi på det som har direkt bäring på molntjänster med tillhörande applikationer. Den fullständiga listan ses i bilaga 2.

Tabell 1. Översikt över nationella riskområden knutet till digitalisering inom offentlig sektor

Digital kommunikation med enskilda	Digital kommunikation med enskilda härleds till behov av rättsligt stöd avseende tekniska lösningar såsom infrastruktur för digital post. Inom hälso- och sjukvården behöver det exempelvis finnas säkra digitala kommunikationsvägar för uppgifter som omfattas av sekretess eller känsliga personuppgifter. Det berör dels vårdfrågor för enskilda och myndighetsöverskridande dialog mellan region och socialtjänst, dels frågor som omfattas av anbudssekretess i upphandling.
Informationsutbyte	Informationsutbyte upplevs ofta hämmas av lagstiftning, särskilt utifrån dataskyddsregleringen i särskilda registerförfattningar samt sekretesslagstiftningen. DIGG hänvisar till kommunutredningen som konstaterade att Sverige saknar vissa förvaltningsgemensamma lösningar för informationsutbyte som finns i jämförbara länder. En utmaning är övergången från traditionell pappershantering till digital hantering samt hur och när en enskild själv kan och bör kunna föra över sin information mellan aktörer och processer.
Upphandling, utkontraktering och IT-avtal	Offentliga aktörer upplever sig inte ha tillräcklig kompetens och förmåga att genomföra upphandlingar avseende IT som svarar för samtliga upphandlingskrav samt rättsliga krav för myndigheter. Det finns behov av samordning av vilka krav på standarder som ska ställas när system upphandlas eller utvecklas. Utkontraktering upplevs problematiskt dels i fråga om att få den tjänst som motsvarar behovet, dels gällande avtalshanteringen och sekretesslagstiftning.
Informationssäkerhet	Informationssäkerheten är aktuell i olika delar av digitaliseringen.
Innovation och användning av nya tekniker	Innovationen och implementeringen av nya tekniker saktas ned till följd av den osäkerhet som finns kring de rättsliga förutsättningarna.
Molntjänstfrågan och andra frågor om dataskydd	Molntjänstfrågan kopplas till att uppgifter inte får överföras till tredje land, lagring av uppgifter, informationsöverföring med anledning av Schrems II-domen[12], hantering av känsliga personuppgifter och uppgifter som omfattas av sekretess i IT-tjänster och system samt informationsutbyte kring informationssäkerhetsrelaterade frågeställningar. De juridiska frågeställningarna berör vanligen praktiska frågor om vilka tjänster eller system som kan, ska och får upphandlas och användas, avtalshantering, avtalsuppföljning i samband med nödvändig verksamhetsutveckling.

Regionen har inget internt styrdokument beträffande begränsningar och ansvarsförhållanden vid förskrivning eller rekommendationer att använda applikationer inom hälso- och sjukvården men följer Socialstyrelsens stöd ”*Förskrivning av hjälpmedel – Stöd vid förskrivning av hjälpmedel till personer med funktionsnedsättning*”.

Vi noterar att Socialstyrelsens stöd endast omfattar hjälpmedelsverksamheten, dvs. en begränsad del av regionens applikationsanvändning.

Rörande begräsningar internt inom regionen pågår ett arbete med att införa en så kallad EMM-plattform (Enterprise Mobility Management), som samtliga anställdas arbetsmobiler ska anslutas till. Denna plattform fungerar som kontroll och spärr mot otillåten användning av applikationer. Exempelvis ska en vårdmobil inom en avdelning vara relativt låst avseende användningsområden, medan chefers mobiler kommer att ha större tillgång till olika program.

[11] Se ett urval av dessa i bilaga 1.

[12] Den så kallade **Schrems II-domen** gjorde det olagligt att föra över personuppgifter till USA om organisationen inte kan stödja det på någon annan grund i GDPR.

5. Ansvar och rollfördelning avseende applikationer är inte helt tydliggjort

Användningen av molntjänster med tillhörande applikationer berör både ordinarie linjestyrning, portföljstyrning inom IT-verksamheten samt behandling inom regionens applikationsråd. Det finns risker att beakta ur många perspektiv, vilket ställer krav på tydliga roller och ansvar, gränssnitt mellan verksamheter och möjligheter till samverkan.

Nedan redogör vi översiktligt för hur ansvaret definieras i dokumentation och utifrån intervjuer. Beskrivningen utgör ingen fullständig redogörelse av samtliga nivåer eller funktioner som berörs av frågor om applikationer.

5.1 Applikationsrådet

Applikationsrådet har funnits i ca 6 år och dess syfte är att handlägga och besluta i frågor där applikationer har avvikelser kopplat till:

- Avvikelser från gällande lagkrav, exempelvis GDPR, PDL och Lag om Medicintekniska Produkter
- Inkompatibilitet/avvikelse från nuvarande IT-plattform, säkerhetsstandard, teknisk standard etc.

Rådet hanterar alla molntjänster sedan november 2019. Beslut i rådet tas formellt av IT-direktör som är ordförande. Rådet kan besluta om att avslå användning eller upphandling av system eller lösningar som inte följer regionens riktlinjer och verkställighetsbeslut. Rådet kan också besluta om tillfälligt godkännande eller hänskjuta ärenden för politiskt beslut eller till regiondirektör.

Enligt intervjuer kan rådet också besluta om renovering och avveckling av applikationer, peka ut ägare om så krävs samt besluta om handlingsplaner för applikationer som av olika skäl kräver åtgärd. Särskilda skäl kan exempelvis vara höga kostnader, säkerhetsbrister, upphandlingsskäl eller juridiska skäl. I rådet finns en föredragande funktion vars ansvar är att samordna inkommande ärenden, följa upp pågående ärenden samt avvikelser i en årlig genomgång. Föredragaren ska även agera som kontaktyta in till applikationsrådet.

Rådet träffas 5 – 6 gånger årligen och består av funktioner inom juridik, dataskydd, informationssäkerhet, medicinsk teknik och IT samt verksamhetsföreträdare.

Intervjuade beskriver att applikationsrådet ligger vid sidan av organisatoriska regionens övriga struktur för portföljstyrning och linjeorganisationen, vilket gör att dess roll och mandat blir otydligt. Vilka ärenden som ska vara föremål för beslut av regiondirektör respektive regionstyrelse är inte tydliggjort i dokumentationen. Det är inte heller tydliggjort vilka följder det får om verksamheter brister i att lyfta ärenden för beslut i applikationsrådet.

Utifrån de ärenden som behandlas i applikationsrådet finns en sammanställning över de molntjänster och applikationer som är godkända att använda, ej godkända eller där annan åtgärd vidtagits. Denna är enligt uppgift inte en komplett lista för vilka molntjänster som används. Vi noterar att det finns flera appar inom exempelvis hälso- och sjukvården samt hjälpmedelsverksamheten som behandlats av rådet. Applikationer inom exempelvis kollektivtrafiken saknas i underlaget.

Det saknas en tydlig struktur och dokumentation avseende uppföljning inom applikationsrådet.[13] Vi har inte inom ramen för granskningen kunnat ta del av något underlag som utgör uppföljning av ärenden. Enligt intervjuade är detta en brist i det löpande arbetet, då det saknas en kontroll över om de beslut som tas i rådet faktiskt verkställs inom verksamheterna som tänkt.

5.2 Portföljstyrning

Verksamhetsutveckling med stöd av IT styrs inom regionen genom portföljstyrning. Portföljstyrning används för att optimera och samordna regionens IT-verksamhet genom koncerngemensam styrning och prioritering. Portföljstyrningen utgår från regionens övergripande målstyrning och målnedbrytning. Innehållet i portföljen utgörs av de projekt och uppdrag som beslutas att starta inom portföljen samt de förvaltningsobjekt som ingår och deras årliga planer.

[13] Rådet kommunicerar idag beslut till verksamheten, det förutsätts att verksamheten sedan följer dessa beslut och att implementation sker därefter. Rådet är idag inte bemannat för att hantera uppföljning och löpande kontroll av verksamheten.

Portföljstyrningen omfattar alla förändringsinsatser och samtliga beslut gällande genomförande av verksamhetsutveckling med stöd av IT samt ramarna för aktiviteter som syftar till vidmakthållande av IT-stöd.

IT-verksamheten delas in i olika styrgrupper och förvaltningsobjekt som tillsammans bildar en *förvaltningsobjektsarkitektur*. Arkitekturen ska spegla regionens verksamhet snarare än organisationen.

Portföljstyrgruppen är det högst beslutande organet och lyder direkt under regiondirektören. Styrgruppen består av IT-direktören (ordförande och portföljägare), ordförande från respektive familjestyrgrupp, hälso- och sjukvårdsdirektör, ekonomidirektör, portföljansvarig, föredragande samt representant från portföljkontoret. Beslut i styrgruppen tas formellt av IT-direktör. Styrgruppen har mandat att:

- besluta om förändring I förvaltningsobjektsarkitekturen samt etablering av förvaltningsobjekt,
- fastställa planerings- och budgetförutsättningar för portföljen,
- besluta om, prioritera och omprioritera inom portföljen som helhet
- besluta om investeringar för kommande år
- besluta om ekonomiska ramar för förvaltningsobjekt och projekt eller uppdrag
- besluta om utökning eller indragning av resurser
- besluta om initiering av projekt, uppdrag eller förstudier
- besluta om stopp av pågående förvaltning eller utveckling
- besluta om bemanning av rollen som objektägare.

Hur denna styrstruktur förhåller sig till linjeorganisation samt applikationsrådets roll är inte tydliggjort i granskad dokumentation.

Av intervjuerna framgår att det löpande finns många beröringspunkter mellan linjeorganisation, portföljstyrningsmodellen samt applikationsrådet, men det är inte alltid tydliggjort i vilken process en fråga ska hanteras eller på vilken nivå beslut ska fattas rörande frågor om applikationer.

5.3 Ansvaret i linjeorganisationen

Flera riskaspekter som anknyter till användningen av applikationer ska hanteras löpande inom ramen för linjeorganisationen.[14] Det är enligt uppgift inte tydliggjort i verkställighetsbeslut eller rollbeskrivningar hur respektive chef ska förhålla sig till exempelvis informationssäkerhet eller de applikationer som används i verksamheten. Det beskrivs dock i flera styrdokument hur ansvar för exempelvis digitalisering, informationssäkerhet och intern kontroll ska följa ansvaret i linjen. Vidare varierar det inom nämndernas olika verksamheter huruvida det finns samordnande resurser knutna till uppdragen.

[14] Med linjeorganisation avses de hierarkiska nivåer av chefer från nämnd till förstalinjechef.

6. Riskanalyser och -bedömningar

Systematiska riskbedömningar avseende applikationer görs främst ur ett informationssäkerhetsperspektiv, genom så kallade ISAK-analyser. Dessa ska genomföras gemensamt med de verksamheter som använder applikationen för att kartlägga risker och åtgärder på ett så effektivt sätt som möjligt. De ska genomföras för alla applikationer/ system innan de implementeras inom Region Dalarna. ISAK-analys skall finnas dokumenterad för de ärenden som bereds inför behandling i applikationsrådet. Tillsammans med administrativa och tekniska skyddsåtgärder ska det säkerställas att information finns tillgänglig vid behov, är korrekt samt att obehöriga inte kan få tillgång till informationen.

I regionen finns internt anpassade säkerhetsnivåer som även gäller externa parter som hanterar regionens information. Syftet är att säkerställa:

- Konfidentialitet (rätt person) – information får endast vara tillgänglig för behöriga användare.
- Riktighet (rätt information) – informationen får inte förändras eller gå förlorad; av misstag, genom inverkan av obehörig eller på grund av tekniskt fel.
- Tillgänglighet (rätt tid och plats – informationen ka kunna användas i förväntad utsträckning, inom önskad tid samt plats.
- Spårbarhet (vem och vad) – händelser i informationsbehandlingen ska kunna spåras genom loggning.

Regionen har en framtagen mall och checklista för genomförande av egenkontroll avseende informationssäkerhet. I checklistan kontrolleras bland annat om en ISAK-analys är genomförd, om säkerhetsåtgärder är genomförda utifrån ISAK-analysen samt om det finns tillräckliga kompetenser och resurser för att upprätthålla informationssäkerhet. Checklistan ska används vid uppstarten av alla nya förvaltningsobjekt.

Vi har tagit del av underlag rörande ett urval av applikationer, för att följa ärendeprocessen. Nedan redovisas två exempel. Vi noterar att det i beredningsprocessen i applikationsrådet finns tydliga former för riskanalyser, ärendeberedning och behandling. Däremot saknas former för uppföljning av ärendet efter fattat beslut.

Typ av tjänst	ISAK genomförd	Beslutsunderlag mottaget	Behandlas i applikationsrådet	Former för uppföljning av verkställighet
Applikation avseende justering av hörapparater	Ja	Ja	Ja	Nej
Molnbaserat analysprogram för behandling av diabetes	Nej – pågående ärende	Ja	Ja	Nej

Under 2019 genomfördes ett test av så kallad Shadow IT[15], genom en lösning som bevakar och analyserar trafik till molntjänster och ger möjlighet att se om riktlinjer för informationssäkerhet följs, samt minskar risken för informationsförlust eller infektion med skadlig kod. Förutom att analysera vilka molntjänster som används så klassades då tjänsterna (av ett externt team) in i olika riskområden utifrån användningsvillkor, GDPR m.m. Av resultatet framgick att den totala användningstillfällen av olika molntjänster under prövoperioden var över 2000 st och av dessa så var 100st klassade som högrisk.

Härutöver genomförs inga löpande riskbedömningar avseende applikationer. Ur verksamhetsperspektiv varierar det vilka analyser som genomförs.

[15] Shadow IT innefattar alla applikationer, programvaror och verktyg som används i arbetet och som inte har godkänts av eller beställs genom organisationens IT-avdelning. Med största säkerhet har IT-avdelningen varken utvecklat verktygen, är medvetna om att de existerar inom organisationen eller kan supportera dem. Detta är ett problem eftersom det sannolikt ökar flödet av inofficiell data vilket gör det svårt att följa krav kopplade till exempelvis GDPR and andra viktiga förordningar och föreskrifter.

7. Uppföljning och återrapportering

7.1 Intern systematisk uppföljning saknas i flera fall

Det finns inga tydliga systematiska former för att följa upp användningen av specifikt molntjänster med tillhörande applikationer inom applikationsrådet eller IT-verksamheten. Vi har inte kunnat ta del av någon samlad uppföljningsdokumentation avseende användning, riskhantering, strategiska avväganden eller liknande. Därmed inte sagt att applikationer inte berörs i uppföljning av exempelvis IT-frågor och frågor rörande informationssäkerhet.

Den sammanställning som finns rörande de molntjänster som behandlats i applikationsrådet ger en viss uppföljning, men enligt intervjuade är denna inte representativ för alla molntjänster som används. Denna kontroll finns i nuläget inte i organisationen.

På nämnd- och verksamhetsnivå har vi noterat att det kan förekomma exempel på beskrivning av användning av molntjänster med tillhörande applikationer, men ingen systematisk kontroll eller uppföljning avseende den totala förekomsten av dessa applikationer eller användningen inom verksamheterna.

7.2 Återrapportering till nämnd och styrelse

När granskningen genomförs är inte årsrapporten för 2021 färdigställd. I årsrapporten 2020 sker en viss uppföljning av applikationsanvändningen. Regionens applikation Min Vård konstateras ha en kraftig ökning av användandet under 2020. Ökningen härleds till att läkare och andra ställde om till digitala arbetssätt under pandemin samtidigt som marknadsföringsåtgärder genomfördes i syfte att främja besök i appen. Min Vård användes för bokning av provtagning för PCR (pågående Covid19-infektion) och totalt lades 58 170 provtagningstider ut i appen. Några vårdcentraler använde även appen för bokning av influensavaccinering. I appen finns det också tillgång till psykologer samt återstart med fysioterapeuter. Användningen av Vårdguidens e-tjänst 1177 konstateras också ha ökat. Under 2020 ökade antal konton hos invånarna från cirka 60 procent till 73 procent.

Vidare anges förväntad utveckling i årsrapporten 2020 genom att arbetet med framtidens vårdinformationssystem, FVIS, är ett samarbete inom SUSSA samverkan. SUSSA står för strategisk utveckling av sjukvårdsstödjande applikationer och är en samverkansgrupp för nio regioner. Den övergripande idén med SUSSA är att samverka för att uppnå målen i nationell vision för e-hälsa 2025. Samverkan skapar förutsättningar för effektivare arbetssätt i vården och bidrar till att regionerna kan erbjuda en god och jämlik vård. Region Dalarna tecknade avtal med leverantören i juni 2020 och ska under 2021 arbeta med förberedelser för implementation. Bytet till det nya vårdinformationsstödet planeras ske 2023–2024.

I övrigt har vi inte noterat någon systematisk återrapportering rörande molntjänster med tillhörande applikationer.

8. Svar på revisionsfrågorna

Revisionsfrågor	Svar
I vilken utsträckning används appar i regionens verksamheter?	Det finns en sammanställning rörande applikationer som används i regionen, men det finns en risk att denna inte är komplett. I det underlag vi tagit del av rör det sig om ca 220 molntjänster med tillhörande applikationer.
Finns någon ändamålsenlig uppföljning/kontroll (centralt eller på nämndnivå) över vilka appar som används, såväl direkt som indirekt, i organisationen?	Nej inte fullt ut. Utifrån applikationsrådet och den struktur för riskbedömning och godkännande som finns, bedömer vi att det finns en kontroll och en uppföljning. Av granskningen framkommer dock att denna struktur inte fångar hela regionens användning av appar, utan att det varierar mellan verksamheter i vilken utsträckning den fastlagda processen används. Kontroll och uppföljning bedöms därför inte vara tillräcklig, vilket vi bedömer medföra risker i informationssäkerhet och kvalitet
Har regionen utarbetat, eller planeras, några övergripande styrdokument (ramverk, rekommendationer etc) för användning av appar i regionens verksamhet? Har regionen klargjort olika ansvarsförhållanden vid t.ex. förskrivning, rekommendationer att använda appar, exempelvis för s.k. ”självmonitorering” inom vården?	Delvis. Det finns en riktlinje avseende molntjänster, som enligt intervjuade behöver revideras eftersom den inte fullt ut speglar hur organisationen arbetar. Vidare berörs frågor avseende applikationer i informations- och dataskyddspolicy. Övergripande direktiv finns även i regionplan och digitaliseringsstrategi. Nej, inte utöver att de använder Socialstyrelsens föreskrifter rörande förskrivning av hjälpmedel.
Finns några begränsningar, t.ex. tekniskt och juridiskt, för styrelser och nämnders möjlighet att använda appar inom verksamheten?	Ja, det finns flera utifrån både gällande lagstiftning och tekniska förutsättningar.
Genomförs ändamålsenliga riskanalyser i samband med anskaffning/förskrivning etc. av appar eller en utrustning etc. till vilken en app kan kopplas?	Delvis. I den utsträckning som ett ärende rörande en app bereds och behandlas av applikationsrådet bedömer vi att det finns en tillräcklig struktur för att genomföra riskanalyser. Då denna struktur inte täcker samtliga appar som används av verksamheterna blir bedömningen delvis.
Har styrelser och nämnder säkerställt att patientuppgifter och andra förekommande personuppgifter hanteras på ett ändamålsenligt och tillräckligt sätt vid användning av appar? Finns t.ex. i regionen någon organisation eller beredskap för att testa/godkänna appar som t.ex. kommer att användas i verksamheten? (t.ex. ur patientsäkerhetsperspektiv, risken för obehöriga att få del av information etc.?	Nej, utifrån att det saknas en tillräcklig kontroll och uppföljning bedömer vi inte att en ändamålsenlig användning säkerställts. Ja, genom applikationsrådet finns en struktur för beredning och beslut i frågor rörande användning av applikationer. Då rådets mandat och roll i förhållande till övrig styrning inte är tydliggjord och då många ärenden idag inte når behandling i rådet, bedömer vi att det endast delvis fyller det tänkta syftet.
Finns det en tydlig koppling mellan överväganden rörande säkerhet för användning av appar och det regionövergripande säkerhetsarbetet?	Ja, främst utifrån ett informationssäkerhetsperspektiv.
Finns ett systematiskt arbete för att säkerställa en tillräcklig intern kontroll avseende behörigheter till den data som appar tillgängliggör?	Nej. Det pågår arbete inom flera verksamheter för att stärka den interna kontrollen utifrån bland annat informationssäkerhetsperspektiv, men det saknas ändamålsenliga former för kontroll och uppföljning.
Genomförs analyser på verksamhetsnivå avseende vilka applikationer som skulle kunna gynna deras arbetssätt mot att nå sina verksamhetsmål?	Det varierar mellan verksamheter vilka analyser som genomförs. Vidare varierar det hur användande verksamheter deltar i genomförande av riskanalyser.

Anja Zetterberg
Certifierad kommunal revisor
EY

Lina Hedlund
Verksamhetsrevisor
EY

Källförteckning

Dokumentation

- Årsredovisning 2020
- Regionplan och budget 2021
- Regionplan och budget 2022
- Beslutsunderlag hantering Shadow IT
- Shadow IT findings
- Riktlinjer för informationssäkerhet – del A: informationssäkerhet och dataskydd för användare
- Digitalisteringsstrategi
- Dokumentation diabetessjukvård
- Dokumentation hörapparater
- Informationssäkerhets- och dataskyddspolicy
- Informationssäkerhetsplan 2022-2024
- IT-säkerhetsarkitektur i Region Dalarna
- Ledningssystem för informationssäkerhet
- Kartläggning av appanvändningen i Region Dalarna
- Utredning och e-hälsas uppdrag
- DIGG – delrapport rättsligt stöd till offentlig förvaltning avseende digitalisering
- Egenkontroll förvaltningsobjekt gällande informationssäkerhet
- Beslutade molntjänster 2019-2021
- Applikationsråd – ansvar och befogenheter
- Molntjänster i verksamheten, SKR 2019
- Riktlinjer för portföljstyrning
- Riktlinje molntjänster 2019
- Socialstyrelsen – förskrivning av hjälpmedel
- Vägledning SKR gällande personuppgiftsansvar och egenvård
- Verkställighetsbeslut molntjänster 2019
- Urval av verksamhetsplaner, riskanalyser och internkontrollplaner

9. Bilaga 1 – summering av relevant lagstiftning

Dataskyddsförordningen (GDPR)

GDPR grundas i mänskliga rättigheter och att alla människor har rätt till respekt för privat- och familjeliv samt till skydd av sina personuppgifter. GDPR reglerar hur personuppgifter får behandlas. Med personuppgifter menas varje upplysning som rör en identifierad eller identifierbar fysisk person. Genom GDPR ställs krav på bland annat incidentrapporteringsrutiner, genomförande av konsekvensbedömningar, dataskyddspolicy (sekretesspolicy/integritetspolicy), gallring och behandling av personuppgifter, personuppgiftsbiträdesavtal och förteckning. Brott mot GDPR kan innebära höga sanktionsbelopp.

Hälso- och sjukvårdslagen (2017:30)

Hälso- och sjukvård ska bedrivas på ett sådant sätt att den uppfyller kraven på en god vård. Detta innebär bland annat att den ska vara av god kvalitet, lättillgänglig samt tillgodose patientens behov av kontinuitet och säkerhet i vården. Ledningen av hälso- och sjukvården ska vara organiserad så att de tillgodoser hög patientsäkerhet. Inom hälso- och sjukvården ska det finnas någon som svarar för verksamheten (verksamhetschef). Verksamhetschefen ska säkerställa att patientens behov av trygghet, kontinuitet, samordning och säkerhet i vården tillgodoses.

Målet för hälso- och sjukvården är en god hälsa och en vård på lika villkor för hela befolkningen. Vården ska ges med respekt för alla människors lika värde och för den enskilda människans värdighet. Den som har det största behovet av hälso- och sjukvård ska ges företräde till vården. Vården och behandlingen ska så långt det är möjligt utformas och genomföras i samråd med patienten. Olika insatser för patienten ska samordnas på ett ändamålsenligt sätt. Varje patient ska, om det inte är uppenbart obehövligt, snarast ges en medicinsk bedömning av sitt hälsotillstånd.

Patientlag (2014: 821)

Patientlagen syftar till att inom hälso- och sjukvårdsverksamhet stärka och tydliggöra patientens ställning samt främja patientens integritet, självbestämmande och delaktighet. Hälso- och sjukvård ska så långt som möjligt utformas och genomföras i samråd med patienten och får inte ges utan patientens samtycke, om inte annat följer av denna eller någon annan lag. Innan samtycke inhämtas ska patienten få information om bl.a. sitt hälsotillstånd, de metoder som finns för undersökning, vård och behandling, det förväntade vård- och behandlingsförloppet samt väsentliga risker för komplikationer och biverkningar.

Lagen om offentlig upphandling (LOU)

Lagen (2007:1091) om offentlig upphandling, LOU, innehåller allmänna bestämmelser om offentlig upphandling av bland annat varor och tjänster, undantag från lagen samt tröskelvärden. Lagen tillämpas när regioner och kommuner upphandlar t.ex. IT-system, applikationer eller hjälpmedel som ska förskrivas eller användas i verksamheten.

Patientdatalagen (2008:355)

Patientdatalagen tillämpas vid vårdgivares behandling av personuppgifter inom hälso- och sjukvården och syftar till att informationshanteringen ska vara organiserad så att den tillgodoser patientsäkerhet och god kvalitet samt främja kostnadseffektivitet. Personuppgifter ska utformas och behandlas så att patienter och övriga registrerades integritet respekteras samtidigt ska de hanteras och förvaras otillgängligt för obehöriga. Patientdatalagen kompletterar delvis GDPR.

En vårdgivare ska se till att åtkomst till patientuppgifter som förs helt eller delvis automatiserat dokumenteras och kan kontrolleras. Vårdgivare ska göra systematiska och återkommande kontroller av om någon obehörigen kommer åt sådana uppgifter.

Lagen om medicintekniska produkter (1993:584)

Lagen om medicintekniska produkter innehåller bland annat en definition av en medicinteknisk produkt samt allmänna bestämmelser om hanteringen av dessa produkter. I lagen anges också krav på att en medicinteknisk produkt ska vara lämplig för sin användning.

En medicinteknisk produkt får släppas ut på marknaden eller tas i bruk i Sverige endast om den uppfyller de krav och villkor som ställs. Det är straffbelagt att släppa ut en medicinteknisk produkt på marknaden eller använda en sådan produkt i Sverige om den inte uppfyller de krav och villkor som gäller.

Läkemedelsverket och Socialstyrelsen har föreskrifter om medicintekniska produkter (LVFS 2003:11 och SOSFS 2008:1).

Patientsäkerhetslag (2010:659)

I patientsäkerhetslagen anges bestämmelser kring vårdgivarens skyldighet att bedriva ett systematiskt patientsäkerhetsarbete. Vårdgivaren ska planera, leda och kontrollera verksamheten på ett sätt som leder till att kravet på god vård upprätthålls. Vårdgivaren ska även vidta de åtgärder som behövs för att förebygga att patienter drabbas av vårdskador. Enligt lagen ska en patientsäkerhetsberättelse årligen upprättas senast den 1 mars.

Hälso- och sjukvård får inte ges utan patientens samtycke om inte annat följer av denna eller någon annan lag. Patienten kan, om inte annat särskilt följer av lag, lämna sitt samtycke skriftligen, muntligen eller genom att på annat sätt visa att han eller hon samtycker till den aktuella åtgärden.

Lagen om tillgänglighet till digital offentlig service (2018:1937)

Sedan 1 januari 2019 gäller lagen om tillgänglighet till digital service och från och med den 23 juni 2021 omfattas alla offentliga mobila applikationer av lagen. Appar ska vara tillgängliga, och det är särskilt viktigt för personer med olika funktionsnedsättningar. För att en app ska vara tillgänglig ska den kunna läsas upp med en skärmläsare, kontraster och färgval ska anpassas, texten ska vara möjlig att förstora och det är viktigt att kunna navigera med hjälp av tangentbordet i appen.[16] Kravet på tillgänglighet innebär att webbinnehållet ska vara tillgängligt och att användaren ska kunna ta del av och föra in information oberoende av enhet och eventuella hjälpmedel. Översiktligt kan lagen sammanfattas i uppdelningen på fyra områden/riktlinjer för tillgänglighet.

- Uppfatta – berör att användaren ska förstå innehållet på webbplatsen, exempelvis genom att kunna skilja på förgrund och bakgrund eller kunna ändra textinnehållet utifrån behov.
- Genomförbar – berör att allting på webbplatsen måste vara användbart, t.ex. tillgänglig funktion från tangentbord.
- Förståelig - berör att informationen måste vara begriplig att förstå.
- Robust – berör att innehållet på webbplatsen ska fungera så att det kan användas av flera olika enheter. Till exempel att användaren kan använda program för att lyssna på innehållet.[17]

Lagen om tillgänglighet till digital offentlig service anger att den offentliga aktören ska tillhandahålla en tillgänglighetsredogörelse på sin digitala plattform, vilket även gäller för mobila applikationer. Tillgänglighetsredogörelse presenterar hur väl en digital service uppfyller de krav som återfinns i lagen om tillgänglighet till digital offentlig service, vilket bland annat innefattar delar och funktioner som inte är tillgängliga, de skäl som ligger till grund för otillgängligheten och eventuella tillgängliga alternativ, möjlighet att lämna synpunkter samt information om och länk till Myndigheten för digital förvaltning.

[16] Nu gäller lagen om tillgänglighet alla offentliga appar | DIGG

[17] Lagen om tillgänglighet till digital service | Vårdgivarguiden (vardgivarguiden.se)

10. Bilaga 2 - Lista över nationella riskområden för offentlig förvaltning avseende digitalisering

Digital kommunikation med enskilda	Digital kommunikation med enskilda härleds till behov av rättsligt stöd avseende tekniska lösningar såsom infrastruktur för digital post. Inom hälso- och sjukvården behöver det exempelvis finnas säkra digitala kommunikationsvägar för uppgifter som omfattas av sekretess eller känsliga personuppgifter. Det berör dels som vårdfrågor för enskilda och myndighetsöverskridande dialog mellan region och socialtjänst, dels frågor som omfattas av anbudssekretess i upphandling.
Digitala identiteter och underskrifter	Digitala identiteter och underskrifter kopplas till möjligheten att använda elektroniska underskrifter från både enskilda och myndigheter. Det finns också behov av formkrav för e-underskrifter.
Informationsförsörjning, datadelning och tillgång till grunddata	Det finns behov av samordning av krav på standarder på nya offentliga IT-system, via utveckling eller upphandling. Myndigheternas oro härleds bland annat till skyddet av den personliga integriteten. Det finns ett identifierat behov av stöd i såväl sakfrågor som generellt.
Informationsutbyte	Informationsutbyte upplevs ofta hämmas av lagstiftning, särskilt utifrån dataskyddsregleringen i särskilda registerförfattningar samt sekretesslagstiftningen. DIGG hänvisar till kommunutredningen som konstaterade att Sverige saknar vissa förvaltningsgemensamma lösningar för informationsutbyte som finns i jämförbara länder. En utmaning är övergången från traditionell pappershantering till digital hantering samt hur och när en enskild själv kan och bör kunna föra över sin information mellan aktörer och processer.
Digitalisering av ärendeprocesser och automatiserat beslutsfattande	Det finns behov av ökad tydlighet beträffande god offentlighetsstruktur vid automatiserade förfarande, säkerställande a offentlighetsprincipen samt rättssäkerhet vid offentliga förvaltningars användande av AI-system med maskininlärda algoritmer. Det finns behov av ökad kunskap kring dokumentationskrav.
Automation av faktiskt handlande	Varken förvaltningslagen (2017:900) eller dataskyddsförordningen ger tillräcklig ledning avseende automation av faktiskt handlande. Det finns luckor gällande den offentligrättsliga statusen för dataprogram, dess beståndsdelar, främst algoritmer, samt rättsliga förutsättningar för fullgod insyn för att följa förvaltningens verksamhet när tekniska lösningar tillhandahålls av utomstående leverantörer.
Upphandling, utkontraktering och IT-avtal	Offentliga aktörer upplever sig inte ha tillräcklig kompetens och förmåga att genomföra upphandlingar avseende IT som svarar för samtliga upphandlingskrav samt rättsliga krav för myndigheter. Det finns behov av samordning av vilka krav på standarder som ska ställas när system upphandlas eller utvecklas. Utkontraktering upplevs problematiskt dels i fråga om att få den tjänst som motsvarar behovet, dels gällande avtalshanteringen och sekretesslagstiftning.
Samverkan	För hantering av de identifierade behoven krävs samverkan. Det bör finnas ett fokus inte enbart på att ett rättsligt stöd ska utformas utan även på hur det ska göras.
Informationssäkerhet	Informationssäkerheten är aktuell i olika delar av digitaliseringen.
Innovation och användning av nya tekniker	Innovationen och implementeringen av nya tekniker saktas ned till följd av den osäkerhet som finns kring de rättsliga förutsättningarna.
Molntjänstfrågan och andra frågor om dataskydd	Molntjänstfrågan kopplas till att uppgifter inte får överföras till tredje land, lagring av uppgifter, informationsöverföring med anledning av Schrems II-domen[18], hantering av känsliga personuppgifter och uppgifter som omfattas av sekretess i IT-tjänster och system samt informationsutbyte kring informationssäkerhetsrelaterade frågeställningar. De juridiska frågeställningarna berör vanligen praktiska frågor om vilka tjänster eller system som kan, ska och får upphandlas och användas, avtalshantering, avtalsuppföljning i samband med nödvändig verksamhetsutveckling.
Övriga rättsfrågor	De övriga frågor som lyfts är bland annat tolkning och förståelse av tillgänglighetskrav på verksamheten.

[18] Den så kallade **Schrems II-domen** gjorde det olagligt att föra över personuppgifter till USA om organisationen inte kan stödja det på någon annan grund i GDPR.