Referansearkitektur for informasjonssikkerhet, digital beredskap og personvern for kommunal sektor (RSB)

Konseptuell beskrivelse
Versjon 1.0
18. august 2020

Overlevert Aksjon prosjektet, 18. august 2020

Innholdsfortegnelse

1. Innledning

Direktoratet for e-helse har fått i oppdrag å gjennomføre et forprosjekt for felles kommunal journal og samhandling mellom aktørene innen helse- og omsorgssektoren. Tiltaket har fått navnet Akson. Tiltaket Akson inneholder to deler. En samhandlingsløsning og en felles kommunal journalløsning. Samhandlingsløsningen skal leveres av Norsk Helsenett SF (NHN), mens felles kommunal journal leveres som tjeneste av Akson Journal AS[1].

Når det refereres til begrepet Akson i dette dokumentet refereres det til felles kommunal journalløsning med tilhørende undersystemer. Når det refereres til Akson journal AS referer det til virksomheten som skal levere journalløsningen som en tjeneste til kommunal sektor.

Tiltaket Akson innebærer økt samling og deling av helseopplysninger og anses som et kritisk system for helsebehandling i kommunal sektor[2]. Informasjonssikkerhet[3] (henter kalt sikkerhet), digital beredskap[4] (heretter kalt beredskap), og personvern har av den grunn høy prioritet for å bidra til god og trygg helsebehandling som oppleves tillitsskapende av den enkelte, og samfunnet generelt.

Det finnes ingen helhetlig tilnærming til referansearkitektur for sikkerhet, beredskap og personvern i kommunal sektor for digitale tjenester. Dette dokumentet er utarbeidet i den hensikt å bistå kommunal sektor med referansearkitektur innen områdene sikkerhet, beredskap og personvern i et digitalt tjenesteperspektiv. Forkortet som RSB.

Formålet med RSB er å sikre at Akson journal AS og kommunal sektor har tilstrekkelig sikkerhet, beredskap, og personvern for å levere og konsumere trygge og sikre digitale tjenester.

RSB versjon 1.0 er en konseptuell beskrivelse, det vil si en introduksjon til hvordan og hva man bør tenke på innen sikkerhet, beredskap og personvern i et digitalt tjenesteperspektiv. RSB versjon 1.0 er rettet mot tiltaket Akson, og har en helhetlig tilnærming til sikkerhet, beredskap og personvern i tjenesteperspektiv. RSB versjon 1.0 kan ses på som et kravsett som kommunal sektor stiller til Akson.

I fremstillingen benyttes også begrepene tjenesteyter om Akson journal AS, og konsument om kommunene. I denne konteksten vil konsumentene (kommuner) gjennom RSB stille krav til tjenesteyter (Akson journal AS) på hva som bør oppfylles av krav for å kunne motta tjenesten. Tjenesteyter (Akson AS) vil sin side bruke RSB for å sikre tilstrekkelig sikkerhets- og beredskapsevne for å være i stand til å levere trygge og sikre digitale tjenester.

Dokumentet er inndelt i følgende struktur:

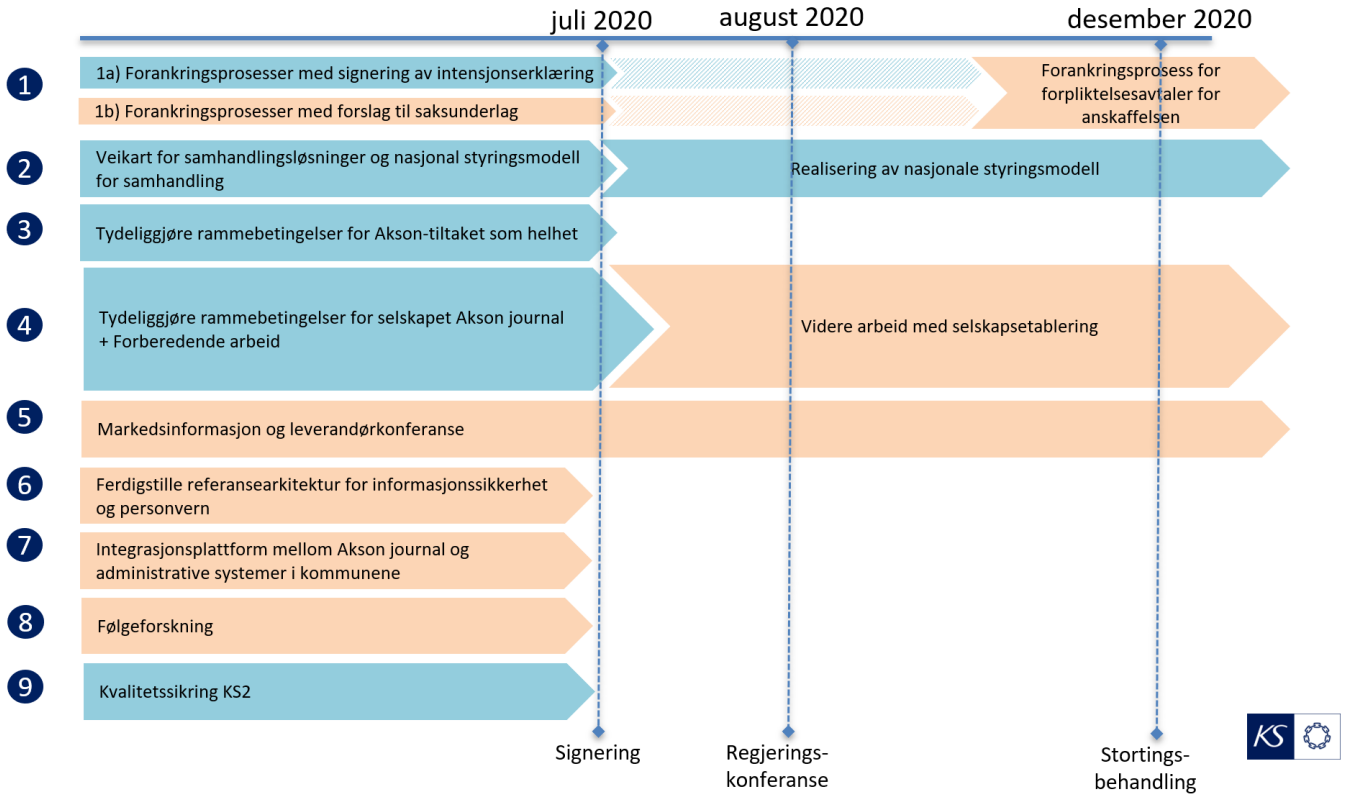
- Bakgrunn for utarbeidelse av RSB.
- RSB i et nøkkeskall.
- Gjennomgang av elementene i RSB.
- Konsekvenser for Akson journal AS og RSB

[1] For mer informasjon om Akson se: https://www.ks.no/fagomrader/digitalisering/utviklingsprosjekter/akson/
[2] Begrepet kommunal sektor benyttes både om kommunene og fylkeskommunene.
[3] Begrepet informasjonssikkerhet inkluderer også teknologisikkerhet.
[4] Begrepet digital beredskap benyttes i forhold informasjonsbehandling.

2. Bakgrunn for utarbeidelse av RSB

Det har vært en dialog mellom Direktoratet for e-helse og kommunal sektor angående hvilke sikkerhetsprinsipper som bør legges til grunn i forbindelse med tiltaket Akson. Ettersom det ikke finnes en helhetlig og metodisk tilnærming til referansearkitektur for sikkerhet, beredskap og personvern i kommunal sektor i et tjeneste- og verdikjedeperspektiv, utarbeidet Oslo kommune og KS i februar 2020 et utkastet til en sådan referansearkitektur.

I diskusjonene etter februar 2020 mellom Direktoratet for e-helse, KS, og kommunene er det satt opp 9 tiltak for videre fremdrift av Akson, se figur 1, *Videre fremdrift Akson*.



Figur 1, Videre fremdrift Akson.

Et av tiltakene i videre fremdrift er tiltak nummer 6, «*Ferdigstille referansearkitektur for informasjonssikkerhet og personvern*» med følgende oppdragsformulering.

Oppdraget
«Utarbeide en referansearkitektur for informasjonssikkerhet, beredskap og personvern som premisser for Akson journal AS og felles kommunale journal sin integrasjon med kommunale administrative systemer, inklusive løsninger for identitets- og tilgangsstyring.»

Leveranser
«*Rapport med beskrivelse av referansearkitektur for kommunesektoren og med tydelig angivelse av premisser for felles kommunal journal og for virksomheten Akson journal AS, inklusive konsekvenser for styringssystem for informasjonssikkerhet og personvern*».

Avgrensninger
«*Referansearkitekturen vil være på strategisk [konseptuelt] nivå med et sett med prinsipper for kommunenes utøvelse av informasjonssikkerhet, beredskap og personvern. Behandlingsansvar er ikke en del av oppdraget*».

Tiltak nummer 6 innebærer å sluttføre det arbeidet som Oslo kommune og KS startet sammen med kommuner og andre aktører i kommunal sektor. Med dette som utgangspunkt har kommunal sektor utarbeidet versjon 1.0 av referansearkitektur for sikkerhet, beredskap og personvern for kommunal sektor (RSB).

Dataeierskapet i Akson er kompleks og det bør nedsettes en egen arbeidsgruppe som bør se på problematikken rundt behandlingsansvaret. Behandlingsansvaret ligger derfor utenfor utforming av RSB.

I forbindelse med utarbeidelsen av RSB er følgende vektlagt:

1) Arbeidsgruppen skal være bredt sammensatt. Hele spekteret av kommunal sektor med kommuner, fylkeskommuner, og skal interkommunale selskaper (IKS) innen IKT skal være representert.
2) Arbeidsgruppen skal være sammensatt av dyktig fagpersonell innen sine respektive fagområder.
3) Legge samstyringsmodellen for kommunal sektor til grunn. Det betyr at RSB behandles i Fagrådet for informasjonssikkerhet og personvern, Digitaliseringsutvalget, og KommIT-rådet for forankring av RSB i kommunal sektor.

Med utgangspunkt i det ovennevnte har arbeidsgruppen for utarbeidelsen av RSB bestått av 11 kommuner, 3 fylkeskommuner, 5 IKS, KINS og KS. Følgende personer har deltatt i arbeidsgruppen:

Type	Navn	Kommune/Fylkeskommune/IKS mv.
Kommuner	Anette Skogstad	Bodø kommune
	Hans Christian Sander	Fredrikstad kommune
	Jørn Hanssen	Harstad kommune
	Marianne Bjønness	Hamar kommune
	Per Jakobsen	Narvik kommune
	Roy Håland	Stavanger kommune
	Rune Nilsen	Tromsø kommune
	Rune Schumann	Oslo kommune
	Sigurd Strand	Larvik kommune
	Thomas Wullun	Horten kommune
	Vilhelm Einen	Larvik kommune
	Øyvind Erikstein	Midt-Telemark kommune
Fylkeskommuner	Egon Nybo Skaar	Viken fylkeskommune
	Espen Solheim	Trøndelag fylkeskommune
	John A. Solstad	Troms og Finnmark fylkeskommune
IKS	Espen Lund	Digitale Gardermoen
	John Horve	LMT Setesdal
	Lars Erik Domaas	Setesdal IKT
	Olve Sveen	IKT Agder
	Stian Jordet	IKT Valdres
Forening	Harald Torbjørnsen	KINS
KS, ledelse	Suhail Mushtaq	KS

I tråd med samstyringsmodellen har RSB vært presentert og diskutert i Fagrådet for informasjonssikkerhet og personvern forløpende. Videre er det gitt en kort orientering om RSB i digitaliseringsutvalget (14. april 2020) og i KommIT-rådet (7. februar 2020). Det er gitt orientering til Fagråd for arkitektur 19. juni 2020. Det blitt gjennomført mer enn 25 møter i perioden januar – juni 2020, både gruppen samlet og bilateralt. Det har blitt også avholdt møter med flere aktører og fagmyndigheter for rådføring og kommentarer. Tilbakemeldinger fra andre aktører og fagmyndighetene er blitt innarbeidet og bidratt til at RSB har blitt enda bedre.

RSB versjon 1.0, fikk faglig tilslutning i Fagrådet for informasjonssikkerhet og personvern den 24. juni 2020.

3. RSB i et nøtteskall

3.1 Dagens utfordringer

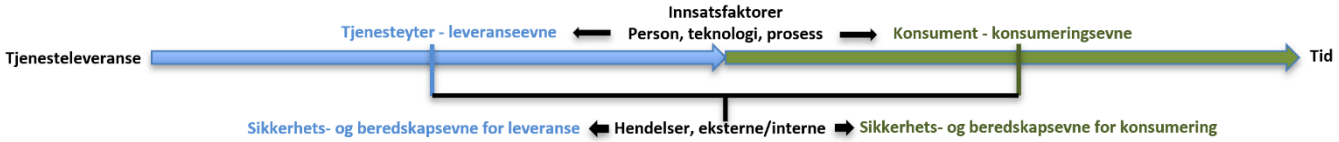
I KS' FoU-prosjekt "Kartlegging av digital modenhet i kommunesektoren"[5] oppgis flere utfordringer knyttet til arbeid med informasjonssikkerhet. Utfordringer er gjerne knyttet til etterlevelse og prioritering og forståelse fra ledelsen. Ofte blir rapporteringer, risikovurderinger, kurs i informasjonssikkerhet og personvern med videre veldig omfattende og med et vanskelig språk. Videre strever mange med å etterleve og gjennomføre alle kravene i en travel hverdag, hvor man har mer enn nok med å gjennomføre de daglige faglige arbeidsoppgaver.

Dagens personvern, sikkerhets- og beredskapsbilde kan fremstå som komplisert, uoversiktlig og utfordrende. For eksempel har man ulik språkbruk om samme teama i ulike lover, standarder og normer. Det virker også å være lite fokus på den menneskelige faktoren. I tillegg til at tjenesteperspektivet virker å være noe fraværende, noe som er primærmålet med enhver virksomhet. Det finnes heller ikke en helhetlig tilnærming til referansearkitektur for sikkerhet, beredskap og personvern i kommunal sektor. Dette i sum gir uheldige ringvirkninger når man skal levere eller konsumenere digitale tjenester i kommunal sektor.

3.2 Hva er RSB

Primærformålet for enhver virksomhet er å levere en eller flere tjenester som enten har et samfunnsøkonomisk[6] eller bedriftsøkonomisk[7] formål. Siden virksomhetens formål er å levere en eller flere tjenester, må disse sikres slik at virksomheten faktisk er i stand til å levere disse tjenestene. Videre, at konsumenten er i stand til å konsumere de. En virksomhet vil ikke operere lenge hvis den ikke er i stand til å levere stabile og gode tjenester til konsumentene over tid.

Tjenesteyter må derfor ha leveranseevne til å levere tjenesten, og sikkerhets- og beredskapsevne til å håndtere hendelser som kan påvirke leveranseevnen. Konsument må ha en konsumeringsevne til å konsumere tjenesten, og sikkerhets- og beredskapsevne til å håndtere hendelser som kan påvirke konsumeringsevnen. Konsumeringsevnen er viktig, ettersom konsumenten som regel er avhengig av denne for å kunne levere sine tjenester. Dette kan uttrykkes som figur 2, *sikkerhets- og beredskapsevne*, nedenfor.



Figur 2, sikkerhets- og beredskapsevne

En tjenesteleveranse kan deles inn i to deler. Del en er tjenesteproduksjon fra tjenesteyter. Tjenesteyter må ha leveringsevne for å kunne levere tjenesten. Del to er konsumeringsevne for konsument til å konsumere tjenesten. Konsumering og leveranse skje ved hjelp av innsatsfaktorer innen dimensjonene person, teknologi, og prosess.

I en optimal verden vil det ikke skje hendelser, og både leveransen og konsumering kan skje uten avbrytelser eller hindringer. Den digitale verden er imidlertid kompleks, ustabil, ukjent, og uforutsigbar. Derfor vil det uavhengig av hvor god sikkerhet, beredskap, og personvern man har, og uavhengig av hvor mange risikoreduserende tiltak som gjennomføres, skje uønskede hendelser. Hendelser som har sitt utspring i interne eller eksterne forhold. Derfor vil

[5] https://www.ks.no/contentassets/3f544fbe44c1404a8b81f7f98737509f/digital-modenhet.pdf

[6] Samfunnsøkonomisk gjelder spesielt offentlige virksomheter. Formålet her er ikke nødvendigvis å tjene penger, men at tjenesten totalt sett gir samfunnet en merverdi. I samfunnsøkonomisk ligger også ideelle organisasjoner med videre.

[7] Bedriftsøkonomisk gjelder spesielt private virksomheter. Poenget med privat virksomheter er ofte å levere tjenester som virksomheten kan tjente penger på. Selv om de er non-profit virksomheter, må også denne type virksomheter tjene penger på sin virksomhet for å kunne videreføres. Unntak kan tenkes i de rene stiftelsesvirksomheter som gir penger til veldedighet og gaver.

evnen til å kunne sikre innsatsfaktorene og håndtere hendelser være avgjørende for å kunne levere kontinuerlig, trygge og sikre tjenester. Det er dette som benevnes som sikkerhets- og beredskapsevne i RSB.

Det er viktig at både tjenesteyter og konsument har tilstrekkelig sikkerhets- og beredskapsevne for å levere og konsumere gode, trygge, og sikre digitale tjenester. Fokuset i RSB er derfor rettet mot digitale tjenesteleveranser, tjenesteyters evne til å levere tjenesten på en trygg og sikker måte, og konsumentens mulighet til å konsumere tjenesten som forutsatt.

RSB har derfor følgende målsetting:

- Ha tjeneste og konsumentfokus – det vil si å sikre tilstrekkelig sikkerhets- og beredskapsevne.
- Redusere risiko langs naturlig arbeidsstrøm ved å ta hensyn til det menneskelig aspekt.
- Legge til rette for Innovasjon, evolusjon og prosessendringer.
- Legge til rette for kontinuerlig utvikling og forbedring.
- Være pragmatisk og ha helhetlig tilnærming til digitale tjenester.

For å finne tilstrekkelig sikkerhets- og beredskapsevne må man kjenne til tjenestekritikaliteten. Dette både fra tjenesteyterens og konsumentens side. For konsumenten er det viktig å vite hvilke kritikalitet og innvirkninger tjenesten vil utgjøre for konsumentens virke. Basert på dette, stille krav til tjenesteyter eller foreta risikoreduserende tiltak slik at tjenesten kan konsumeneres på en trygg og sikker måte. For tjenesteyter vil tjenestekritikaliteten gi en retning på hvilke krav tjenesteyter må oppfylle for å kunne levere tjenesten på en trygg og sikker måte.

Kjernen i RSB er at den skal være pragmatisk og ha en helhetlig tilnærming til å finne tjenestekritikalitet for digitale tjenester. Tjenestekritikaliteten er avgjørende for å kunne dimensjonere tilstrekkelig sikkerhets- og beredskapsevne. Og i en forlengelse av dette, hvilke sikkerhets-, beredskaps-, og personvernprinsipper som bør legges til grunn for å oppnå tilstrekkelig sikkerhets- og beredskapsevne i tråd med tjenestekritikaliteten.

For å finne tjenestekritikalitet, og med hvilken styrke de ulike sikkerhets, beredskaps, og personvernprinsippene skal implementeres for tjenesten, baserer RSB seg på fem grunnprinsipper og fire styringsprinsipper. Disse gir en veiledning på hvilke hensyn som bør vektlegges når man skal finnes tjenestekritikalitet og hvilke sikkerhets-, beredskaps og personvern prinsipper som bør implementeres.

Basert på det ovennevnte kan man uttrykke RSB som en modell med fire lag, og grunn- og styringsprinsipper, se figur 3, *RSB i tjenesteperspektiv*, nedenfor. Modellen leses nedenifra og opp, og hvert lag baserer seg på det underliggende laget. I lag 4 er noen av prinsippene felles for konsument og tjenesteyter, mens andre er kun for konsument, og atter andre er kun for tjenesteyter. Grunn- og styringsprinsippene er gjennomgående i de fire lagene.

Figur 3, RSB i tjenesteperspektiv

Oppsummert kan det sies at jo mer kritisk en tjeneste anses å være, jo sterkere grad må sikkerhets- og beredskapsevnen være til stede både fra tjenesteyter og konsument. Dette for at tjenesten skal kunne leveres og konsumeneres på en trygg og sikker måte som forutsatt. Dette er også kjernen i RSB. Å finne tjenestekritikalitet, og basert på denne, finne hvordan man kan oppnå tilstrekkelig sikkerhets- og beredskapsevne for å levere og konsumere trygge og sikre digitale tjenester.

Med dette som utgangspunkt kan RSB anses som en veiledning/kravsett på hvordan man kan oppnå nødvendig og tilstrekkelig sikkerhets- og beredskapsmessig evne både for tjenesteyter og konsument for å levere eller konsumere sikre og trygge digitale tjenester.

3.2.1 RSB sett fra konsumentens side

Det sentrale i RSB er leveranse og konsumering av digitale tjenester på en trygg og sikker måte. For konsumenten er det viktig å finne ut hvilke kritikalitet og innvirkninger tjenesten vil utgjøre for konsumentens virke. RSB bistår konsumenten med å finne kritikaliteten på tjenesten.

Videre må konsumenten ha tilstrekkelig sikkerhets- og beredskapsevne for å konsumenere tjenesten på en trygg og sikker måte. Basert på tjenestekritikalitet, må konsumenten derfor implementere ulike sikkerhets-, beredskaps-, og personvernprinsipper for å oppnå tilstrekkelig sikkerhets- og beredskapsevne. Disse vil sikre at konsumenten evner å konsumenere tjenesten på en trygg og sikker måte.

For konsumenten er lag 1, 2 og 3 viktig for å finne tjenestekritikalitet for tjenesten som skal konsumenere, samt prinsippene som gjelder for konsument i lag 4 for å oppnå tilstrekkelig sikkerhets- og beredskapsevne.

3.2.2 RSB sett fra tjenesteyters side

Basert på tjenestekritikalitet vil konsumenten stille krav innen sikkerhet, beredskap, og personvern til tjenesteyter slik at tjenesten leveres i forhold til avtale, lov, og forventning. Disse kravene vil tjenesteyter finne igjen som prinsipper i lag 4 basert på tjenestens kritikalitet.

Tjenesteyter må også gi input til konsument i forhold lag 1, 2, og 3. Dette for å komme frem til en felles konsensus om tjenestens innhold, kritikalitet og leveransekvalitet.

Tjenesteyter kan bruke RSB som konsument når tjenesteyter selv skal konsumenere digitale tjenester for sin egen tjenesteproduksjon fra andre underleverandører.

3.3 Hva baserer RSB seg på

Kommuner og fylkeskommuner er fortrolig/familiære med at det skal etableres styringssystem for informasjonssikkerhet og personvern. Det finnes allerede veiledere og standarder for etablering av slike systemer, eksempelvis ISO/IEC 27001/2. Det er derfor viktig å relatere regelverket og forklaringen av regelverket til noe som er praktisk knyttet til egen hverdag. Erfaringen fra kommunal sektor er at man vil følge retningslinjer, rutiner og lovverk, men at de komplekse og ressurskrevende å følge i en hektisk hverdag.

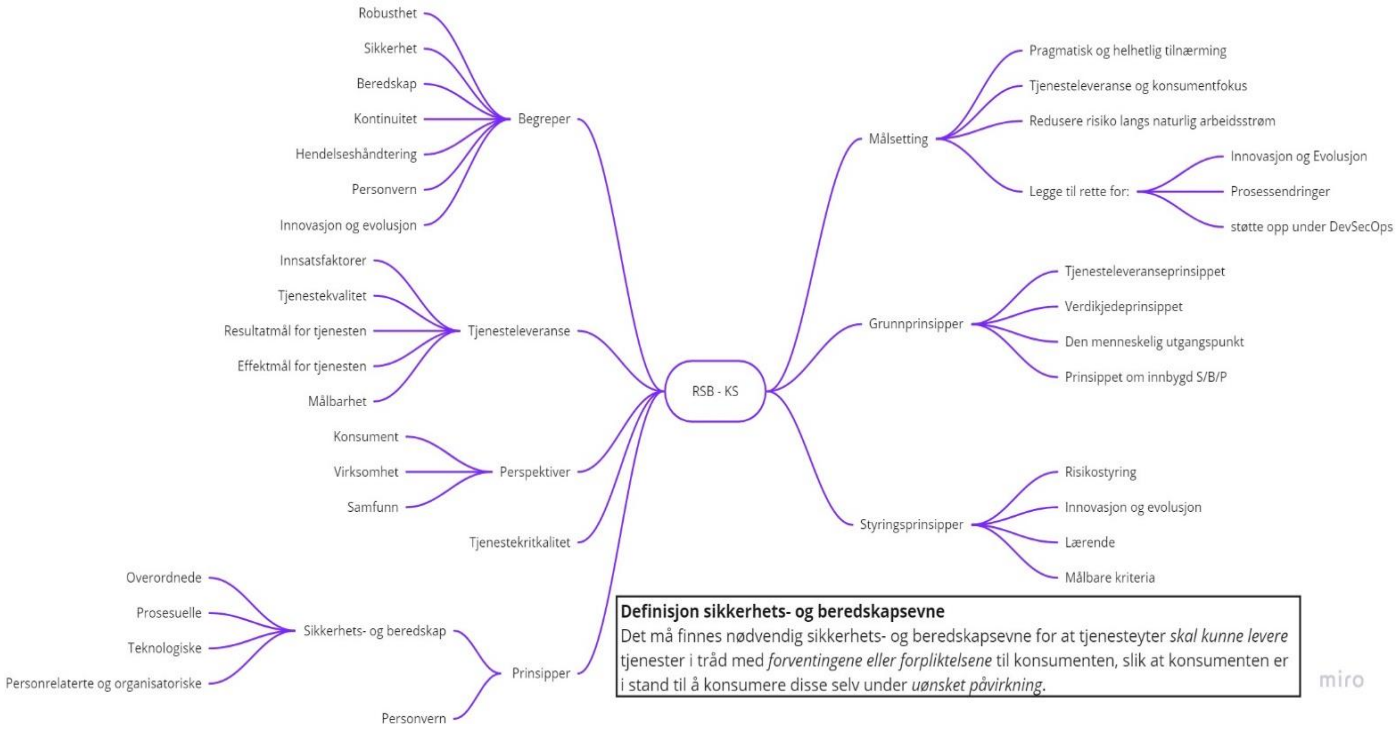
RSB prøver å forenkle et komplekst og krevende tema slik at det blir lettere og oppnå tilstrekkelig sikkerhets- og beredskapsevne for å kunne levere og konsumenere trygge og sikre digitale tjenester. RSB tar utgangspunkt i de strategiske føringene i en rekke standarder, lover, og prinsipper for å systematisere disse på slik måte at de kan følges og etterleves i en hektisk hverdag. RSB kombinerer teorier om forretnings- og leveranseprosesser med sikkerhets-, beredskaps-, og personvern prosesser.

RSB har tatt utgangspunkt i strategiske føringer fra en rekke standarder og prinsipper så som for eksempel:

- ISO27001 / ISO27002 / ISO27005 / ISO270031 / ISO270034 / ISO27035 / NS 5830
- ISO27701 - Security techniques for privacy information management.
- NSM sine grunnprinsipper.
- Nasjonale arkitekturprinsipper (Digitaliseringsdirektoratet), spesielt prinsipp 7.

- Norm for informasjonssikkerhet og personvern i helse- og omsorgstjenesten (Normen).
- Krav til informasjonssikkerhet for skytjenester i offentlige anskaffelser[8].
- NIST.
- CIS Controls.
- Sabsa.
- HRO.
- Six Sigma.
- Lean.
- Med flere.

3.4 Oversikt over RSB



[8] https://www.anskaffelser.no/hva-skal-du-kjope/it/skytjenester-cloud/krav-til-informasjonssikkerhet.

4. Gjennomgang av elementene i RSB

4.1 RSB modellen

Som tidligere nevnt er kjernen i RSB å finne tjenestekritikalitet for å kunne dimensjonere tilstrekkelig sikkerhets- og beredskapsevne for å levere og konsumere trygge og sikre digitale tjenester.

Nedenfor gjennomgås de enkelte elementene i RSB.

4.2 Grunnprinsipper

RSB basere seg på fire grunnprinsipper som gir veiledning på hvilke hensyn som bør vektlegges når man skal finne tjenestekritikalitet, og hvilke sikkerhets-, beredskaps og personvern prinsipper som bør implementeres for å oppnå tilstrekkelig sikkerhets- og beredskapsevne:

- Tjenesteleveranseprinsippet.
- Verdikjedeprinsippet.
- Den menneskelig utgangspunkt – lov om minst mulig anstrengelse i tråd med innovasjon og evolusjon.
- Prinsippet om innbygd personvern, sikkerhet, og beredskap.

Grunnprinsippene som er skissert overfor inngår i ulike lag i RSB modellen og vil bli belyst ytterligere når de ulike lagene gjennomgås. Nedenfor gås det kort gjennom grunnprinsippene.

4.2.1 Tjenesteleveranseprinsippet

Tjenesteleveranseprinsippet handler om evnen til å levere og konsumenere tjenester i tråd med avtale, lov, eller forventninger. Det vil si om virksomheten og konsumenten har nødvendig sikkerhets- og beredskapsmessig evne til å levere og konsumenere sikre og trygge digitale tjenester. I den forbindelse er det avgjørende og finne tjenestekritikalitet. Tjenestekritikaliteten vil avgjøre hvilke sikkerhets- og beredskapsmessig evner som trengs for å kunne levere tjenesten på en trygg og sikker måte.

RSB legger til grunn at ansatte i Akson journal AS og kommunene har en felles forståelse av formålet, innholdet, og viktigheten av de tjenester som skal ytes av Akson journal AS. Dette vil være avgjørende for å kunne levere sikre og trygge tjenesteleveranser.

4.2.2 Verdikjedeprinsippet

Verdikjedeprinsippet handler om tjenesten inngår i en eller flere verdikjeder. Verdikjede[9] kan ses på som en sammenhengende «forsyningskjede» fra ulike virksomheter for å oppfylle en konsumentforespørsel. En verdikjede vil for eksempel kunne spenne over mange sektorer og flere land. En tjeneste vil dermed være en delmengde i en verdikjede.

Verdikjedeprinsippet ser på tjenestens betydning i ulike verdikjeder. Det må derfor komme tydelig frem hvilke kaskadevirkninger tjenesten vil få for konsumentene, det vil si kommunene og innbyggerne, hvis tjenesten blir utilgjengelig eller mister tillitt.

4.2.3 Den menneskelig utgangspunkt

Det menneskelig utgangspunkt tar utgangspunkt i adferdsøkonomi (Behavioral economics), beslutningstaking (Decision making), psykologi og kommunikasjon. RSB legger til grunn at Akson journal AS og kommunene har en klar formening om hvordan tjenesten vil påvirke den daglige arbeidsutførelsen til brukerne. Og i en forlengelse av dette, legger opp arbeidsflyten i tjenesten på en slik måte at den blir en naturlig del i arbeidsutførelsen.

[9] Se NOU 2015: 13 15, *Digital sårbarhet – sikkert samfunn* for mer informasjon om verdikjeder.

4.2.4 Prinsippet om innebygd sikkerhet, beredskap, og personvern

Prinsippet om innebygd sikkerhet, beredskap, og personvern innebærer at tjenesten skal ha innebygde mekanismer for å bistå brukerne med å ivareta sikkerhet, beredskap og personvern. Dette er spesielt viktig i forbindelse for å gjøre tjenesten mer robust, fjerne feilkilder, og redusere risiko for kompromittering av tjenesten eller arbeidsflyten.

4.3 Styringsprinsipper

En kritikalitetsvurdering av tjenesten vil gi en indikasjon på hvor kritisk tjenesten er.

Selv om tjenesten anses som svært kritisk er det ikke dermed sagt at samtlige av sikkerhets, beredskap, og personvern prinsipper skal implementeres for å oppnå god sikkerhets- og beredskapsmessig evne. Det må foretas en avveining i forhold til kost/nytte på hvilke sikkerhets, beredskaps-, og personvern prinsipper som bør implementeres. RSB inneholder styringsprinsipper som gir veiledning til hva som bør vektlegges ved implementering av sikkerhets-, beredskap, og personvernprinsippene.

RSB inneholder følgende styringsprinsipper:

- Risikostyring
- Innovasjon og evolusjon
- Læring
- Målbarhet

4.3.1 Risikostyring

Når det gjelder personvernprinsippene angir artikkel 35 i personvernforordningen når det skal foretas en personvernkonsekvensvurdering. Personvernforordningen er risikobasert. Det må derfor gjøres gode risikoanalyser i tråd med lovgivningen for å ivareta personvernet. For Akson innebærer det at kommunal sektor og Akson journal AS gjør gode risikoanalyser sammen slik at personvernet blir ivaretatt for å skape nødvendig tillitt hos innbyggerne.

Når det gjelder sikkerhets- og beredskapsprinsippene er ikke gitt at alle prinsippene vil være aktuelle. Det må gjennomføres en kost- og kvalitetsanalyse som munner ut i en risikoanalyse med en risikoaksept og restrisiko.

Naturligvis jo høyere kritikalitet på tjenesten, jo sterke styrke vil de ulike prinsippene slå inn. Som eksempel her kan nevnes at hvis man antar at systemet er svært kritisk, bør man gjennomføre kontinuerlige automatiske sikkerhetstester. Er systemer derimot ikke kritisk, trenger man ikke å gjennomføre denne type tester. På den annen side, selv om systemet er svært kritisk, betyr det ikke at man må gjennomføre kontinuerlige automatiske sikkerhetstester. Det kan hende at risikoappetitten er høy eller at det gjennomføres andre risikoreduserende tiltak, at det ikke er nødvendig å gjennomføre denne type tester.

Prinsippet ligger imidlertid fast, tjenestekritikalitet sett opp mot en kost-, kvalitet-, og risikoanalyse vil gi en retning på hvilke prinsipper som bør implementeres.

4.3.2 Innovasjon og evolusjon

Det vil komme ny teknologi på markedet, behovene, arbeidsprosessene, og organisering i kommunale helse- og omsorgstjenesten vil endre seg, og ikke minst vil det skje helsefaglig tjenesteutvikling og samfunnsendringer. Derfor det helt vesentlig at sikkerhet og beredskap ikke legger hindre for innovasjon og evolusjon, men heller søker å øke forenklings- og effektivitetsevne for helsepersonell.

Tjenesten, samt sikkerhets- og beredskapsprinsippene, må derfor designes og gjennomføres på en slik måte at de ikke hindrer innovasjon og evolusjon for tjenesteyter og konsument. De må tvert imot legge til rette og støtte opp under innovasjon og evolusjon.

RSB setter som styringskrav at innovasjon og evolusjon er vurdert i kost-, kvalitets-, og risikoanalyser og for hvert prinsipp som ønskes implementert.

4.3.3 Læring

RSB legger til grunn at den digitale verden er kompleks, ustabil, og uforutsigbar. RSB forutsetter derfor at både tjenesteyter og konsument har gode læringsprosesser spesielt rundt hendelseshåndtering, og av de ulike elementene i leveranse- og konsumentkjeden.

4.3.4 Målbarhet

RSB setter som styringskrav at effektene av sikkerhets-, beredskaps-, og personvern prinsippene som implementeres kan måles. Kost-, kvalitets-, og risikoanalyser sett opp mot tjenestekritikalitet vil gi indikasjoner på hvilke prinsipper innen sikkerhet, beredskap, og personvern som bør implementeres for å oppnå tilstrekkelig sikkerhets- og beredskapsevne.

Styringsprinsippet om målbarhet er gjennomsyret i hele RSB og ikke bare for prinsippene innen sikkerhet, beredskap, og personvern. RSB forutsetter at hvert tiltak eller handling som er av betydning har målbarhetsparametere for å forsikre at tjenestene leveres i tråd med avtale, lov, eller forventning.

4.4 Tjenesteleveranse (lag 1)

Første steg i RSB er å definere hvilke tjeneste(r) som skal leveres og konsumeres. I RSB defineres tjeneste som en leveranse en tjenesteytende virksomhet leverer, og som en konsument konsumerer. Tjenestebegrepet benyttes både om produkter og tjenester.

Tjenesten vil være satt sammen av innsatsfaktorer (innen dimensjonene mennesker, teknologi, og prosesser) hos tjenesteyteren for å oppfylle en konsumentforespørsel. Tjeneste i RSB er definert som et sluttprodukt som leveres av tjenesteyteren til konsumenten. I forbindelse med produksjon av en tjeneste kan denne bestå av mindre delleveranser fra ulike enheter internt/eksternt hos tjenesteyter. Delleveranser anses ikke tjenester i RSB sammenheng, men som en «komponent» inn i tjenesten.

Begrunnelsen for dette er at RSB har konsument- og samfunnsperspektiv. For en konsument er det irrelevant hvordan tjenesteyteren produserer, eller om det inngår delleveranser i tjenesten. For konsument er det viktigst å få sluttproduktet som konsument kan konsumere i tråd med avtale, lov, eller forventning. For tjenesteyteren er det imidlertid viktig å ha oversikt og kontroll over innsatsfaktorene og delleveransene. Dette er helt nødvendig for å sikre gode og robuste tjenesteleveranser. Ved å ha oversikt og kontroll over innsatsfaktorer og delleveranser vil man også kunne finne «enkelt feilpunkter» (single points of failure), avhengigheter, og andre faktorer som kan forstyrre tjenesteleveransen. Et annet aspekt er at det er viktig for tjenesteyteren å ha kunnskap om hva som skal til av innsatsfaktorer for å kunne levere robuste tjenester i tråd med avtale, lov, eller forventning.

I forbindelse med tjenesteleveranser i RSB gjør følgende to aspekter seg gjeldende:

- Innsatsfaktor.
- Tjenestekvalitet (kvalitetsnivå).

For å kunne levere en tjeneste av en viss kvalitet (tjenestekvalitet), må det finnes innsatsfaktorer som gjør det mulig å levere tjenesteleveransen. Tjenestekvalitet innebærer hvilken kvalitet tjenestene skal leveres til konsumenten. Det kan være en eller flere kvalitetsnivåer. Hva som ligger i de forskjellige kvalitetsnivåene vil kunne variere i henhold til avtale, lov eller forventning mellom partene.

Sammenheng mellom innsatsfaktorer og tjenestekvalitet vises i figur 5 nedenfor (kvalitetsnivåene bronse, sølv og gull er kun navneeksempler på tjenestekvalitet).

Tjeneste-leveranse	Tjenestekvalitet		
	Bronse	Sølv	Gull
	Innsatsfaktor 1		
	Innsatsfaktor 2	Innsatsfaktor 4	
	Innsatsfaktor 3	Innsatsfaktor 5	Innsatsfaktor 7
		Innsatsfaktor 6	Innsatsfaktor 8
			Innsatsfaktor 9

Figur 5, sammenheng mellom innsatsfaktorer og tjenestekritikalitet

I elementet tjenesteleveranse er fem faktorer som gjør seg gjeldene for konsument og tre for tjenesteyter.

For konsument gjelder følgende fire faktorer som må kartlegges:

1) Hvilke tjenester skal mottas og i hvilke kvalitet, hva de skal utrette, og hvilke gevinster tjenesten skal gi (resultat- og effektmål).
2) Om tjenesten støtter opp under naturlig arbeidsflyt.
3) Om tjenesten vil bidra til forenkling, automatisering, forbedring, og en god brukeropplevelse.
4) Avhengigheter og andre kritiske faktorer som kan medføre at tjenesten kompromitteres eller mister tillitt.
5) Målbare indikatorer for å bekrefte om tjenesten utretter det den skal, gir antatt gevinst, og understøtter konsumentens virke.

For tjenesteyter gjelder følgende tre faktorer som må kartlegges:

1) Hvilke innsatsfaktorer som skal til å kunne levere tjenesten med en gitt kvalitet.
2) Avhengigheter og andre kritiske faktorer som kan medføre at tjenesten kompromitteres eller mister tillitt.
3) Målbare indikatorer for å bekrefte om leveransen er i tråd avtale, lov, eller konsumentens forventning.

Det er viktig at konsumenten og tjenesteyteren har en felles forståelse av hva tjenesteleveransen innebærer, hvilke kvalitet denne skal leveres i, hvilke robusthet tjenesten skal ha, og ikke minst hvordan den skal leveres. Det er derfor viktig at kommunal sektor og Akson Journal AS har en felles forståelse og konsensus på hva som er tjenesteleveransen og innholdet i denne.

4.5 Perspektiver (lag 2)

Første steg i RSB handler om at konsumenten og tjenesteyteren har en felles forståelse og konsensus om tjenesten, og hva tjenesteleveransen innebærer. Steg to i RSB handler om å vurdere føringene som ligger i virksomhets-, konsument- og samfunnsperspektivet. Perspektivene gir input til kritikalitetsvurderingen, og i neste omgang sikkerhets-, beredskaps-, og personvernprinsippene.

Nedenfor gjennomgås disse perspektivene.

4.5.1 Virksomhetsperspektivet

Virksomhetsperspektivet handler om tjenesteyter. Tjenesteyter må ha en robust virksomhet som evner å levere avtalte tjenester. Det innebærer blant annet at tjenesteyter må pålitelighet ved utførelse av komplekse oppgaver under tidspress, samt ha lav forekomst av ulykker, avbrudd og feiltoleranse gjennom flere år. Jo høyere kritikalitet på tjenesten, jo høyre krav til robusthet for tjenesteyter og pålitelighet for tjenesten.

I virksomhetsperspektivet ligger det vurdering av leveranse- og modenhetsevne til tjenesteyter:

- Om tjenesteyter og dens ansatte forstår tjenesteleveransen og verdikjeden og har nødvendig modenhet for å levere tjenesten.
- Om tjenesteyter har en organisasjonskultur som legger til rette for læring, samhandling og korreksjon.
- Om nødvendige kommunikasjonslinjer mellom tjenesteyter og samarbeidspartnere er opprettet.

- Om det er felles konsensus om tjenesteleveransens viktighet for konsumenten mellom tjenesteyter og tjenesteyters samarbeidspartnerne.
- At tjenesteyter forutsetter at feil vil skje, men forstår verdikjeden og tjenesteleveransen og kan derfor håndtere selv det uventede. Dette for å påse at tjenesten leveres kontinuerlig i tråd med avtale, lov og forventning.

4.5.2 Samfunnsperspektivet

Den teknologiske utviklingen og integrerte informasjonssystemer bidrar til økt samvirke og mer effektive tjenester. Samtidig fører dette med seg avhengigheter mellom konsumenter og tjenesteytere, mellom tjenesteytere, mellom konsumenter, og samfunnet med det resultat at man i praksis kan se på mange delsystemene som et stort hele med innbyrdes varierende grad av kritikalitet.

Den overordnet målsetting for Akson er å tilrettelegge for bedre samvirke i helsesektoren, med mer tidseffektive og tidsriktige løsninger for å løse de utfordringer som helsesektoren står ovenfor. Det underliggende spørsmålet er derfor hvilke kaskadeeffekter det vil få for konsument, samfunnet, tjenesteyter, samarbeidspartnere, og innbyggerne hvis man for eksempel tenker seg at tjenesten blir kompromittert (for eksempel integriteten, tilgjengeligheten, konfidensialiteten, eller kvalitet), eller at tillitt til systemet bortfaller i ulik grad.

I samfunnsperspektivet ligger det vurdering av kaskadevirkninger og kost/gevinstberegninger:

- Hvilke kaskadeeffekter det vil få for konsument, samfunnet, samarbeidspartnere, innbyggerne og verdikjedene hvis tjenesten blir kompromittert eller at tillitt til tjenesten bortfaller i ulik grad.
- Om det finnes alternative tjenester eller prosesser (og på hvilket nivå), for å opprettholde konsumentens virke i den perioden tjenesten er bortfalt eller tillitten til tjenesten er lav.
- Om tjenesten lar seg reetablere og i hvilken grad hvis kompromitteringen er fatal.

4.5.3 Konsumentperspektivet

Konsumentperspektivet (for Akson vil dette både være kommunene og innbyggerne) handler om konsumentens mulighet til å konsumere tjenesten i forhold til avtale, lov, og forventning.

Selv om kritikaliteten og sensitiviteten til informasjonen vil variere, må konsumenten forvente at informasjon håndteres i tråd med avtale, lov, og forventing. I tillegg er det viktig at konsumenten selv evner å levere sine tjenester ved å konsumere tjenesteyters tjenester. Poenget er at tjenesten må leveres og bygges på en slik måte at konsumenten faktisk er i stand til å konsumere disse med positivt utfall, og ikke bare få «levert» tjenesten.

I konsumentperspektivet ligger hvilken grad konsumenten kan nyttiggjøre seg av tjenesten:

- Om tjenesten er bygd og levert slik at konsumenten evner å konsumere tjenesten med positivt utfall.
- At informasjonen håndteres på en trygg måte både i forhold til informasjonsbehandlingen og ivaretakelse.
- At tjenesten er endringsdyktig i tråd med konsumentsbehov, følger teknologi- og samfunnsutviklingen, og legger til rette for innovasjon og evolusjon for konsumenten.
- At konsumenten forstår tjenesteleveransen og har nødvendig modenhet for å nyttiggjøre seg av denne.

4.5.4 Oppsummering perspektivene

Formålet med perspektivene er å gi generell input for å finne kritikalitet til en tjeneste. Perspektivene er ikke uttømmende, og det vil være andre vurderingskriteria avhengig av tjenestetype.

4.6 Tjenestekritikalitet (lag 3)

Første steg i RSB er å kartlegge tjenester. Andre steg er å gå gjennom perspektivene for å gi input til kritikalitetsvurderingen. Tredje steg i RSB er å finne ut hvilken kritikalitet en tjeneste har. Dette er helt nødvendig å finne ut hvilken kritikalitet tjenesten representerer for konsument, tjenesteyter, og samfunnet som sådan.

Fra konsumentens ståsted er viktig og finne ut hva tjenesten betyr for konsumentens virke og oppdragsutførelse, samt hvilke prosessøkonomiske konsekvenser tjenesten representerer hvis tjenesten blir utilgjengelig eller at tillitten til den bortfaller (for eksempel på grunn av at integriteten i systemet er brutt). I forhold til Akson betyr det å finne ut hvor viktig felles kommunal journal er for kommunen(e), og hvilke prosessøkonomiske konsekvenser dette vil gi kommunen(e) hvis løsningen er utilgjengelig eller mister tillitt.

For tjenesteyter blir det viktig å finne ut hva det vil innebære hvis tjenesteyter ikke evner å levere tjenesten, eller at tillitt til tjenesten bortfaller. For Akson journal AS betyr det å finne ut hvilke innsatsfaktorer er nødvendig for å oppfylle tjenesteleveransen, avhengigheter, og andre kritiske faktorer. Og videre, hvordan innsatsfaktorene skal beskyttes for å opprettholde nødvendig robusthet i kontinuerlig tjenesteleveranse.

Fra et samfunnsperspektiv blir det også viktig å kartlegge kaskadevirkningene av at tjenesten blir utilgjengelig, eller at den mister tillitt. For eksempel at persondata kommer på avveie. Eller at personene som skal inn til behandling ikke får nødvendig behandling fordi tjenesten er utilgjengelig. Eller at integritet til data er brutt og man ikke lenger kan stole på innholdet. For Akson journal AS og kommunene betyr det å finne ut hva det innebærer for samfunnet og innbyggerne at felles journalløsning ikke er tilgjengelig eller har mistet tillitt. Og i forlengelse av dette, om det finnes alternativer (for eksempel gjennom manuelle rutiner) som fortsatt kan bidra til å opprettholde en viss grad av kommunenes virke og forpliktelser.

Å finne kritikalitet på tjenesten er en viktig del av RSB. Hvis man ikke har en fellesforståelse og konsensus av kritikalitet mellom konsument og tjenesteyter, da vil det være vanskelig å dimensjonere robusthet og leveransekrav til tjenesten. For at tjenesteyter og konsument skal ha samme forståelse til tjenestekritikalitet bidrar RSB med en veiledning på hvordan man kan regne ut kritikalitet til en tjeneste. Dette gjøres ved å sette score fra 0 – 5 på 20 elementer av konsumenten og tjenesteyter i samarbeid, se tabellene nedenfor.

Kategori	Kritikalitetselement	Beskrivelse
Vurderes av konsument		
Informasjon	**Tilgjengelighet**	Maksimal utilgjengelighet. Jo kortere tid som aksepteres, jo høyere score.
	Integritet	Om man kan stole på de data som ligger i systemet. Jo mindre avvik som aksepteres, jo høyere score.
	Konfidensialitet	Andel av data som kan komme på avveie eller blir tilgjengeliggjort for uvedkommende. Jo mindre avvik som aksepteres, jo høyere score.
	Autentisitet (identifikasjon)	Ektheten til data og tjenester samt opprinnelse. Jo mindre avvik som aksepteres, jo høyere score.
	Kvalitet	Om data skal brukes som beslutningsdata. Jo større krav til at data skal være beslutningsdata, jo høyere score.
	Tillitt (pålitelighet)	Grad av tillitt til tjenesten. Jo høyre grad av tillitt som kreves, jo høyere score.
	Sporbarhet	Krav til sporbarhet for data og transaksjoner. Jo større krav til sporbarhet, jo høyere score.
	Persondata	Krav til behandling av personopplysninger. Jo større krav til sikring av personopplysninger, jo høyere score.
Leveranse	**Funksjon**	Om hvor viktig eller avgjørende tjenesten er for konsumentens arbeidsutførelse. Jo mer viktig/avgjørende tjenesten anses å være, jo høyere score.
	Alternativer	Om det finnes alternativer til å opprettholde konsumentens virke og forpliktelser ved bortfall av tjenesten. Jo færre alternativer, jo høyere score.
	Avtaleverk	Om avtalen oppfyller tjenesteleveransens formål og krav. Jo dårligere oppfyllelse, jo høyere score.

	Leveringsevne	Om benyttede leverandører/tjenesteyter har tilstrekkelig overlevelsesevne. Jo mindre overlevelsesevne, jo høyere score.
	Modenhet tjenesteyter	Om tjenesteyter er moden til å levere tjenesten. Jo større krav til modenhet, jo høyere score.
	Modenhet konsument	Om konsument er moden til å konsumenere tjenesten. Jo større krav til modenhet, jo høyere score.
Teknologi og ressurser	**Teknologisk modenhet**	Om teknologien som er tenkt valgt er agil, skalerbar, åpen, utskiftbar, fremtidsrettet og levedyktig. Jo mindre teknologisk modenhet, eller større krav til teknologisk modenhet, jo høyere score.
	Kompetanse	Om det finnes mye kompetanse/ressurser på produkter/tjenester. Jo mindre tilgjengelig kompetanse, jo høyere score.
Økonomi	**Kostberegning**	Det gjennomføres en kostnadsutregning for bortfall av tjenesten (økonomi, liv/helse, kaskadeeffekt mv) for konsument og samfunn. Jo høyere kost, jo høyere score.
Vurderes av tjenesteyter i samarbeid konsument		
Prosess	**Kontrollerbarhet**	Om hvor kontrollerbar tjenesteleveransen er fra produksjon til konsum. Jo mer krav til kontroll, jo høyere score.
	Avhengigheter	Om tjenesten har avhengigheter og andre kritiske faktorer som er en forutsetning for leveransen. Jo flere avhengigheter/kritiske faktorer, jo høyere score.
	Økonomisk tilfang	Om tjenesten vil få økonomisk tilfang slik at den at den kan leveres med ønsket resultat og funksjonsevne i tjenestens livsløp. Jo større usikkerhet til økonomisk tilfang, jo høyere score.

Når det gjelder elementet økonomisk tilfang er det viktig å understreke at hvis tjenesten ikke sikres økonomisk tilfang i tjenestens livsløp, anses dette til å være så kritisk for tjenesten at det bør revurderes om den bør igangsettes.

Etter at man har satt score mellom 0 – 5 på hvert enkelt element vil man få en totalscore mellom 0 – 100 for tjenesten. Hva det betyr kan man lese ut av veiledningstabellen for kritikalitetsskala nedenfor.

Kritikalitetsskala		**Beskrivelse**
For elementene	**For tjenesten**	
5	81 – 100	Svært kritisk
4	61 – 80	Kritisk
3	41 – 60	Mindre kritisk
2	21 – 40	Noe kritisk
1	1 – 20	Ikke kritisk
0	0	Ikke relevant

Kritikalitetsmetodikken i RSB benyttes både av konsumenten og tjenesteyter. For konsumenten å finne ut hvor kritisk tjenesten er for konsumentens funksjonsevne. For tjenesteyter å finne ut hvor robuste innsatsfaktorene må være for å kunne levere kontinuerlig trygge og sikre tjenester.

Det er derfor vesentlig at kommunal sektor og Akson Journal AS har en felles forståelse og konsensus av kritikalitet til tjenester som skal leveres. Kritikalitetsvurderingen kan anses som et grunnleggende kravsett på hvor robust tjenesten må være i forhold til leveranse og konsum.

4.7 Sikkerhets-, beredskaps-, og personvernprinsipper (lag 4)

Fjerde steg i RSB er å avgjøre hvilke av sikkerhets-, beredskaps, og personvernprinsipper som bør innføres for å gi tilstrekkelig sikkerhets- og beredskapsevne for å levere tjenesten på en trygg og sikker måte.

For å ivareta informasjonssikkerhet må sikkerhetsdimensjonene fysisk sikkerhet, logisk sikkerhet (herunder psykologisk sikkerhet), og teknologisk sikkerhet være til stede. I RSV versjon 1.0 fokuseres det hovedsakelig på logisk og teknologisk sikkerhet.

4.7.1 Begreper i RSB

RSB bruker flere begrep for å beskrive innholdet i prinsippene for sikkerhet, beredskap, og personvern. I den videre fremstillingen går man først gjennom begrepsapparatet som blir brukt i prinsippene, deretter forholdet mellom begrepene, og til slutt selve prinsippene. Denne tilnærmingen er gjort da det gir en bedre bakgrunn for å forstå prinsippene og formålet med RSB. Prinsippene må leses med bakgrunn i begrepsapparatet.

RSB benytter følgene begreper:

- Robusthet.
- Sikkerhet.
- Beredskap.
- Kontinuitet.
- Hendelseshåndtering.
- Personvern.

Nedenfor gjennomgås de ulike begrepene i RSB.

7.5.1.1 Robusthet i tjenesteleveransen

RSB skal bidra til å oppnå tilstrekkelig sikkerhets- og beredskapsevne for å levere og konsumere trygge og sikre digitale tjenester. RSB har fokus på tjenesteleveranser. RSB handler derfor ikke om sikkerhetsstyring på virksomhetsnivå eller operativ sikkerhetshåndtering.

Sikkerhetsstyring på virksomhetsnivå handler om hvordan man skal arbeide med informasjonssikkerhet i et virksomhetsperspektiv. Det vil si styringssystemer, ledelsens gjennomgang, og sikkerhetsorganisering med videre. Operativ sikkerhetshåndtering handler om hvordan man operasjonaliserer og effektuerer ulike tiltak. For eksempel være patching, overvåking av systemer, teknisk sikkerhetsarkitektur med videre. Selv om RSB først og fremst har fokus på tjenesteleveranser, vil RSB kunne være dimensjonerende for sikkerhetsstyring og sikkerhetshåndtering. eller sikkerhetshåndteringen. Dette fordi kritikaliteten til tjenesten kan gi utslag i dimensjonering av sikkerhetsstyring og sikkerhetshåndtering.

I RSB defineres sikkerhets- og beredskapsevne på denne måten:

Det må finnes nødvendig sikkerhets- og beredskapsevne for at tjenesteyter *skal kunne levere* tjenester i tråd med *forventingene eller forpliktelsene* til konsumenten, slik at konsumenten er i stand til å konsumere disse selv under *uønsket påvirkning*.

Med utgangspunkt i den ovennevnte definisjonen inneholder den tre perspektiver og fire grunnelementer. Disse kan man lese ut av det som er skrevet i kursiv.

De tre perspektivene er (for mer informasjon om perspektivene se kapittel 4.5):

- Virksomhetsperspektivet
- Samfunnsperspektivet
- Konsumentperspektivet

De fire grunnelementene er:

- Sikkerhet
- Beredskap og kontinuitet
- Personvern
- Innovasjon og evolusjon

I ordene *skal kunne levere* ligger virksomhetsperspektivet og grunnelementet sikkerhet. I ordene *forventingene eller forpliktelsene* ligger konsumentperspektivet og grunnelementene personvern, innovasjon og evolusjon. I ordene *uønsket påvirkning* ligger samfunnsperspektivet og grunnelementene beredskap og kontinuitet. Det er viktig å understreke at grunnelementene og perspektivene er uavhengig av hverandre og flere grunnelementer kan inngå i et perspektiv.

I perspektivene og grunnelementene ligger det implisitt et viktig grunnelement som går gjennom alle perspektivene og grunnelementene – hendelseshåndtering. Det vil før eller siden skje hendelser uavhengig av hvor god sikkerhet, beredskap og personvern man har. Det er derfor helt avgjørende at man evner å håndtere hendelser for å opprettholde gode, trygge og sikre tjenesteleveranser. Hendelseshåndtering er derfor en viktig del av RSB.

7.5.1.2 Begrepet sikkerhet

Tjenesteleveranseperspektiv i RSB har både en konsument- og tjenesteytendeside. Konsumenten forutsetter at tjenesten leveres som avtalt eller forventet fordi konsumenten selv er avhengig av tjenesten for å gjennomføre sitt virke. Tjenesteyteren på sin side må forholde seg til alle typer avvik som kan forstyrre tjenesteleveransen, uavhengig hvilke merkelapper man ønsker å sette på hendelsene.

Med utgangspunkt i det ovennevnte kan man oppsummer leveranseevnen på følgende måte:

1) Tjenesteyters evne til å kunne levere tjenesten.
2) Tjenesteyters evne til å skape tillit til tjenesteleveransen og mellom partene.
3) Konsumentens evne til å konsumere tjenesten i en positiv kontekst. Det vil si om det er knyttet positivitet til bruk av tjenesten for konsumenten. Det vi si at tjenesten ikke oppleves som en hinder i konsumentens naturlige arbeidsflyt, innovasjon og evolusjon.

En tjenesteleveranse vil kunne forstyrres av mange typer avvik. Tjenesteyter må derfor ha en evne til å håndtere ulike hendelser, herunder sikkerhetshendelser. Det vi si at en tjenesteyter må ha nødvendig og tilstrekkelig sikkerhetsmessig evne til å levere tjenesten ved å beskytte innsatsfaktorene, tiltak mot avbrudd, samt ha nødvendig kapasitet for å håndtere hendelser.

I en slik kontekst defineres begrepet sikkerhet i RSB som ulike risikoreduserende tiltak for å oppnå en tilstrekkelig sikkerhetsevne for å kunne levere digitale tjenester kontinuerlig i henhold til avtale, lov, eller en forventning.

7.5.1.3 Begrepene beredskap og kontinuitet

7.5.1.3.1 Beredskap

Beredskap[10] betyr i utgangspunktet «å være beredt». Beredskap betyr at man har dimensjonert seg på slik måte at hvis en uønsket hendelse inntreffer og som krever ressurser utover normal drift skal man kunne håndtere denne på en effektiv måte. Dette for å redusere risikoen for tjenestens utilgjengelighet, og opprettholdes av funksjonsevnen.

God beredskap er avgjørende for å opprettholde trygge og sikre tjenesteleveranser. Kvalitet, læringsevne, evne til kontinuerlig forbedring av organisasjon, teknologi, prosesser, og kompetent personell på alle nivå i organisasjonen er derfor nøkkelfaktorer for å kunne lykkes med god beredskap. Robuste

[10] DSB sin veileder til forskrift for kommunal beredskapsplikt, jf også NOU 2000:24 Et sårbart samfunn, NOU 2006:6 Når sikkerheten er viktigst.

beredskapsorganisasjoner har gode prosesser og kompetent personell for å håndtere krevende og kompliserte situasjoner som kan strekke seg over lengre tidsperioder.

RSB baserer seg på de nasjonale beredskapsprinsippene om ansvars, likhet, nærhet og samvirke. Prinsippene innebærer at det er den ordinære linjen som er fundamentet i beredskapsarbeidet, og at risikodempende tiltak i størst mulig grad skal håndteres som linjeaktiviteter. Samtidig har alle i virksomheten et selvstendig ansvar for å sikre best mulig samvirke med andre interne og eksterne relevante aktører, organisatoriske enheter og virksomheter. Innen beredskap vil det finnes ulike beredskapsnivåer, f.eks. grønn (nivå 0), gul (nivå 1), oransje (nivå 2), og rød (nivå 3) og så videre avhengig av hendelseskritikalitet.

7.5.1.3.2 Kontinuitet

Med kontinuitet menes en uavbrutt sammenheng. En virksomhet eller dets konsumenter er i stor grad avhengig av IKT-systemer, og i mange tilfeller er det IKT-systemene som muliggjør virksomhetens eksistens.

Kontinuitetsstyring i RSB har to dimensjoner. Den ene dimensjonen er hvordan man benytter sikkerhet for å opprettholde kontinuitet i normal tjenesteproduksjon.

Det andre dimensjonen er hvordan man hurtigst mulig gjenopptar tjenesteleveranser etter en større feil eller katastrofe. Dette for at tjenesteyter raskest mulig skal være i stand til å gjenoppta sin normale virksomhet og leveranse av tjenester. Kontinuitetsstyring skal bidra til å sikre virksomhetens funksjonsevne, og i forlengelse av dette, omdømme, merkevare, interesser og tjenester. Kontinuitetsstyring skal også bidra til at konsumenten får gjennomført sine leveranser slik at kaskadevirkningen blir minst mulige.

I RSB refereres kontinuitetsstyring til den andre dimensjonen. Det vil si gjenoppretting. Det innebærer at man gjennom kontinuitetsstyringen skal gjenopprette tjenesteleveransen raskest mulig for å kunne tilby kontinuerlige trygge, sikre og pålitelige digitale tjenester til konsumenten.

7.5.1.4 Kort om hendelseshåndtering

Uavhengig av hvor god sikkerhet, beredskap, og personvern man har, og uavhengig av hvor mange risikoreduserende tiltaks som gjennomføres, vil det skje uønskede hendelser.

Det er ikke praktisk mulig å forhindre alle hendelser. Som en del av risikohåndteringen etableres det derfor tiltak som har til hensikt å oppdage uønskede hendelser (enten tilsiktede eller utilsiktede), og for å håndtere og redusere konsekvensene av disse. Hendelseshåndtering handler om evnen til å kunne oppdage og håndtere hendelsen ved hjelp av teknologiske, organisatoriske, og personelle tiltak.

I RSB anses hendelseshåndtering som en svært viktig komponent for å kunne opprettholde tjenesteyterens og konsumentens funksjonsevne. RSB legger videre systematikken rundt hendelseshåndtering tett opp til drifts-, forvaltnings-, sikkerhets-, og beredskapsplanverk, slik at man benytter samme begrepsapparat for alle dimensjoner av tjeneleveransen for å fjerne eventuelle misforståelser i leveransekjeden.

7.5.1.5 Begrepet personvern

Personvern[11],[12] anses som en ivaretakelse av personlig integritet. Det vil si ivaretakelse av enkeltindividers mulighet for privatliv, selvbestemmelse (autonomi) og selvutfoldelse. Personvern blir knyttet til retten til å ha en egen private sfære som man selv kontrollerer, ytringsfrihet, og det å kunne operer som et selvstendig individ.

Personopplysningsvern har ivaretakelse av personvern som hovedmål, og handler om å ha regler og standarder for behandling og oppbevaring av persondata. Regelens formål er å sikre enkeltindividers oversikt

[11] https://www.datatilsynet.no/rettigheter-og-plikter/hva-er-personvern/
[12] https://www.regjeringen.no/no/tema/statlig-forvaltning/personvern/id1373/

og kontroll over behandling av opplysninger om dem selv. Personopplysningsvern blir knyttet til muligheten til selv å kontrollere hvordan, når, hvor mye, og hvilken informasjon om seg selv kan spres til andre aktører/entiteter. I hverdagen brukes gjerne personvern om personopplysningsvern, og da spesielt i forhold til General Data Protection Regulation (GDPR).

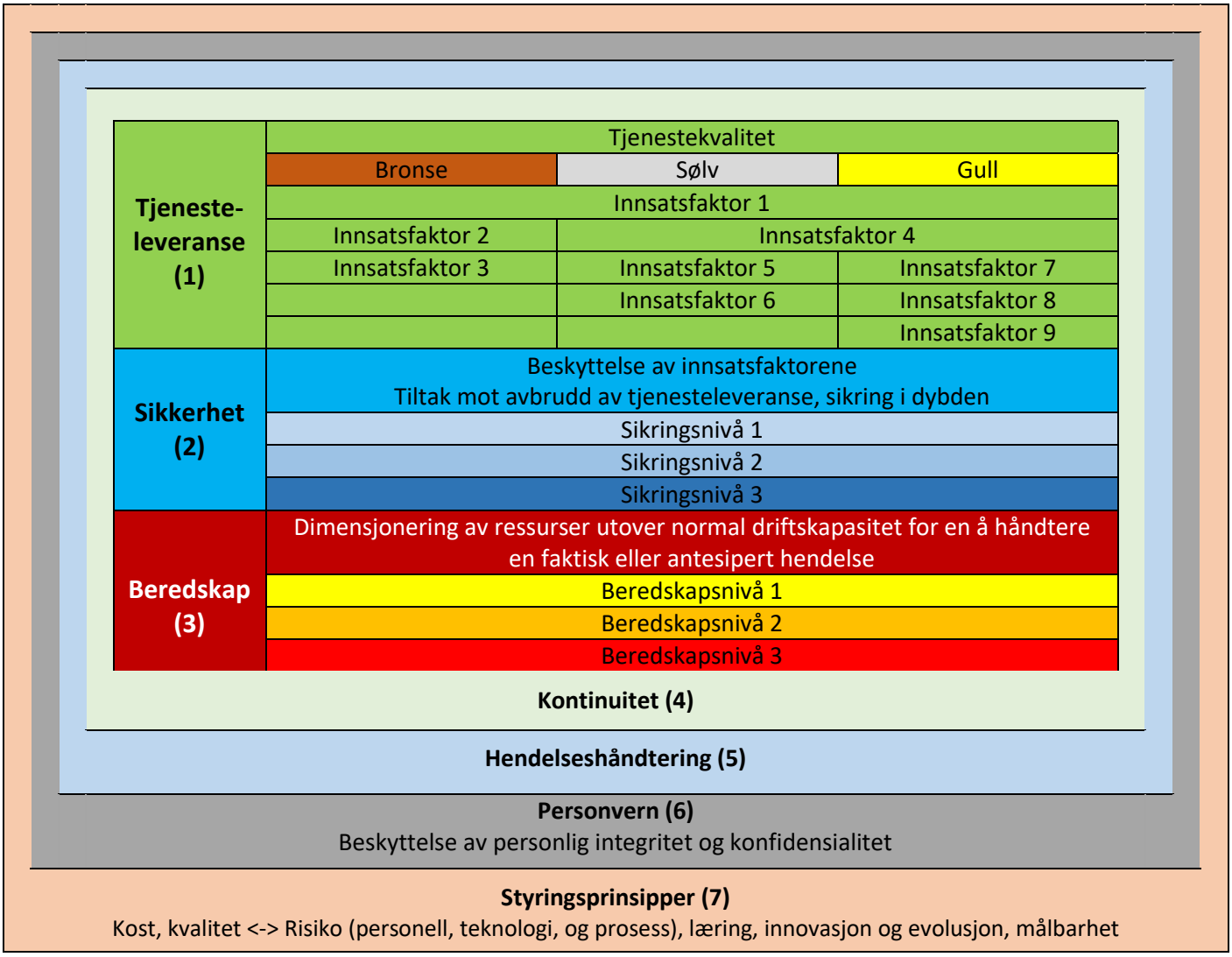
Akson kommer til å samle store mengder av persondata, herunder sensitiv helsedata. Personvernet skal sikre behandlingen av persondata, slik at individers integritet og privatliv ikke krenkes. Derfor er registrertes tillitt til tjenesten helt avhengig av at persondata data håndteres i tråd med lov og registrertes forventninger.

For å forenkle fremstillingen bruker RSB begrepet personvern som et samlebegrep om beskyttelse av personlig integritet og konfidensialitet i tråd med personvernlovgivningen.

Med personlig konfidensialitet menes at informasjonen til registrerte behandles fortrolig, lovlig, og riktig med et klart definert formål. I dette ligger det også at det er åpenhet om formålet og hvordan registrertes informasjon håndteres. Med personlig integritet mens ansvarlighet og ivaretakelse av registrertes rettigheter slik at rettsikkerheten og den personlige sfæren til registrerte er ivaretatt.

7.5.1.6 Sammenhengen mellom tjenesteleveranse og begrepene i RSB

Ovenfor har vi gått gjennom sentrale begreper i RSB. Sammenhengen mellom begrepene illustreres med figur 6, *sammenheng mellom begreper*, nedenfor. Figuren leses innen ifra og ut med tjenesteleveranse som startpunkt.



Figur 6, RSB, sammenhengen mellom begreper

Nedenfor følger en forklaring på sammenheng mellom begreper i RSB.

(1) Tjenesteleveranse:

1) En tjenesteleveranse er ofte inndelt i ulike tjenestekvaliteter. Navnet på tjenestekvalitetene vil variere avhengig av sektor og bransje. For å kunne levere en tjeneste i en viss kvalitet må det finnes ulike personelle, teknologiske, og prosessuelle innsatsfaktorer.
2) Innsatsfaktorene må dimensjoneres slik at tjenesteyter evner og levere sammenhengende digital tjeneste i tråd med avtale, lov, eller forventning til konsumenten.

(2) Sikkerhet:

3) Det må finnes nødvendig sikkerhet (risikoreduserende tiltak) for å beskytte innsatsfaktorene, og mot avbrudd i tjenesteleveransen.
4) Sikkerhet gjennomføres ved sikring i dybden gjennom ulike sikringsnivåer, slik som f.eks. sikringsnivå 1, 2 og 3 osv. Innholdet i sikringsnivåene vil avhenge av tjenestekritikalitet sett opp imot tjenestekvalitet og risiko.

(3) Beredskap:

5) I noen situasjoner vil ikke sikkerhet eller innsatsfaktorene være nok til å opprettholde tjenesteleveransen. Man må derfor gjennom beredskap dimensjonere seg på slik måte at hvis en uønsket hendelse inntreffer (enten faktisk eller antesipert) og som krever ressurser utover normal drift/forvaltning, kan håndteres på en effektiv måte.
6) Beredskapen vil inneholde ulike beredskapsnivåer avhengig av tjenestekritikalitet sett opp imot tjenestekvalitet og risiko.

(4) Kontinuitet:

7) Uansett hvor mye man sikrer seg vil det inntreffe større feil av «katastrofal» art.
8) Man må derfor ha en kontinuitetsstyring for å sikre og funksjonsevne både for seg selv og de som er avhengig av tjenesten. Dette for å være i stand til å gjenoppta normal drift og leveranser av tjenester raskest mulig.

(5) Hendelseshåndtering:

9) Hendelseshåndtering handler om hvordan man skal oppdage og håndtere hendelser.
10) Uavhengig av hvor god sikkerhet, beredskap, og antall risikoreduserende tiltaks som gjennomføres, vil det skje uønskede hendelser som driftsavbrudd, sikkerhetsbrudd og andre avvik. Derfor må det finnes metoder for varsling, analyse/mobilisering, sikring/respondering, gjenoppretting og normalisering innen samtlige dimensjoner av tjenesteleveransen.

(6) Personvern:

11) Innen dimensjonene tjenesteleveranse, sikkerhet, beredskap, kontinuitet og hendelseshåndtering vil det behandles persondata av ulik karakter og sensitivitet.
12) Personvern må sørge for beskyttelse av personlig integritet og konfidensialitet. Det må derfor finnes metodikk som ivaretar behandling av personrelatert data i tråd med lov og forventning.

(7) Styringsprinsipper:

13) Se kapitel 4.3, *Styringsprinsipper*, for mer informasjon.

RSB tar utgangspunkt i ovennevnte modell som et bakteppe når man skal vurdere ulike sikkerhets-, beredskaps- og personvern prinsipper i tråd med tjenestens kritikalitet.

4.7.2 Sikkerhets-, beredskaps-, og personvernprinsipper

Når kritikalitetsvurdering av tjenesten er foretatt vil det gi en indikasjon på hvor kritisk tjenesten er. Tjenestekritikaliteten sett opp mot en kost-, kvalitets-, og risikoanalyse vil gi en retning på hvilke sikkerhets-, beredskaps-, og personvern prinsipper bør implementeres.

Når det gjelder personvernprinsippene er disse direkte lovhjemlet gjennom personvernlovgivningen. Lovgivningen gir også anvisning på hva som ligger i de ulike personvern prinsippene og hvordan de skal forstås.

Når det gjelder sikkerhets-, beredskaps-, og kontinuitetsprinsipper må det i stor grad søkes i faglitraturen, standarder, og ulik lovgivning.

Ved utvikling, forvaltning, og bruk skal det være helhetlig tilnærming til både personvern (brukersiden/registrerte), sikkerhet (redusere risikoen for hendelser), og beredskap (evne til å gjenopprette eller alternativ oppgave gjennomføring). RSB skal bidra til at kommunale virksomheter og Akson journal AS gjennom implementering av prinsippene kan ha gjensidig tillit til at behandling av helse- og personopplysninger gjennomføres på en forsvarlig og trygg måte.

Noen av sikkerhets-, beredskaps, og personvern prinsippene vil kun gjelde for konsument, andre for tjenesteyter, og atter andre for begge. Selv om et prinsipp gjelder for begge, betyr ikke det at begge skal oppfylle det i samme grad eller på samme måte. Det kan hende at konsumenten skal kun gi input til tjenesteyter og visa versa. Eller at konsumenten skal se prinsippet i forhold til sin funksjonsevne, mens tjenesteyter skal se prinsippet i forhold til sikring av den digitale plattformen. Hvilken styrke prinsippene skal implementeres med vil avhenge av kost-, kvalitets-, og risikovurderingene sett opp mot kritikalitet for tjenesten.

Nedenfor gjennomgås de ulike sikkerhets-, beredskaps-, og personvern prinsippene på et overordnet nivå.

7.5.2.1 Personvernprinsipper

EUs personvernforordning artikkel fem oppstiller personvernprinsipper. All behandling av persondata må skje i samsvar med disse. Prinsippene er basert på tanken om at behandling av persondata skal skje på en måte som i størst mulig grad sikrer forutsigbarhet og forholdsmessighet for enkeltpersoner. For ytterligere informasjon henvises det til personvernforordningen.

Som tidligere nevnt er dataeierskapet i Akson er kompleks og det bør nedsettes en egen arbeidsgruppe som bør se på problematikken rundt behandlingsansvaret. På det stadiet som prosjektet er i nå, vil personvernprinsippene både gjelder for Aksjon journal AS og kommunene. Nedenfor gjennomgås personvernprinsippene, og de må leses med dette som bakteppe.

Lovlighet, rettferdighet og åpenhet: Prinsippet om lovlighet innebærer at behandlingen av personopplysninger må ha et rettslig grunnlag etter EUs personvernforordningen eller eventuelt særlovgivningen. Prinsippet om rettferdig behandling innebærer bl.a. at den registrerte ikke må forskjellsbehandles. Prinsippet om at behandlingen skal være åpen, betyr at den skal være oversiktlig og forutsigbar for den registrerte, slik at vedkommende er i stand til å ivareta sine egne interesser og rettigheter. I åpenhet ligger det også at det må være enkelt for den registrerte å ta kontakt for å få mer informasjon om løsningen, dette skal bidra til tillit og at den registrerte lettere kan ivareta sine rettigheter.

Formålsbegrensning: I formålsbegrensning ligger at persondata bare kan behandles for spesifikke, uttrykkelig angitte og berettigede formål.

Dataminimering: Prinsippet om dataminimering henger tett sammen med formålsbegrensningsprinsippet. I dette ligger at den dataansvarlige skal begrense mengden av persondata til det som er relevant og nødvendig for å oppnå det konkrete formålet.

Riktighet: Prinsippet om at persondata som behandles skal være korrekte. Det skal treffes ethvert rimelig tiltak for å sikre at persondata som er uriktige med hensyn til formålene de behandles for, uten opphold slettes, eller rettes.

Lagringsbegrensning: Prinsippet om at persondata skal slettes når formålet de ble samlet inn for er oppnådd.

Integritet og konfidensialitet: Prinsippet om integritet betyr at persondata som behandles må være korrekte, gyldige, fullstendige, og sikres mot utilsiktet eller uautorisert endring eller sletting. Prinsippet om konfidensialitet handler om å sikre at persondata bare er tilgjengelige for de som rettmessig skal ha tilgang til dem.

Ansvarlighet: Prinsippet om ansvarlighet understreker at den dataansvarlige er den ansvarlige for at behandlingen oppfyller personvernprinsippene, og at den registrertes rettigheter og friheter blir ivaretatt.

Ivaretakelse av den registrertes rettigheter: EUs personvernforordning kapittel III oppstiller de rettigheter den registrerte har etter personvernregelverket når persondata samles inn og behandles om enkeltpersoner. Den registrertes rettigheter står sentralt i forordningen, og en av hovedbegrunnelsene for reguleringen er å sikre at den enkelte får bedre kontroll med behandlingen av persondata om seg selv.

7.5.2.2 Sikkerhets- og beredskapsprinsipper

Nedenfor gjennomgås sikkerhets- og beredskapsprinsippene. Noen av sikkerhets- og beredskapsbegrepene vil kun gjelde for konsument, andre for tjenesteyter og atter andre for begge.

7.5.2.2.1 Overordnede sikkerhets- og beredskapsprinsipper

Tjenestemobilitet (gjelder tjenesteyter): Handler om tjenesten lett kan flyttes fra en leverandør til en annen, eller fra en plattform til en annen. Mobilitet for tjenesten bør vurderes.

F.A.F.B (gjelder tjenesteyter og konsument): Forenkling, automatisering, forbedring, og en god brukeropplevelse. Innebærer at man må ha søkelys på forenkling, automatisering, forbedring, og brukeropplevelse og at tjenesten har et positivt utfall for konsument. F.A.F.B for tjenesten bør vurderes.

Proaktivitet: (gjelder tjenesteyter og konsument): Innebærer å prøve å forutse begivenheter eller problemer, snarere enn bare å reagere når de er oppstått. Begrunnelsen for dette er at kostnaden ved å handle reaktivt er lagt høyere enn å handle proaktiv. Proaktivitet for tjenesten bør vurderes.

7.5.2.2.2 Prosessuelle sikkerhets- og beredskapsprinsipper

Passiv sikkerhet (gjelder tjenesteyter og konsument): Med passiv sikkerhet menes innretninger som hjelper bruker uten nevneverdig innvirkning/interaksjon fra bruker. Passiv sikkerhet kan best forklares med å sammenligne bilens utvikling innen passiv sikkerhet så som radarsystemer, anti-skrens, airbag med videre. Det betyr at naturlige menneskelig adferd skal legges til grunn og hjelpe brukeren til å gjennomføre oppgaven på en trygg måte. Passive sikkerhetsmekanismer bør bygges inn slik at brukeren trygt kan gjennomføre ulike oppgaver uten å bli kompromittert i sin arbeidsutførelse.

Fail safe prinsippet (gjelder tjenesteyter og konsument): Fail safe er en egenskap som gjør at systemet ved feil går til en sikker tilstand. Det vil si at ingen sikkerhetskritisk situasjon skal oppstå som følge av feil i systemet. Det

betyr ikke at et system som er Fail safe ikke kan svikte, men snarere at systemets design forhindrer eller demper utrygge konsekvenser av systemets feil. Det vil si at hvis et fail system feiler, forblir det minst like trygt som det var før feilen. Fail safe prinsippet bør legges til grunn for tjenesten.

Self healing prinsippet (gjelder tjenesteyter og konsument): Self healing prinsippet går ut på at et system har en innebygd evne til å oppdage og rette feil uten å ha hjelp utenfra. For eksempel at et nettverket skal kunne diagnostisere og ordne nettverksproblemene automatisk. Self healing prinsippet bør legges til grunn for tjenesten.

Sikker utviklingssyklus (gjelder tjenesteyter) og anskaffelse (gjelder tjenesteyter og konsument): Det finnes ulike rammeverk for sikker utviklingssyklus, for eksempel Microsoft Security Development Lifecycle (SDL). For å ha en sikker og agil leveransemodell bør DevSecOps prinsipper legges til grunn. SDL eller tilsvarende rammeverk vil være en delmengde av DevSecOps. Sikkerutviklingssyklus varer gjennom hele livssyklusen til produktet. Datatilsynets veileder for programvareutvikling med innebygd personvern legges til grunn[13]. Ved anskaffelse legges hele livssyklusen til systemet til grunn. Brukerinvolvering og interaksjonsdesign bør være sentrale elementer i DevSecOps.

Agilt og skalerbarhet (gjelder tjenesteyter og konsument): Funksjonene i tjenesten bør være skalerbare og agile for hele livsløpet. Dette for å legge til rette for innovasjon og evolusjon.

Dynamisk risikostyring (gjelder tjenesteyter og konsument): På de mest kritiske funksjonene bør det gjøres dynamisk (kontinuerlig) risiko- og sårbarhetsvurdering slik at man evner å levere tjenestene selv under uønsket påvirkning, eller redusere risikoen for bortfall av tjenestene uavhengig om handlingen er tilsiktet eller utilsiktet.

Enkelhetsprinsippet (gjelder tjenesteyter og konsument): Systemet bør baseres seg på enkelthetsprinsippet. Det gjelder både i forhold til brukerinteraksjon og ved oppbygning av løsningen. Løsningsdesign bør være transparent og enkel slik at feilkilder kan oppdages raskt og nye funksjoner kan implementer «on the fly», uten at dette går utover løsningens leveranseevne. I enkelhetsprinsippet ligger også at konsumenten skal være i stand til å konsumere løsningen.

Avhending (gjelder tjenesteyter og konsument): Avhending må gjennomføres på en slik måte at det ikke kommer i konflikt med lov eller de andre sikkerhetsprinsippene.

Åpenhet og åpne standarder (gjelder tjenesteyter): Sårbarheten ved å utvikle selv kontra bruk «off the shell produkter», åpne APIer og tekniske standarder må vurderes. Om det finnes åpne APIer, tekniske standarder som er anerkjent, eller «off the shell produkter» bør disse benyttes.

Transparent og ansvarlighet (gjelder tjenesteyter og konsument): Tjenesten bør være transparent slik at man har oversikt over hele tjenesteleveransen (og verdikjeden) med dets sårbarheter og enkelt feil (singel point of failure). Ansvarsforholdene for tjenesten mellom partene bør være avklart og konsensus om dette bør være oppnådd.

7.5.2.2.3 Teknologiske sikkerhets- og beredskapsprinsipper

Tilgangsstyring (gjelder tjenesteyter og konsument): En zero-trust-tilnærming bør ligge til grunn for autentisering og autorisering samt prinsippet om tjenstlig tilgang. Det vil si at tilgang kun skal gis ved tjenstlig behov og kun til personell og digitale enheter som er autentisert og autorisert. Dette gjelder alle moduler og komponenter i løsningen(e). Samtidig må ikke løsning kompliseres unødvendig. En kost/kvalitetsanalyse munnet ut i risikoaksept vil gi en indikasjon på nivået på fullstendig tillitsprinsippet i en ytterkant, kontra zero-trust tilnærming i andre ytterkant.

[13] https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/innebygd-personvern/programvareutvikling-med-innebygd-personvern/

Seperasjon av data og applikasjon (gjelder tjenesteyter): Fleksibilitet, skalerbarhet, innovasjon og næringsutvikling bør legges til grunn for tjenesten. Data skal derfor være adskilt og være tilgjengelige gjennom APIer. Dette for å understøtte utvikling av tilleggsfunksjonalitet og integrasjon med andre løsninger, herunder endring av organisasjonsstrukturer, prosesser og applikasjoner, f.eks. bruk av maskin læring og på sikt kunstig intelligens (KI).

Kommunikasjonssikkerhet (gjelder tjenesteyter): All data krypteres ved overføring i henhold til kritikalitet og nasjonale anbefalinger. All informasjon som kommer fra en part utenfor løsningen(e) bør signeres slik at avsender kan verifiseres. Det bør vurderes kryptering på data som er i bero.

Sporbarhet, preventive, detekterende og korrigerende mekanismer samt kontinuerlig sikkerhetstesting (gjelder tjenesteyter og konsument): Det vil alltid være sårbarheter i tjenesteleveranse og det må tas høyde for at sikkerhetsmekanismer svikter. Det bør finnes mekanismer for å oppdage og hvordan man skal reagere for å gjenopprette normal situasjon og minimere skadeomfang. Komponenter som håndterer kritiske/sensitiv informasjon bør i størst mulig grad beskytte seg selv, og ha minst mulig tillit til omkringliggende komponenter. Det bør gjennomføres kontinuerlige sikkerhetstester av kritiske systemer. Dette både i forhold til gjennomgang av kode, inntrengningstesting, og sårbarhetsskanning.

Seperasjon av kritiske komponenter (gjelder tjenesteyter og konsument): Komponenter som inneholder sikkerhetsfunksjoner/behandler kritisk/sensitiv funksjoner (informasjon) bør separeres i størst mulig grad fra komponenter som utfører andre funksjoner. Dette for å hindre at sikkerhetskomponentene ikke blir påvirket av feil eller sikkerhetsbrudd i de andre komponentene. Separasjon bør praktiserer på alle lag. Diversitet bør praktiseres så langt det lar seg gjøre.

Minst mulig privilegium (gjelder tjenesteyter og konsument): Funksjonene bør har mist mulig privilegium (rettigheter) for å utføre sin funksjon.

Lagdelt sikkerhetsarkitektur og sikring i dybden (gjelder tjenesteyter og konsument): En utfordring med operasjonelle kontroller kan være at de ikke nødvendigvis hindrer feil fra å skje. Sikringstiltak kan gjøre at feil sjeldnere oppstår, eller gjøre det mulig å oppdage de innen rimelig tid i etterkant, men kan ikke garantere tilstrekkelig sikring. Det bør derfor implementeres flere lag av sikkerhet og derav ha tilstrekkelig sikring og oppdagelsesmulighet i dybden hvor diversitet bør være et av flere målparametere.

Tjenesteplattform (gjelder tjenesteyter): Innebærer at tjenesteplattformen må ha nødvendig robusthet i forhold til tjenestekritikalitet med hensyn til flyttbarhet, redundans, skalerbarhet, reverserbarhet, modulærbarhet og stabilitet i tråd med prinsippene om kost, kvalitet og risiko.

Sikker kode (gjelder tjenesteyter): Kildekode, og spesielt åpen kildekode, eller logikk bør testes og sikres gjennom automatiske og manuelle kilde- og logikkrevisjoner, og sårbarhetstester.

7.5.2.2.4 Personrelaterte og organisatoriske sikkerhets- og beredskapsprinsipper

High Reliability Organization (HRO) (gjelder tjenesteyter og konsument): HRO-teorien tar utgangspunkt i at verden er kompleks, ustabil, ukjent og uforutsigbar. Kjernen i teorien er årvåkenhet som gjør det mulig å se betydningen av svake signaler og respondere enhetlig på disse. Utgangspunktet er å håndtere det uventede ved årvåkenhet og oppdage problemer mens de er under utvikling. Om en hendelse ikke kan stanses, bør den demmes opp. Hvis problemet klarer å bryte igjennom oppdemning, må det være robusthet i systemet som gjør det mulig å hurtig reetablere systemfunksjonalitet. HRO-systemer er ikke feilfrie, men samtidig fører ikke feil til at organisasjonen eller funksjonene bryter sammen. Poenget med å benytte HRO er tjenesteyter og konsument utvikler en god evne til å kontrollere komplekse teknologier uten å forårsake individuelle eller organisatoriske ulykker. HRO prinsippet bør legges til grunn for tjenesten.

Kontinuitet (gjelder tjenesteyter og konsument): Det bør etableres en strukturert tilnærming til kontinuitet og gjenoppretting. Virksomhetskontinuitet skal ivareta at de kritiske virksomhetsprosessene vil fortsette innenfor akseptable nivåer når uønskede hendelser inntreffer. Virksomhetskontinuitet omfatter virksomhet som helhet, det vil si også de tilknyttede kommunene i tillegg til Akson Journal AS.

Beredskaps- og drift (gjelder tjenesteyter og konsument): Beredskap og drift skal basere i tråd med nasjonale prinsipper om ansvar, likhet, nærhet og samvirke. Virksomheten bør dimensjonere beredskap i tråd med tjenestekritikalitet og kost-, kvalitets-, og risikovurdering.

Opplæring av personell innen sikkerhet, beredskap og personvern (gjelder tjenesteyter og konsument): Personell bør gis tilstrekkelig opplæring i løsningen(e) og tjenesteleveransen slik at hver enkelt kan ivareta sitt ansvar for sikkerhet, beredskap og personvern. Personell bør også gis opplæring innen kontra psykologiske virkemidler, herunder typiske virkemidler innen sosial manipulering. Årlig sertifiseringsordning for bruk av systemet bør innføres.

Kontrollbarhet personell (gjelder tjenesteyter og konsument): Det må gjennomføres egnet bakgrunnssjekk av personell som skal ha tilgang til kritiske komponenter eller kritiske deler av tjenesten. For annet personell bør det gjennomføres en risikovurdering.

Varslingssystem (gjelder tjenesteyter og konsument): Det bør finnes varsling og koordineringssystem i forhold til leverandører, konsumenter og andre aktuelle entiteter for å minimere kaskadevirkningene minst mulig og for å kunne håndtere en «situasjonen» raskest mulig.

Øvelser (gjelder tjenesteyter og konsument): Det bør gjennomføres øvelser både i forhold til kontinuitets-, sikkerhets- og beredskapsstyring.

Seperasjon av ansvar (gjelder tjenesteyter og konsument): Seperasjon av ansvar bør være avklart i forhold til tjenestens kritikalitet.

Dokumentasjon og tilgang (gjelder tjenesteyter og konsument): Kritisk tjenestedokumentasjon bør være oppdatert og befinne seg på et område som lar seg aksessere når alt feiler.

Leverandør og leveranser (gjelder tjenesteyter og konsument): Anskaffelsene bør støtte oppunder tjenestekritikalitet. Prinsippet om innovative anskaffelser bør vurderes.

Nasjonale krav (gjelder tjenesteyter og konsument): Tjenesten må oppfylle avtalemessige, lovmessige, eller nasjonale krav til sikkerhet, beredskap og personvern.

Organisasjonens modenhet (gjelder tjenesteyter og konsument): Organisasjonen (både tjenesteyter og konsument) bør legge til rette for systematisk forståelse av tjenestekritikalitet, tjenesteleveranser, og øvelser som muliggjør en god tjenesteleveranse i tråd med sikkerhets-, beredskap, og personvernprinsippene.

Revisjonsbarhet (gjelder tjenesteyter og konsument): Tjenesten bør enkelt kunne underkastes revisjon. Det bør legges til rette for eksterne revisjoner for å skape økt tillitt til systemet. Revisjoner bør gjøres på innenfor personvern, sikkerhet, beredskap, kontinuitet, og hendelseshåndtering. Automatiske revisjoner bør vurderes.

7.6 Oppsummering RSB

Kjernen i RSB er at den skal være pragmatisk og ha en helhetlig tilnærming til å finne tjenestekritikalitet for tjenestene. Tjenestekritikaliteten er avgjørende for å kunne dimensjonere rett og tilstrekkelig sikkerhets- og beredskapsevne for å levere og konsumere trygge og sikre tjenester. Og i en forlengelse av dette, hvilke sikkerhets-, beredskaps-, og personvernprinsipper som bør legges til grunn for å oppnå tilstrekkelig sikkerhets- og beredskapsevne i tråd med tjenestekritikaliteten.

For å finne tjenestekritikalitet, og hvilke sikkerhets, beredskaps, og personvernprinsippene som skal implementeres, baserer RSB seg på fire grunnprinsipper og fire styringsprinsipper. Disse gir en veiledning på hvilke hensyn som bør vektlegges når man skal finnes tjenestekritikalitet og hvilke sikkerhets-, beredskaps og personvern prinsipper som bør implementeres.

RSB kan anses som en veiledning/kravsett på hvordan man kan oppnå en sikkerhets- og beredskapsevne for å levere og konsumere trygge og sikre digitale tjenester. RSB handler ikke om sikkerhetsstyring på virksomhets- eller på operativnivå, men vil være styrede for dimensjonering av sikkerhetsstyring, operativ sikkerhet, og teknisk sikkerhetsarkitektur.

Det finnes allerede gode ulike rammeverk som gir god veiledning sikkerhetsstyring på virksomhetsnivå og teknisk sikkerhetsarkitektur som kan benyttes. Som eksempler her kan nevnes Norm for informasjonssikkerhet og personvern i helse- og omsorgstjenesten (Normen), ISO27001 (ISO27002) med flere, NIST Cyber Security Framework, CIS Center for Internett Security (CIS) kontroller, Nasjonal sikkerhetsmyndighets grunnprinsipper, og Nasjonal sikkerhetsmyndighets rammeverk for håndtering av IKT-hendelser, og SABSA (Sherwood Applied Business Security Architecture) for å nevne noen.

7.7 Konsekvenser for Akson

Slik RSB er designet vil det gjøre kommunal sektor bedre rustet til å vurdere tjenestekritikalitet og oppnå nødvendig sikkerhets- og beredskapsevne for å kunne konsumenere digitale tjenester levert av Akson journal AS (og NHN) på trygg og sikker måte.

RSB er kost, kvalitet, og risikobasert slik at i hvilken styrke den enkelte personvern, sikkerhets- og beredskapsprinsipp skal implementeres i vil avhenge av tjenestekritikalitet og tjenestetype. RSB vil gi en felles plattform for å skape nødvendig tillit mellom Akson Journal AS og kommunal sektor for behandling av dataene i Aksons økosystem. En felles plattform og tillitt er helt nødvendig for å legges til rette for innovasjon, kontinuerlig utvikling, og prosessendringer i en verden som endrer seg raskt i forhold til teknologi, økonomi og arbeidsprosesser.

Slik RSB er designet, vil ikke dette medføre noen ekstra kostnader eller dreining av prosjektet i forhold til den planlagte leveransen. Tvert imot vil RSB gjøre leveransen fra Akson Journal AS mer robust, og legge til rette for innovasjon, forenkling, og forbedring.