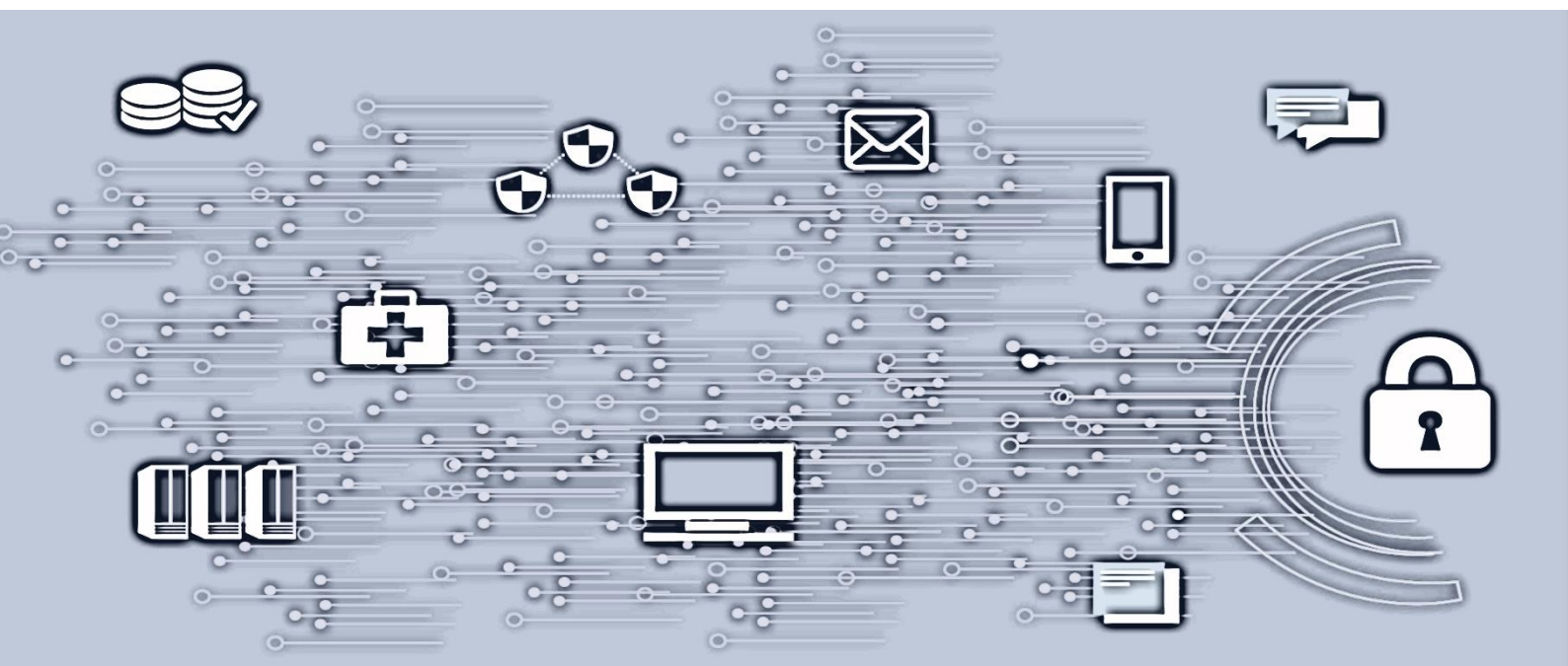


Regional sikkerhetspolicy for skytjenester



Innhold

1	Introduksjon.....	4
2	Formål og scope	4
2.1	Målgruppe	4
2.2	Virkeområde.....	4
2.3	Avhengigheter og forutsetninger.....	4
3	Kilder	4
3.1	Lovverk og styrende dokumentasjon.....	4
3.2	Rammeverk og standarder.....	5
3.3	Interne og eksterne strategier.....	5
4	Forkortelser og begreper.....	5
5	SABSA rammeverk for sikkerhetsarkitektur	7
5.1	SABSA for skytjenester.....	8
6	Kontekstuell arkitektur	9
6.1	Forretningsbehov.....	9
6.2	Drivere for sikkerhet	11
7	Konseptuell sikkerhetsarkitektur.....	11
7.1	Sikkerhetsledelse og ansvar	12
7.1.1	Ansvarsfordeling for sikkerhetstiltak.....	13
7.1.2	Intern forvaltning og kompetanse	14
7.2	Leverandørhåndtering.....	14
7.2.1	Risikovurdering av leverandører	14
7.2.2	Avtaler og kontrakter	15
7.2.3	Tjenesteleveranseavtaler (SLA)	15
7.2.4	Databehandleravtaler og behandling av virksomhetssensitive opplysninger.....	15
7.3	Risikostyring/risikovurdering	16
7.4	Personvern.....	16
7.4.1	Innebygd personvern	16
7.4.2	Personvernkonsekvensvurdering	16
7.4.3	Behandlingens lokasjon	17
7.4.4	Segmentering av data	17
7.5	Revisjon.....	17
7.6	Klassifisering av informasjon.....	18
7.7	Tilgangsstyring (IAM)	18
7.7.1	Autorisering og autentisering.....	18
7.7.2	Separation of duties.....	19
7.7.3	Administrative/privilegerte tilganger.....	19
7.7.4	Kontroll av tilganger	19
7.8	Fysisk sikkerhet/adgangskontroll.....	19
7.9	Monitorering, logging og deteksjon	20
7.10	Hendeshåndtering og etterforskning.....	20
7.11	Trussel- og sårbarhetshåndtering	20
7.12	Endringshåndtering.....	21
7.13	Business Continuity, tilgjengelighet og oppetid	21
7.14	Datasikkerhet og -livssyklusshåndtering	22
7.15	Kryptering og nøkkelhåndtering	23
7.16	Mobilsikkerhet.....	23

7.17	Human Resource-sikkerhet	23
7.18	Infrastruktur og virtualisering	24
7.19	Applikasjonssikkerhet	24
7.20	Interoperabilitet og portabilitet.....	25

Versjon	Dato	Godkjent av
1.0	02.10.2020	Christian Jacobsen
1.01	08.04.2021	Christian Jacobsen
1.02	21.05.2021	Christian Jacobsen
1.1	14.02.2022	Christian Jacobsen

1 Introduksjon

Bruk av skytjenester skal kunne gi tilstrekkelig tilgjengelighet, god kvalitet og sikkerhet i driftstjenester samtidig som det effektivt understøtter helseforetakenes behov. En sikkerhetsarkitektur for skytjenester er en forutsetning for at dette skal kunne oppfylles.

Denne sikkerhetsarkitekturen har vi valgt å kalle «Grunnmur for skytjenester». Dokumentene som utgjør «Grunnmur for skytjenester» ligger i det regionale ISMS. Det er et sett med basiskapabiliteter som beskriver informasjonssikkerhet og personvernstiltak for hvordan skytjenester tas i bruk, inkludert bla. tilgangsstyring, risikostyring, leverandørhåndtering, sikkerhetskrav, personvern og endring- og hendeshåndtering.

Grunnmur for skytjenester skal understøtte tjenester som etableres i skyen uansett tjeneste- og leveransemodell.

2 Formål og scope

Formålet med regional sikkerhetspolicy for skytjenester er å sammenfatte og befeste de styrende forhold som gjør seg gjeldende for Helse Sør-Øst sin bruk av skytjenester. Hensikten er å ivareta informasjonssikkerhets- og personvernmessige forhold ved bruk av skytjenester uavhengig av hvilken type data som behandles.

Dokumentet beskriver krav til fellestjenester i skyen i tillegg til et sett med basistjenester.

2.1 Målgruppe

Regional sikkerhetspolicy for skytjenester skal vise «de store linjene» – altså en oversiktlig fremstilling av hvilke områder som skal hensyntas når et program, prosjekt eller foretak ønsker å ta i bruk skytjenester.

Dokumentet er hovedsakelig ment å treffe ledere og prosjektledere som oftest sitter med beslutningsmyndighet og må forholde seg til prinsipielle eller strategiske valg i sitt virke.

Dokumentet må likevel leses i sammenheng med NO-30 Regionale sikkerhetsprinsipper og –krav for skytjenester (RSPS), som detaljerer og tydeliggjør krav som utledes fra dette dokumentet.

2.2 Virkeområde

Dokumentet gjelder for de leveranser eller tjenester som på en eller annen måte omfatter bruk av skytjenester i Helse Sør-Øst.

2.3 Avhengigheter og forutsetninger

I de tilfeller dette dokumentet påpeker manglende styrende dokumentasjon i regionen, må dette utarbeides for å dekke de mangler som fremkommer.

3 Kilder

3.1 Lovverk og styrende dokumentasjon

Hovedkildene til krav for informasjonssikkerhet i skytjenester hentes fra (ikke uttømmende):

- [Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren](#) v.6
- [NSM – Grunnprinsipper for IKT sikkerhet v.2](#)

- [Arkivlova¹](#)
- [Bokføringsloven](#)
- [Personopplysningsloven](#) og [personvernforordningen \(GDPR\)](#)
- [Pasientjournalloven](#), [Helseregisterloven](#) og [Helsepersonelloven](#)

3.2 Rammeverk og standarder

Hovedkilde til rammeverk som benyttes for HSØ hentes fra:

- [SABSA – Sikkerhetsarkitektur rammeverk](#)
- [Cloud Security Alliance – kontrollrammeverk for skytjenester](#)
- [Security Guidance for Critical Areas of Focus in Cloud Computing v4.0](#)
- [CSA – Cloud Control Matrix](#) (ivaretar delvis ISO27001/ISO27018)

3.3 Interne og eksterne strategier

Kilder til forretningsbehov:

- [Nasjonal strategi for bruk av skytjenester](#)
- [Informasjonssikkerhet ved bruk av private leverandører i helse- og omsorgstjenesten](#)
- [Veileder i bruk av skytjenester til behandling av helse- og personopplysninger](#)
- [Målarkitektur for IAM](#) (internt dokument)
- Tilnærming for bruk av skytjenester (internt dokument)

4 Forkortelser og begreper

Forkortelse/ begrep	Fullt navn/forklaring
ASR	Arkitektur i program og prosjekter
AWS	Amazon Web Services
CAIQ	Consensus Assessment Initiative Questionnaire
CASB	Cloud Access Security Broker
CCM	Cloud Control Matrix
Community cloud	Skytjenester for fellesskap av virksomheter
CSA	Cloud Security Alliance
DBA	Databehandleravtale
DevOps	Software Development and Information Technology Operations
DLP	Data Loss Prevention
eIDAS	Electronic Identification, Authentication and Trust Services. EU regulativ om elektronisk ID.
EMM	Enterprise Mobility Management
GCP	Google Cloud Platform
GDPR	General Data Protection Regulation (personvernforordningen)
HF	Helseforetakene under Helse Sør-Øst inkludert Sykehuspartner

¹ [NOU 2019:9](#) legger grunnlag for ny arkivlov. Dette skal tas hensyn til i dette dokumentet når ny arkivlov foreligger.

Helseforetakene i regionen	Her menes alle HF, inkludert Sykehuspartner HF og Helse Sør-Øst RHF.
HSØ	Helse Sør-Øst RHF
Hybrid cloud	Kombinasjon av private og public cloud. Både eksklusive og delte skytjenester
IaaS	Infrastructure-as-a-Service
IAM	Identity and Access Management
ISMS	Information Security Management System
Leveransemodell sky	Typen leveranse av sky: private/public/hybrid/community cloud
LG1	Ledermøtet SPHF
MA	Microsoft Azure
MAM	Mobile Application Management
MDM	Mobile Device Management
MFA	Multi Factor Authentication
NDA	Non-Disclosure Agreement
NKOM	Nasjonal kommunikasjonsmyndighet
NSM	Nasjonal Sikkerhetsmyndighet
PaaS	Platform-as-a-Service
PKV	Personvernkonsekvensvurdering (DPIA)
Private cloud	Skytjenester tilbudt eksklusivt for en (isolert) virksomhet
Public cloud	Skytjenester som deles mellom flere virksomheter
RPO	Recovery Point Objective – Største akseptable datatap målt i tid, gir rammer for hvor ofte back-up skal tas.
RTO	Recovery Time Objective – Lengste akseptable nedetid i strekk, setter ambisjonsnivå for hvor fort tjenesten skal kunne gjenopprettes ved en feilsituasjon eller hendelse.
RSR	Regionalt Sikkerhetsfaglig Råd
RSS	Regional Sikkerhetspolicy for Skytjenester
RSPS	Regionale Sikkerhetsprinsipper for Skytjenester
RSV	Regionalt Sikkerhetsvurderings team
SaaS	Software-as-a-Service
SABSA	Sherwood Applied Business Security Architecture
SECaaS	Security-as-a-Service
SLA	Service Level Agreement
Skyleverandør	En skyleverandør tilbyr skybasert plattform, infrastruktur, program eller lagringstjenester
Skytjeneste	Skytjenester er en samlebetegnelse for leveransemodeller som muliggjør tilgjengelige, tilpassede, «on-demand», tilgang til en pool med delte ressurser som kan skaleres opp eller ned (både for kunde og leverandør). Infrastrukturen som leverer skytjenesten kan være tilgjengelig både i egen infrastruktur, og via eksterne nettverk (utenfor virksomhetens infrastruktur).
SPARK	Sykehuspartner Arkitekturråd
SPHF	Sykehuspartner HF
TCO	Total Cost of Ownership

Tjenestemodell sky	Typen skytjeneste: IaaS, PaaS, SaaS
TOGAF	Arkitektur-rammeverk

5 SABSA rammeverk for sikkerhetsarkitektur

HSØ benytter TOGAF som rammeverk for arkitektur. I TOGAF håndteres sikkerhet og risiko gjennom krav til interessenter, og det kan derfor være nyttig med ytterligere detaljering og et eget rammeverk for sikkerhetsarkitektur. Beslutningen om å ta i bruk SABSA Sikkerhetsarkitektur som et tillegg til TOGAF ble tatt 14/11/2019 i LG1. Dokumentene som foreløpig utgjør en sikkerhetsarkitektur for skytjenester omtales som «Grunnmur for skytjenester» og oppbyggingen er basert på rammeverket [SABSA](#).

SABSA supplerer med en forretnings- og risikobasert sikkerhetsarkitektur som en del av den overordnede virksomhetsarkitekturen. En SABSA-basert sikkerhetsarkitektur skal understøtte forretningen, noe som er i tråd med grunnprinsippene i TOGAF. SABSA kan dermed brukes som rammeverk for en sikkerhetsarkitektur uten at dette går på bekostning av en TOGAF-basert virksomhetsarkitektur.

SABSA rammeverket har en metode for å utvikle risikodrevne informasjonssikkerhets- og informasjonssikringsarkitekturer for virksomheter og for å levere løsninger som støtter viktige forretningsinitiativer. SABSA er gratis å bruke for alle, uten krav til lisensiering for sluttbrukerorganisasjoner. SABSA anvendes til å utvikle og implementere arkitekturer og løsninger.

SABSA-modellen består av seks lag som vist i tabellen nedenfor (Figur 1). Hvert lag representerer et perspektiv sett fra en aktør i prosessen med å spesifisere, designe, konstruere og bruke målarkitekturen.

Det er seks horisontale lag av abstraksjon i arkitekturmodellen (kontekstuell, konseptuell, logisk, fysisk, komponent og serviceadministrasjon). For hvert av de horisontale lagene svares det på spørsmålene hva, hvorfor, hvordan, hvem, hvor og når gjennom seks vertikale elementer. Dette gir en matrise på 6x6 som representerer hele modellen for sikkerhetsarkitektur (Figur 1). Det nederste laget, Service Management Architecture, må tolkes i detalj på alle de andre lagene. Dette laget får dermed også en tverrgående vertikal dimensjon.

	ASSETS (What)	MOTIVATION (Why)	PROCESS (How)	PEOPLE (Who)	LOCATION (Where)	TIME (When)
CONTEXTUAL ARCHITECTURE	Business Decisions	Business Risk	Business Processes	Business Governance	Business Geography	Business Time Dependence
	Taxonomy of Business Assets, including Goals & Objectives	Opportunities & Threats Inventory	Inventory of Operational Processes	Organisational Structure & the Extended Enterprise	Inventory of Buildings, Sites, Territories, Jurisdictions, etc.	Time dependencies of business objectives
CONCEPTUAL ARCHITECTURE	Business Knowledge & Risk Strategy	Risk Management Objectives	Strategies for Process Assurance	Roles & Responsibilities	Domain Framework	Time Management Framework
	Business Attributes Profile	Enablement & Control Objectives; Policy Architecture	Process Mapping Framework; Architectural Strategies for ICT	Owners, Custodians and Users; Service Providers & Customers	Security Domain Concepts & Framework	Through-Life Risk Management Framework
LOGICAL ARCHITECTURE	Information Assets	Risk Management Policies	Process Maps & Services	Entity & Trust Framework	Domain Maps	Calendar & Timetable
	Inventory of Information Assets	Domain Policies	Information Flows; Functional Transformations; Service Oriented Architecture	Entity Schema; Trust Models; Privilege Profiles	Domain Definitions; Inter-domain associations & interactions	Start Times, Lifetimes & Deadlines
PHYSICAL ARCHITECTURE	Data Assets	Risk Management Practices	Process Mechanisms	Human Interface	ICT Infrastructure	Processing Schedule
	Data Dictionary & Data Inventory	Risk Management Rules & Procedures	Applications; Middleware; Systems; Security Mechanisms	User Interface to ICT Systems; Access Control Systems	Host Platforms, Layout & Networks	Timing & Sequencing of Processes and Sessions
COMPONENT ARCHITECTURE	ICT Components	Risk Management Tools & Standards	Process Tools & Standards	Personnel Man'ment Tools & Standards	Locator Tools & Standards	Step Timing & Sequencing Tools
	ICT Products, including Data Repositories and Processors	Risk Analysis Tools; Risk Registers; Risk Monitoring and Reporting Tools	Tools and Protocols for Process Delivery	Identities; Job Descriptions; Roles; Functions; Actions & Access Control Lists	Nodes, Addresses and other Locators	Time Schedules; Clocks, Timers & Interrupts
SERVICE MANAGEMENT ARCHITECTURE	Service Delivery Management	Operational Risk Management	Process Delivery Management	Personnel Management	Management of Environment	Time & Performance Management
	Assurance of Operational Continuity & Excellence	Risk Assessment; Risk Monitoring & Reporting; Risk Treatment	Management & Support of Systems, Applications & Services	Account Provisioning; User Support Management	Management of Buildings, Sites, Platforms & Networks	Management of Calendar and Timetable

Figur 1 SABSA Matrix

De øverste lagene i sikkerhetsarkitekturen Contextual, Conceptual og delvis Logical som ivaretar overordnede forretningsmål og beskriver drivere for sikkerhet finnes i Regional Sikkerhetspolicy for Skytjenester (RSS).

I Regionale sikkerhetsprinsipper og -krav for skytjenester (RSPS) fokuseres det på det logiske-, fysiske- og komponentlaget i Grunnmur for skytjenester. Dette inkluderer identifisering og spesifisering av logiske elementer og forholdet mellom dem, krav til fysiske elementer som støtter logiske elementer, og krav til spesifikke prosesser og verktøy.

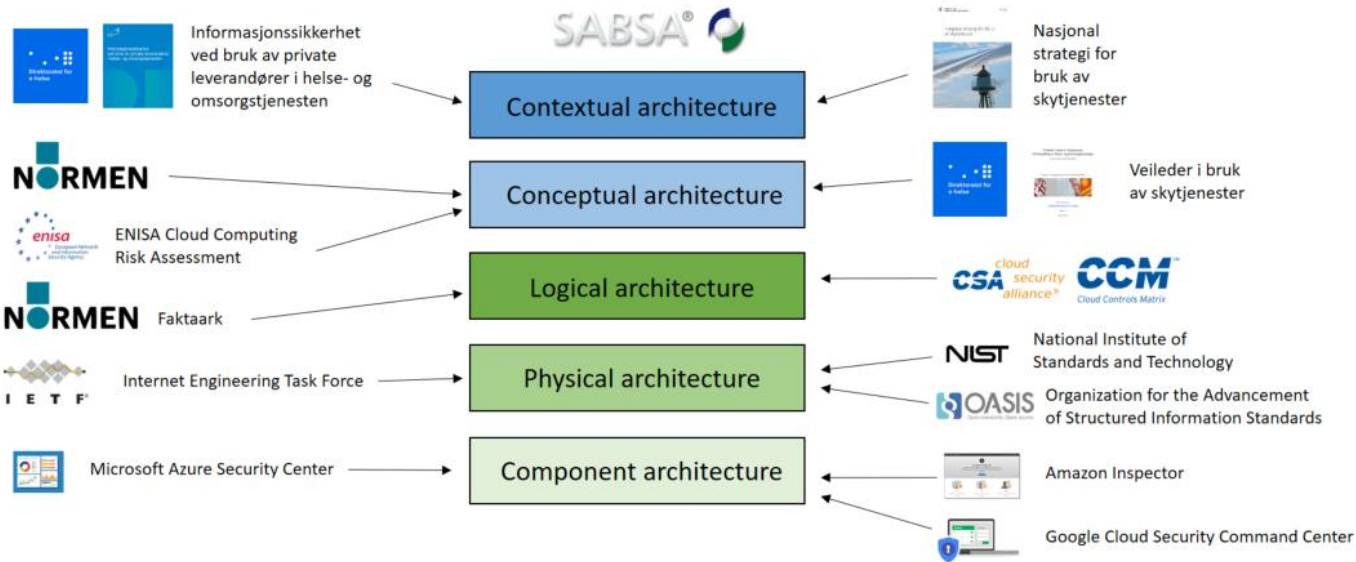
Ved å bruke SABSA får vi en toveis sporbarhet i Grunnmur for skytjenester. I policyen utledes forretningsbehovene ved bruk av skytjenester, som danner grunnlaget for drivere for sikkerhet. Deretter beskrives overordnede mål og behov for informasjonssikkerhet, verdier som må sikres og risikoer knyttet til drift og kjernevirksomhet. Slik kan vi sikre at forretningsbehov møtes ved å gå «nedover» i dokumentene gjennom krav og prinsipper helt til man har en konkret løsning på forretningsbehovene. På samme måte kan man starte med en konkret løsning og spore seg tilbake til krav, prinsipper og overordnede mål, og hva som var forretningsbehovet som drev dette i utgangspunktet.

5.1 SABSA for skytjenester

Som vist i Figur 2² er SABSA et rammeverk som kan binde sammen andre standarder og rammeverk på de ulike nivåene i arkitekturen. Nasjonale kilder til krav for skytjenester, kap. 3, kommer inn som

² Det vises i tegningen til NIST, OASIS, IETF. De har ikke vært brukt i dette dokumentet, men er med som eksempler.

en del av Contextual Architecture, mens internasjonale standarder gjerne benyttes som referanse for sikkerhetsmekanismer i Conceptual Architecture. Sikkerhetstiltak fra skyleverandørene er beskrevet i Component Architecture.



Figur 2 SABSA for skytjenester

6 Kontekstuell arkitektur

Dette kapitlet inneholder overordnede forretningsbehov og målsetninger relatert til bruk av skytjenester. De har som mål å knytte investeringen i sikkerhet og bruk av skytjenester både til eksterne retningslinjer for bruk av sky³ og til SPHF's mål om sikre og stabile tjenester som kan standardiseres, moderniseres, digitaliseres og effektiviseres. De er hentet fra de autorative kildene nevnt i kapittel 3.

6.1 Forretningsbehov

Forretningsbehovene er formulert som funksjonelle krav. De er altså ikke absolutte krav, men overordnede målsetninger.

Drivere for sikkerhet, generelle prinsipper for- og tekniske krav til bruk av skytjenester skal kunne støtte opp under disse forretningsbehovene.

Krav #	Kravbeskrivelse	Kilde
R1	SPHF skal levere skytjenester som er kostnadseffektive å drifte i skyen.	Tilnærming for bruk av skytjenester
R2	Skytjenester skal gi Helse Sør-Øst ekstra kapasitet, fleksibilitet og robusthet	Tilnærming for bruk av skytjenester

³ [Nasjonal strategi for bruk av skytjenester](#)

R3	SPHF skal vurdere å benytte tjenester som gir høyere kvalitet som skytjenester	Nasjonal strategi for bruk av skytjenester
R4	SPHF skal benytte tjenester i skyen som gir brukerne og foretakene i regionen økt sikkerhet	Nasjonal strategi for bruk av skytjenester
R5	SPHF må kunne tilby helseforetakene tjenester som kun er tilgjengelig i skyen (cloud native).	Normen
R6	Skytjenestene skal håndtere eksterne brukere på tilsvarende sikker måte slik tjenestene leveres i eget datasenter.	Normen
R7	Skytjenester skal legge til rette for samhandling. Dette gjelder bl.a. diskusjon, informasjonsdeling og videokonferanser.	Regional Sikkerhetspolicy for skytjenester
R8	Skytjenester skal legge til rette for virtuelle helsetjenester der kommunikasjon med pasient er sentralt.	Nasjonal strategi for bruk av skytjenester
R9	HSØ skal vurdere å benytte skytjenester som understøtter etablering av utviklingskapasitet i skyen basert på virtuelle maskiner eller containerteknologi.	Nasjonal strategi for bruk av skytjenester
R10	SPHF skal utvide testkapasitet ved å etablere testmiljøer i skytjenester.	Nasjonal strategi for bruk av skytjenester
R11	Skytjenester skal legge til rette for analyse og maskinlæring.	Nasjonal strategi for bruk av skytjenester
R12	Målarkitektur for IAM skal ivareta brukere uavhengig av lokasjon og på mobile klienter.	Målarkitektur for IAM
R13	Skytjenestene skal være fleksible og kunne utvides etter behov.	Veileder i bruk av skytjenester
R14	Styringssystemet skal kunne anvendes ved konsum av ulike tjenestemodeller i skyen, f.eks. Saas, Paas og IaaS.	Veileder i bruk av skytjenester
R15	Databehandleravtale med skyleverandør må tilfredsstille krav i personvernforordningen (GDPR).	Veileder i bruk av skytjenester
R16	Total Cost of Ownership (TCO), kost/nytte-vurdering, skal tas hensyn til når tjenester i skyen skal vurderes.	Nasjonal strategi for bruk av skytjenester
R17	SPHF skal ta i bruk skytjenester på en måte som gir nødvendig portabilitet og forutsigbare kostnader ved exit.	Nasjonal strategi for bruk av skytjenester
R18	Skytjenestene som konsumeres av SPHF skal leveres av leverandører som har relevante sertifiseringer eller kan dokumentere at de oppfyller standarder som er etablert for leveranser til HSØ.	Veileder i bruk av skytjenester
R19	Når SPHF etablerer skytjenester skal ansvar for utførelse av sikkerhetsoppgaver være avklart mellom SPHF, Helseforetak og Leverandør.	Informasjonssikkerhet ved bruk av private leverandører i helse- og omsorgstjenesten
R20	Sikkerhet i skytjenester skal være i henhold til Normen, NSMs Grunnprinsipper for IKT sikkerhet og Regionens ledelsessystem for informasjonssikkerhet.	Veileder i bruk av skytjenester
R21	Skytjenester skal muliggjøre interoperabilitet og samarbeid, i et klinisk perspektiv, mellom foretakene i regionen for å understøtte prinsippet rundt «En pasient – en journal».	Tilnærming til bruk av skytjenester

6.2 Drivere for sikkerhet

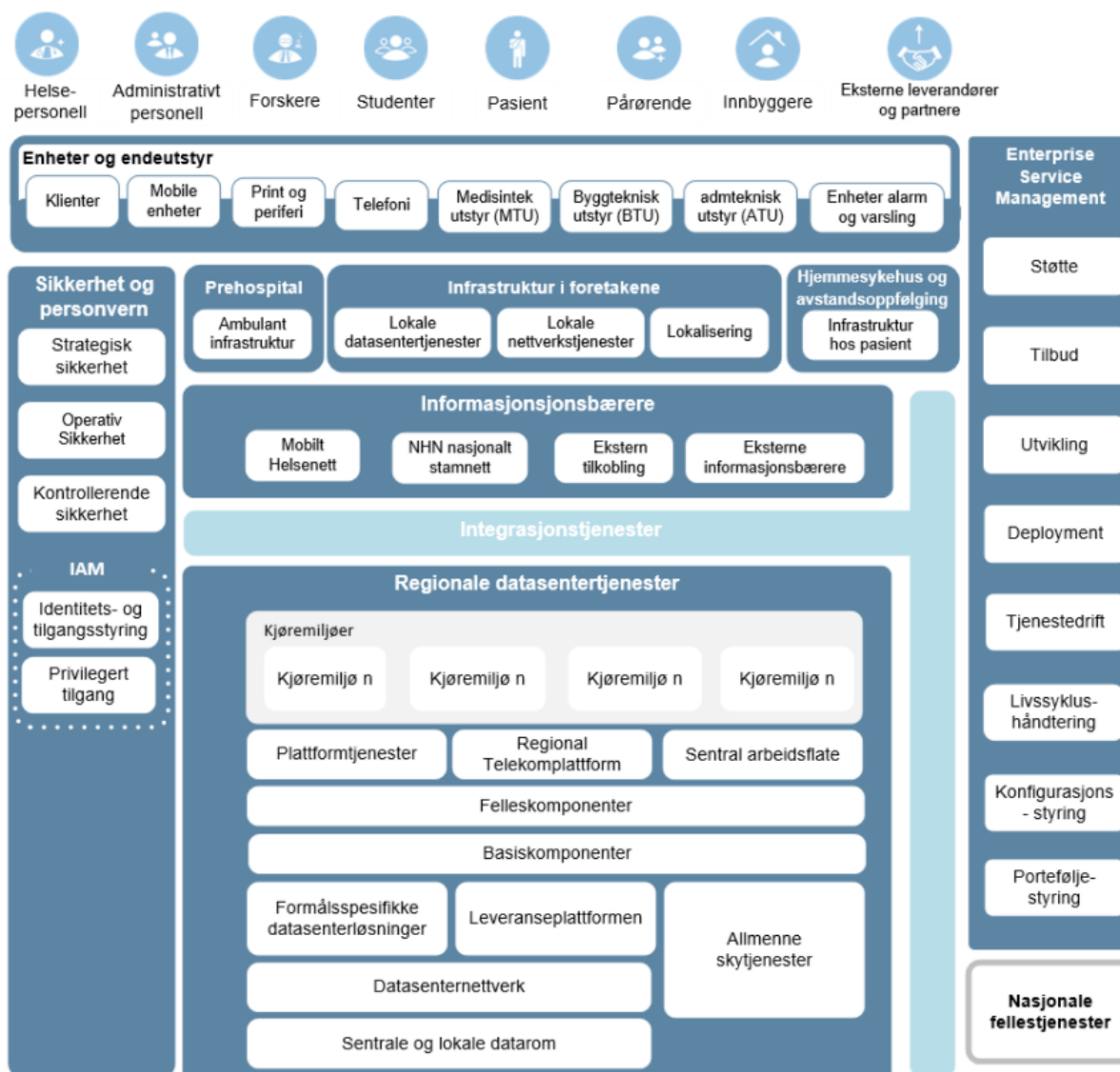
De funksjonelle kravene i kapittel 6.1 danner et grunnlag for drivere for sikkerhet. Driverne for sikkerhet er formulert som strategiske mål som implementeres for å støtte opp under spesifikke forretningsbehov og funksjonelle krav. Tabellen under lister opp driverne for sikkerhet og knytningen hver driver har til de funksjonelle kravene.

Driver#	Driver for sikkerhet - Beskrivelse	Knyttet til Krav#
BD1	Helseforetakene skal kunne ha tillit til at skytjenestene gir samme grad av konfidensialitet, integritet og tilgjengelighet som interne tjenester.	R4, R6, R15, R18, R20
BD2	Gi brukere tilgang til tjenester eksternt og fra mobile enheter med tilstrekkelig informasjonssikkerhet og personvern.	R6, R12
BD3	Brukere i helseforetakene skal kommunisere med hverandre og med pasienter og pårørende med tilstrekkelig konfidensialitet, integritet og tilgjengelighet for tjenestene.	R3, R4, R6, R7, R8, R20, R21
BD4	Skytjenestene skal tilfredsstillere helseforetakene i regionens sikkerhetskrav og regulatoriske krav til sikkerhet og personvern.	R15, R18, R20
BD5	Skytjenestene skal kunne driftes sikkert og kostnadseffektivt med høy grad av sentralisering og automatisering, og leverandør skal kunne byttes uten urimelige kostnader eller at data går tapt	R1, R4, R6, R16, R17, R20
BD6	Skytjenestene skal dekke krav knyttet til samhandling, dokumentdeling og videokonferanser i henhold til informasjonssikkerhetskrav gitt gjennom Helse Sør-Øst sitt ISMS.	R2, R3, R5, R15, R20, R21
BD7	SPHF må tilpasses drift av skytjenester basert på en modell der ansvar for sikkerhet er synliggjort og ivarettat slik at ingen deler av arkitekturen er uten aktiv forvaltning.	R19, R20
BD8	Skytjenester skal være underlagt helseforetakenes styring og ettersyn (governance) i henhold til Helse Sør-Øst sitt ISMS.	R18, R19, R20
BD9	Skytjenestene skal kunne skalere i takt med behovet og være fleksible med hensyn på tjenestemodell.	R2, R5, R13, R14
BD10	Teknisk miljø for skytjenester må kunne samhandle med tjenester i eksisterende datasenter på en måte som ivaretar krav til konfidensialitet, integritet og tilgjengelighet.	R8, R9, R10, R11, R21
BD11	Skytjenestene skal kunne tilby programvareutvikling og testing, samt analyse av store datasett i henhold til informasjonssikkerhetskrav gitt gjennom Helse Sør-Øst sitt ISMS.	R9, R10, R11
BD12	Valg og håndtering av skytjenesteleverandører skal utføres slik at gjeldende informasjonssikkerhetskrav etterleves.	R15, R18, R19

7 Konseptuell sikkerhetsarkitektur

Den konseptuelle sikkerhetsarkitekturen fokuserer på foretakene i regionen sine behov og mål for informasjonssikkerhet, hvilke av regionens verdier som må sikres samt risikoer og muligheter knyttet opp mot regionens drift og kjernevirksomhet. Her defineres altså konsepter og krav i forbindelse med

bruk av skytjenester sett fra et sikkerhetsperspektiv, som setter føringer for valg og organisering av logiske og fysiske sikkerhetselementer på lavere nivå⁴.



Figur 3 – Overordnet målarkitektur for IKT-infrastruktur i HSØ

7.1 Sikkerhetsledelse og ansvar

Når det gjelder informasjon, data og opplysninger⁵ er det alltid dataansvarlig, HF-ene i regionen, som har det endelige ansvar for at dataene blir behandlet i henhold til gjeldende regelverk. Dette betyr at ansvaret for å etterleve regelverk ikke kan fraskrives HFene, selv om dataene behandles hos en skyleverandør. SPHF er databehandler for de øvrige HFene, og skal forvalte IKT-avtaler i regionen på vegne av HFene.

⁴ Se dokumentet «Regionale sikkerhetsprinsipper for bruk av skytjenester»

⁵ Herunder personopplysninger, personopplysninger av særlig kategori, virksomhetsinformasjon, konfigurasjonsdata mv.

Det vil alltid være dataansvarlig sitt ansvar å klassifisere de data som er i bruk i skyløsningen. Data skal klassifiseres i henhold til gjeldende modell for informasjonsklassifisering hentet fra det Regionale ISMS. Data skal håndteres og sikres i henhold til denne klassifiseringen.

Hvem som har ansvar for beskyttelse av sluttbrukerapplikasjoner, tilgangskontroll, sikkerhet på applikasjonsnivå, nettverksnivå, og infrastruktur, kommer an på valgt tjeneste- og leveransemodell og må avklares før skytjenesten tas i bruk.

7.1.1 Ansvarsfordeling for sikkerhetstiltak

Hvordan sikkerhetsledelse og ansvar for utførelse av sikkerhetstiltak i praksis fordeles når det kommer til skytjenester, kommer an på valgt tjenestemodell. Enkelte sikringstiltak må alltid utføres av Sykehuspartner og helseforetakene selv, mens andre ivaretas av skyleverandøren. Fordeling av ansvar kontraktstfestes. Områdene Sykehuspartner og helseforetakene er ansvarlig for må det etableres rutiner for å ivareta, og utførelsen må kvalitetssikres med bl.a. risikovurdering. Områdene skyleverandøren det avtales at leverandøren er ansvarlig for må skyleverandøren utføre tilsvarende kvalitetssikring av, og kvalitetssikres av Sykehuspartner gjennom revisjon.

Skyleverandøren kan benytte underleverandører for å levere deler av tjenesten, eller til å utføre sikkerhetsoppgaver, men Sykehuspartner forholder seg alltid til parten det er inngått kontrakt med. Dette gjelder også i risikovurderinger, leverandørvedlegg, og revisjoner.

Ansvarsfordeling	On-prem	IaaS	PaaS	SaaS
Dataklassifisering og ansvar	☐	☐	☐	☐
Klient og endepunktbeskyttelse (mobiler og pc-er)	☐	☐	☐	☐
Kontoer og identiteter	☐	☐	☐	☐
Identitet katalog infrastruktur	☐	☐	☐	☐
Applikasjon	☐	☐	☐	☐
Middelvare	☐	☐	☐	☐
Operativsystem	☐	☐	☐	☐
Virtuell maskin	☐	☐	☐	☐
Virtuelt nettverk	☐	☐	☐	☐
Hypervisor	☐	☐	☐	☐
Prosessering og minne	☐	☐	☐	☐
Datalagring	☐	☐	☐	☐
Nettverk grensesnitt	☐	☐	☐	☐
Fasilitet og datasenter	☐	☐	☐	☐

Skykonsument sitt ansvar
 Delt ansvar
 Skyleverandør sitt ansvar

Figur 4 - Matrise for sikkerhetstiltak mellom ulike typer tjenestemodeller

Der hvor områder er delt mellom SPHF og skyleverandør (kategori 2) er det vesentlig at ansvarsfordelingen innenfor området presiseres i kontrakten slik at alle sikkerhetstiltak har en eier.

7.1.2 Intern forvaltning og kompetanse

Skytjenester krever også intern forvaltning hos Sykehuspartner. De syv horisontale nivåene i Figur 4 gir et overordnet bilde på hva slags type kompetanse SPHF må inneha for å sikre og forvalte skytjenester på en god måte. Figuren sier likevel ikke noe tydelig om hvilken mengde eller omfang av ressurser med riktig kompetanse som er nødvendig for å drifte og forvalte skytjenester på en trygg og sikker måte. Dette vil naturligvis avhenge av hvor mange, og hvor kompliserte, skytjenester som benyttes i regionen.

Valgt tjenestemodell (IaaS, PaaS eller SaaS) setter føringer for hva som er Sykehuspartners utøvende ansvar, hva som er leverandørens utøvende ansvar og hva som er delt utøvende ansvar mellom Sykehuspartner og leverandør, med hensyn til sikkerhetstiltak. I de tilfeller hvor Sykehuspartner har et utøvende ansvar, eller der det utøvende ansvaret er delt mellom Sykehuspartner og leverandør, må det foreligge intern kompetanse og forvaltning i henhold til type og mengde ansvar hos Sykehuspartner.

Med referanse til hva som kreves av avtaleinngåelse og –forvaltning er det også en forutsetning at Sykehuspartner innehar nødvendig juridiske ressurser, samt tilstrekkelig ressurser og kompetanse for ivaretagelse av avtaleverk på lang sikt. Figur 4 viser også behov for intern kompetanse av teknisk karakter, samt innen identitets- og tilgangsstyring og sikkerhet.

Berørte forretningsdrivere: BD7

7.2 Leverandørhåndtering

7.2.1 Risikovurdering av leverandører

Bruk av skytjenester krever at den dataansvarlige gjør dekkende risikovurderinger, og ellers følger kravene til avtaler og leverandøroppfølging i blant annet Normen. Sykehuspartner HF utarbeider risikovurderinger på vegne av de andre foretakene i regionen i henhold til etablert rutine og praksis. Det enkelte helseforetak står endelig ansvarlig for risikoaksept med bakgrunn i utarbeidet risikovurdering. Risikovurderinger som Sykehuspartner HF utarbeider på vegne av ett eller flere andre foretak i regionen skal som minimum inneholde beskrivelse av at⁶

- ansvarsfordelingen mellom dataansvarlig og databehandler er avklart, og tilpasset tjeneste- og leveransmodellen som benyttes
- dataansvarlig har oversikt over hvor data behandles geografisk
- databehandlers personell arbeider innenfor EU/EØS området.
- dataansvarlig påser at skyleverandørens eventuelle standardavtaler ikke er i motstrid med lovbestemte krav og Normens krav
- Dataansvarliges plan for ivaretagelse av informasjonssikkerhet og personvern ved avslutning av skytjenesten

Se også kapittel 7.2.2 til 7.2.4 for SLA og databehandleravtaler, 7.3 Risikostyring/risikovurdering, 7.4.3 for detaljer rundt databehandlingens lokasjon og **Feil! Fant ikke referanseilden. Feil! Fant ikke referanseilden..**

Berørte forretningsdrivere: BD5, BD12

⁶ Norm for informasjonssikkerhet kapittel 3

7.2.2 Avtaler og kontrakter

Gitt at skytjenester er en standardisert tjeneste så reguleres ansvarsfordelingen og forholdet mellom en kunde og skyleverandør gjennom en kontrakt. Som hovedregel vil en skyleverandør være den som stiller med standardiserte kontrakter og avtaleverk, dette være seg databehandleravtaler, tjeneste- og serviceavtaler (SLA) mv. Dette betyr at kvalitetssikring av kontrakten mellom kunde og leverandør av en skytjeneste er særdeles viktig. Rettigheter knyttet til styring og ettersyn av data må også gjelde skytjenester, noe som sikres gjennom avtaler med leverandør.

SPHF skal vurdere skyleverandører SPHF inngår kontrakter med. Ved å inngå avtaler med SPHF påtar leverandøren seg plikten til å pålegge sine underleverandører tilsvarende forpliktelser som skyleverandøren selv har påtatt seg ovenfor SPHF. Dette innebærer bl.a. at leverandør gjennomfører leverandørvurderinger av sine underleverandører og gjennomfører landvurderinger av land som er relevante for tjenesten. SPHF har rett til å revidere skyleverandøren for å kvalitetssikre at parten faktisk har utført sine oppgaver og forpliktelser.

Berørte forretningsdrivere: BD8, BD12

7.2.3 Tjenesteleveranseavtaler (SLA)

I alle tilfeller hvor skytjenester skal benyttes må det inngås avtaler mellom kunde og leverandør. Skytjenester er i stor grad en standardisert tjeneste med hensyn til avtaleverk og tilpasses aldri eller sjelden til den enkelte kundes ønsker eller behov.

Alle skyleverandører skal realisere tilgang til informasjonssystemer gjennom godkjente og dokumenterte løsninger. Leverandørtilgang skal ivareta krav til revisjonsspor og uavviselighet.

Tjenestene som skal leveres av en skyleverandører skal formaliseres i SLA-avtaler, som skal inkludere relevante sikkerhetskrav og ansvar for risiko og risikoreduserende tiltak (se kapittel 7.3).

Berørte forretningsdrivere: BD1, BD5, BD12

7.2.4 Databehandleravtaler og behandling av virksomhetssensitive opplysninger

I de tilfellene hvor leverandør behandler person- eller virksomhetssensitive opplysninger, skal behandlingen være underlagt avtale mellom gjeldende HF (i de fleste tilfeller SPHF) og skyleverandøren. Avtalen skal inngås gjennom egen databehandleravtale, eller så skal kravene til avtale med databehandler ivaretas av andre avtaler eller rettslige dokumenter. Avtalene må også dekke kjeden av eventuelle underleverandører.

Der mulig skal en integrator, eller skyleverandør, underskrive sikkerhetsinstruks eller så må dette søkes ivaretatt gjennom kontrakt som inngås for tjenesten (Non-Disclosure Agreement eller tilsvarende). Der det er relevant skal ansatte hos integratoren, eller skyleverandøren, signere taushetserklæring med gjeldende HF.

SPHF inngår databehandleravtaler som er i samsvar med norsk lovgiving, lever opp til GDPRs minimumskrav og ivaretar krav fra Normen⁷. Det skal fremkomme av databehandleravtalen eller kontrakt i hvilke(t) land data kan lagres og hvilke land data kan aksesseres fra. SPHF skal alltid kunne kreve innsyn i og måling av hvorvidt leverandørs sikkerhetskrav etterleves, se kapittel 7.5 Revisjon for ytterligere spesifikasjoner rundt dette.

Berørte forretningsdrivere: BD4, BD12

⁷ Se spesielt krav 5.7.8 og 5.7.9

7.3 Risikostyring/risikovurdering

Risikovurdering gjennomføres ved alle endringer som kan ha betydning for informasjonssikkerheten, herunder også anskaffelser, implementering/installering, konfigurasjonsendringer og utfasing av systemer relatert til skytjenester. All ny, eller endring i, behandling av helse- og personopplysninger skal også risikovurderes.

Når bruk av skytjenester skal risikovurderes må man se til ansvarsfordelingen mellom SPHF og skyleverandør og hvilken tjeneste- og leveransemodell man velger (se kapittel 7.1.1, Figur 4). Valg av tjeneste- og leveransemodell påvirker handlingsrommet for å håndtere risiko og må vurderes ved bruk av skytjenester.

Basert på tjeneste- og leveransemodell vil gjennomføringen av noen risikoreduserende tiltak treffe skyleverandøren, mens andre treffer HFene i regionen (ref kap7.1.1).

Dataansvarlig vil alltid eie risikoene ved bruk av skytjenester. Håndteringen av risikoreduserende tiltak kan overføres til skyleverandøren.

Risikovurderinger skal gjennomføres i henhold til Sykehuspartners risikovurderingsmetodikk. Utøvende ansvar for å følge opp tiltak fra risikovurderinger tildeles henholdsvis leverandør eller SPHF i henhold til valgt tjenestemodell ref. (Figur 4). For eksempel vil risikoreduserende tiltak på applikasjonsnivå i en IaaS treffe SPHF, mens det i en SaaS vil treffe leverandøren (Figur 4).

Berørte forretningsdrivere: BD1, BD12

7.4 Personvern

Helse- og personopplysninger i skyen skal behandles i tråd med gjeldende lovkrav og øvrig styrende dokumentasjon i Helse Sør-Øst. Skyleverandører vil ha rollen som databehandlere og vil ha selvstendige plikter etter personvernlovgivningen. Skyleverandører skal kun behandle personopplysninger etter instruks fra dataansvarlig.

Berørte forretningsdrivere: BD1, BD4

7.4.1 Innebygd personvern

Innebygd personvern er et sentralt krav i personvernforordningen. I forbindelse med skytjenester betyr dette at den dataansvarlige skal sørge for å velge en leverandør som er i stand til å levere skytjenester som hjelper den dataansvarlige med å etterleve personvernprinsippene.

7.4.2 Personvernkonsekvensvurdering

I enkelte tilfeller skal det gjennomføres personvernkonsekvensvurdering (DPIA)⁸. Bruk av skytjenester kan være behandlinger av personopplysninger som utløser krav om gjennomføring av DPIA. Eksempler (ikke uttømmende) på tilfeller det det må gjennomføres DPIA er:

- Når skytjenester benyttes til å behandle genetiske opplysninger om store mengder mennesker
- Når skytjenester benyttes sammen med «innovativ teknologi», som velferdsteknologi
- Når skytjenester benyttes til systematisk monitorering av personer
- Når skytjenester benyttes til å behandle lokasjonsopplysninger
- Når skytjenester benytter personopplysninger til å trene kunstig intelligens

⁸ [Datatilsynet - Når må man gjennomføre en vurdering av personvernkonsekvenser?](#)

Alle foretak i regionen har et personvernombud. Vedkommende kan rådføres når det gjelder personvernkonsekvensvurderinger mv.

7.4.3 Behandlingens lokasjon

Når helseforetak benytter skyløsninger til å behandle personopplysninger, skal den geografiske lokasjonen der behandlingen skjer være kjent og skriftlig dokumentert. Den dataansvarlige skal ha tilgang til dokumentasjonen av hvor behandlingen skjer.

SPHF skal kun benytte leverandører som kan garantere tilfredsstillende garantier for de registrertes personvern. SPHF skal tilstrebe å benytte leverandører som er registrert i EU/EØS-området (inkludert Norge), og følger regelverket her. Behandling av personopplysninger hos leverandører som er registrert utenfor EU/EØS er likevel tillatt når ett av vilkårene nedenfor er oppfylt:

- Behandlingen av personopplysninger skjer i en stat som Europakommisjonen har funnet til å ha tilstrekkelig vernnivå⁹
- Behandlingen skjer av et selskap som har tatt EUs standardpersonvernbestemmelser (Standard Contractual Clauses) inn i sin avtale med dataansvarlig
- Behandlingen skjer på bakgrunn av Binding Corporate Rules (BCR) hvor selskapet er etablert i EU/EØS og innenfor sitt konglomerat overfører personopplysninger ut av EU/EØS. BCR må være godkjent av kompetent tilsynsmyndighet.

I tillegg må personvernet være tilstrekkelig ivaretatt i overføringen av personopplysninger, og dette må kvalitetssikres.

Behandlinger av personopplysninger i tredjestat (dvs. stat utenfor EU/EØS) er heftet med risiko og usikkerhet. Det er muligheter for at alle de tre vilkårene for behandlinger av personopplysninger i tredjestater kan bortfalle og gjøre behandlingen lovstridig. Ved enhver behandling i tredjestater bør det derfor planlegges alternative modeller.

I tillegg til vilkårene ovenfor, må det vurderes om behandlingen av personopplysninger skjer i tråd med PSTs trusselvurderinger. Behandlinger av personopplysninger i stater der PST anser etterretningsrisikoen som høy bør unngås.

7.4.4 Segmentering av data

Skyleverandøren skal ha tekniske mekanismer som sikrer tilfredsstillende skille mellom data fra ulike dataansvarlige i skyleverandørens tekniske infrastruktur. De tekniske mekanismene skal være dokumentert. Feil på teknisk oppsett eller andre brudd på personopplysningssikkerheten som berører én av skyleverandørens kunder, for eksempel feil tilgangsstyring, skal ikke kunne ha negative konsekvenser for leverandørens øvrige kunder.

7.5 Revisjon

Det må være tydelig hvilke krav det aktuelle helseforetaket skal etterleve før bruk av skytjenester innføres. Dette slik at helseforetakene vet at attestasjoner fra leverandør og revisjoner som skal måle etterlevelse dekker relevante krav.

⁹ [EU's Adequacy decisions](#)

For å vise etterlevelse eller påpeke mangler mot gitte krav relatert til informasjonssikkerhet og personvern i forskrift, standarder, policyer eller rutiner skal det gjennomføres revisjoner av skyleverandøren og tilbudte tjenester.

Revisjon av skyleverandører kan gjennomføres på følgende måter:

- Leverandøren gjør en internrevisjon, hvor leverandøren selvdeklarerer etterlevelse til visse prinsipper
- En uavhengig tredjepart kan gjennomføre revisjon av skyleverandøren (på bestilling fra helseforetaket)
- Helseforetaket utfører selv revisjon av skyleverandøren. Dette er derimot uvanlig, gitt hvordan sky-teknologi fungerer.

I tilfeller hvor uavhengig tredjepart eller helseforetaket selv skal utføre revisjon, må det påregnes en økonomisk kostnad knyttet til dette, og det er viktig at muligheten for revisjon kontraktsfestes med skyleverandøren. Valgt tjeneste- og leveransemodell innen skytjenester kan påvirke hvordan revisjoner av skyleverandører kan gjennomføres.

Revisjoner gir kun et bilde av nåsituasjonen, og de relativt raske endringene og utviklingen av teknologi og tjenestetilbud innenfor skytjenester. Dette fordrer at det må legges opp til høy frekvens av revisjoner for å følge utviklingen.

Revisjon av skytjenester bør inngå i Sykehuspartners planverk og revisjonshjul.

Berørte forretningsdrivere: BD1, BD4, BD7

7.6 Klassifisering av informasjon

Det vil alltid være respektive HF (informasjonseier/dataansvarlig) sitt ansvar å klassifisere de data som er i bruk i skyløsningen. Data skal klassifiseres etter gjeldende modell for informasjonsklassifisering hentet fra det Regionale ISMS. Data skal håndteres og sikres i henhold til denne klassifiseringen.

Berørte forretningsdrivere: BD1, BD4

7.7 Tilgangsstyring (IAM)

Tilgangsstyring til skytjenester skal etableres i henhold til målarkitektur for Identity and Access Management (IAM). Tilgang til skytjenester skal bare gis til brukere med tjenstlig behov.

7.7.1 Autorisering og autentisering

Det ligger i en skytjenestes natur at tilgangsstyring må administreres både av Sykehuspartner og av skyleverandøren. Tilgangsstyringen ved bruk av skytjenester kan kompliseres ytterligere ved at flere skytjenester og –leverandører benyttes. Krav til tilgangsstyring gjelder likt for lokale informasjonssystemer som for informasjonssystemer basert på en skytjeneste. Tilgangsstyring for skytjenester skal baseres på gjeldende prosesser i Sykehuspartner HF og benytte samme autorative kilde som lokale tjenester.

Alle brukere skal være underlagt en prosedyre som kan verifisere at en bruker er en autentisk eier av en identitet.

Skytjenester skal bare tillate handlinger som er eksplisitt godkjent. De forskjellige brukergruppene som skal benytte skytjenester har forskjellige autorisasjoner som er gitt av administratorer. Det er mange interessenter med ulike tilgangsbehov på tvers av skytjenestene og det kreves derfor en finkornet autorisasjonsmekanisme for å gi alle brukere autorisasjoner i henhold til forretningsbehov.

Tilgang til skytjenester skal bare gis til autentiserte og autoriserte brukere. Sykehuspartner skal ha rutiner for autorisering, endring og avslutning av tilganger til og i skytjenester. Federering mot eksterne autentiseringstjenester skal benyttes for eksterne brukere slik at man unngår vedlikehold av disse brukerne i Sykehuspartner. Tilgang på tvers av juridiske enheter skal sikre sømløs samhandling, og identitet og tilhørende attributter skal fødereres på tvers av HF/eksterne virksomheter.

Når skytjenester benyttes skal eksisterende tilgangsstyring, så langt det lar seg gjøre, også benyttes for tilgangshåndtering i sky. Tilganger i skyen som ikke er knyttet til en intern tilgang bør minimeres.

Berørte forretningsdrivere: BD1, BD2, BD3, BD4, BD6

7.7.2 Separation of duties

Roller og rettigheter skal være tilstrekkelig finkornet slik at (administrative) brukere aldri har flere rettigheter enn de har tjenstlig behov for. Dette gjelder både på infrastruktur- og applikasjonsnivå.

Berørte forretningsdrivere: BD4, BD7

7.7.3 Administrative/privilegerte tilganger

Administrative brukere i skyen har utvidet ansvar og myndighet og det er viktig å redusere faren for misbruk av identiteter med utvidede rettigheter. Bruker med administratortilganger skal benytte personlig separat brukerkonto for administratoroppgaver. Driftspersonell skal ha personlige brukerkontoer for oppgaver som ikke krever administratortilganger.

Risikovurdering skal begrunne behovet for ulike administratorbrukere, også administratorbrukere lokalt for skytjenesten.

Berørte forretningsdrivere: BD1, BD4, BD7

7.7.4 Kontroll av tilganger

Det skal gjøres kontroll av tilganger til skytjenester på lik linje med kontroll av andre tilganger i Sykehuspartner HF.

Berørte forretningsdrivere: BD1, BD4.

7.8 Fysisk sikkerhet/adgangskontroll

Det respektive helseforetak i regionen er endelig ansvarlig for sine data (dataansvarlig) som lagres i sky.

Ved bruk av skytjenester er skyleverandør helt og fullt utøvende ansvarlig for fysisk sikring og adgangskontroll til sine anlegg. Grad av fysisk sikring må reguleres gjennom avtaler med skyleverandør.

Sykehuspartner, på vegne av foretakene i regionen, må derfor be leverandøren fremskaffe dokumentasjon på at tiltak knyttet til fysisk sikring er i henhold til gjeldende lovverk¹⁰ og nasjonale føringer og anbefalinger.

Berørte forretningsdrivere: BD12

7.9 Monitorering, logging og deteksjon

Monitorering, logging og deteksjon i forbindelse med skytjenester skal integreres i Sykehuspartners eksisterende regime for dette. Hvordan dette oppnås er i noen grad avhengig av hvilken tjenestemodell som benyttes¹¹ og hva leverandør tilbyr av data.

Det vil være nødvendig å tilpasse og videreutvikle Sykehuspartners evne til å drive tilstrekkelig monitorering, logging og deteksjon i forbindelse med skytjenester.

Behandling av helse- og personopplysninger skal logges i henhold til gjeldende lovkrav.

Viktige informasjonssikkerhetshendelser, for eksempel intrusjonsforsøk, må detekteres og rapporteres umiddelbart slik at angrep kan begrenses og stoppes.

Berørte forretningsdrivere: BD1, BD4, BD5

7.10 Hendelseshåndtering og etterforskning

Med bakgrunn i skytjenesters flyktighet og fleksibilitet som kan gi store endringer i raskt tempo vil hendelseshåndtering og etterforskning i større grad fordre automatisering.

Hendelseshåndtering og etterforskning i skytjenester må planlegges og beskrives i Sykehuspartners beredskapsplan, og videre avtales med den enkelte leverandør i SLA med hensyn til hendelseshåndteringsprosessen.

Det er viktig at skyleverandøren har ett kontaktpunkt i regionen når det gjelder sikkerhetshendelser. Tjenesteansvarlig for den enkelte skytjeneste må sørge for at skyleverandøren har en kommunikasjonskanal mot regionens Computer Emergency Response Team (CERT), slik at hendelser, sårbarheter, trusler og etterforskning kan varsles. Slike kommunikasjonskanaler må dokumenteres i Sykehuspartners beredskapsplanverk.

Leverandør av skytjenester skal uten ugrunnet opphold varsle Sykehuspartner CERT i henhold til avtalte rutiner om sikkerhetsavvik som må håndteres.

Berørte forretningsdrivere: BD4, BD7

7.11 Trussel- og sårbarhetshåndtering

Trusler mot, og sårbarheter i, infrastruktur eller nettverk i en skytjeneste håndteres hovedsakelig av skyleverandøren selv¹². Dette kan håndteres ulikt fra leverandør til leverandør. SPHF må i denne sammenheng etterspørre dokumentasjon fra skyleverandør knyttet til utførte sikkerhetsrevisjoner og sertifiseringer med hensyn til trussel- og sårbarhetshåndtering.

¹⁰ Herunder [Sikkerhetsloven](#), samt veiledninger og retningslinjer fra Nasjonal Sikkerhetsmyndighet, eventuelt tilsvarende lovverk i den aktuelle stat.

¹¹ Tilgang til logger og loggtyper er oftest mer tilgjengelig for dataansvarlig ved bruk av IaaS og PaaS, og i mindre grad ved SaaS.

¹² Unntaket gjelder for IaaS-tjenester. Mer om dette i regionale sikkerhetsprinsipper for bruk av skytjenester

Både driftspersonells personlige sertifiseringer og leverandørsertifiseringer er informasjon som skal innsamles for å vurdere en leverandørs modenhet med tanke på operasjonell sikkerhet.

Sikkerhetskonfigurasjon for IKT-utstyr i skytjenesten skal være dokumentert og tilgjengelig for Sykehuspartner som leverandør av IKT-tjenester til helseforetak i regionen. Skyleverandør skal ha en sporbar endringskontroll på konfigurasjon av IKT-utstyr og systemer.

Berørte forretningsdrivere: BD1, BD4, BD5, BD7, BD8, BD10, BD12.

7.12 Endringshåndtering

Med hensyn til Normen kap. 5.4.2¹³ skal alle HF ha et regime for endringshåndtering. Dette gjelder også for skytjenester. Alle tjenester som tas i bruk i skyen må følge gjeldende prosess for endringshåndtering. Dette omfatter også tjenester i skyen levert etter SaaS, PaaS eller IaaS modellene. Det er derimot viktig å merke seg at skyleverandøren selv har et eget endringshåndteringssystem, og at disse ikke nødvendigvis er kompatible med foretakets system. Det er derfor viktig at det opprettes en kommunikasjonskanal mellom Sykehuspartner HF og skyleverandør, slik at endringshåndtering hos skyleverandøren kan synkroniseres, eller hensyntas, hos relevant HF. Dette er viktig for å sikre en uavhengig kvalitetssikring og vurdering av risikoer, samt sikre nødvendig tilgjengelighet.

Berørte forretningsdrivere: BD1, BD5, BD7

7.13 Business Continuity, tilgjengelighet og oppetid

Alle skytjenester skal klassifiseres basert på tilgjengelighetskrav. Kravene skal spesifiseres i tjenestebeskrivelsen og er viktig fordi alle tjenester ikke trenger å ha samme krav til kontinuitet. Krav til tilgjengelighet og oppetid trenger ikke vurderes annerledes for skytjenester enn for interne tjenester og infrastruktur.

Når det kommer til forretningskontinuitet, tilgjengelighet og oppetid er det viktig å etablere hva som er det enkelte HFs ansvar og hva som er skytjenesteleverandørens ansvar.

Det enkelte HF har ansvar for å etablere og vedlikeholde beredskapsplaner (disaster recovery og business continuity). Sett opp mot skytjenester må disse dekke¹⁴:

- Ansvar og vaktordninger for håndtering av hendelser hos gjeldende HF
- Effektiv håndtering gjennom godkjente og kjente retningslinjer, instruksjoner, prosedyrer og prosesser
- Varslingsrutiner internt i HFet, samt varsling mot relevante leverandører og andre interessenter
- Kontinuitetsplanverk, inkludert for hver skytjenesteleverandør
- Prioriteringsliste over informasjonssystemer, inkludert skytjenester
- Årlige beredskapsøvelser, gjerne inkludert for skytjenester og involvering av leverandør

I avtaler mellom Sykehuspartner HF, som regional IKT-leverandør, og skytjenesteleverandøren må det være klart hva varslingsrutiner er og hvem som har ansvar for hva når det kommer til kontinuitet og gjenoppretting av skytjenester, dersom noe skjer på HFet eller skytjenesteleverandørens side.

¹³ Normen punkt 5.4.2

¹⁴ Helse Sør-Øst Sikkerhetsstrategi punkt 4.2.27

Tjenester skal være overvåket for bortfall av hele eller deler av tjenesten. Skytjenesteleverandøren har også et ansvar for vaktordning for håndtering av hendelser internt hos seg, og for at de holder seg oppdaterte og forberedte gjennom beredskapsøvelser.

Det er viktig at en skytjenesteleverandørs kapabilitet til å levere sikre og stabile tjenester tas med som et element i risikovurderingen av nye tjenester og leverandører.

Informasjon som legges i skyen skal være enkelt tilgjengelig for brukere, både fra mobile og stasjonære enheter.

Skytjenestene må kunne tilbakeføres til operasjonell status etter sammenbrudd eller annen hendelse som medfører driftsstans i henhold til SLA.

Berørte forretningsdrivere (tilgjengelighet): BD1, BD2, BD3

Berørte forretningsdrivere (oppetid): BD1, BD5

7.14 Datasikkerhet og -livssyklus håndtering

Datasikkerhet er viktig også når skytjenester benyttes, og alle former for cyberkriminalitet må forebygges. Bruk av skytjenester skal beskyttes mot ondsinnede handlinger og angrep både internt og eksternt fra over nettverk via nettverksperimeter. Prinsipper for zero-trust må gjelde også for skytjenester.

Alle sikringstiltak også for skytjenester skal være risikobaserte, slik at ikke alle tjenester, systemer og informasjon beskyttes likt. Når det kommer til bruk av skytjenester er det viktig at det finnes en oversikt over:

- Hvilke data som går til skyen og hvor, data må sikres både under overføring til og når den er lagret i skyen
- Beskytte og administrere data i skyen
 - o Tilgangskontroll (se kapittel 7.7)
 - o Kryptering (se kapittel 7.15)
 - o Arkitektur (se kapittel 7.18)
 - o Monitorering (se kapittel 7.9)
 - o Tilleggskontroller relatert til spesifikk leverandør samt tjeneste- og leveransemodell
- Håndtering av livssyklus for datasikkerhet og informasjon
 - o Styring og etterlevelse
 - o Backup og forretningskontinuitet, tilgjengelighet og oppetid

Det må sikres at eksisterende policyer rundt livssyklus håndtering for sikring av data også gjelder i skyen. Dette inkluderer regler og prinsipper for etablering og oppdatering, lagring, bruk, deling, arkivering og sletting av data i sky. Datasikkerhetslivssyklus håndteres gjennom kontraktuelle tiltak og sikkerhetskontroller. Alle tjenester som tas i bruk i skyen må følge gjeldende prosess for service asset & configuration management¹⁵.

Berørte forretningsdrivere: BD1, BD4, BD6

¹⁵ [Service Asset and Configuration Management](#)

7.15 Kryptering og nøkkelhåndtering

Med hensyn til kryptering av data følger Helse Sør-Øst anbefalinger gitt av Nasjonal Sikkerhetsmyndighet (NSM).

Kryptografiske kontroller for bruk av skytjenester må implementeres i de tilfeller dette fremkommer som nødvendig på bakgrunn av en risikovurdering. De kryptografiske kontrollene skal være sterke nok til å mitigere de risikoer som er identifisert. Hvordan kryptering og nøkkelhåndtering gjøres i praksis for skytjenester, vil avhenge av valgt leverandør og valgt tjeneste- og leveransemodell. IaaS, PaaS og SaaS gir ulike krypteringsmuligheter, og valgt krypteringsløsning må gjøres på bakgrunn av gjeldende trusselbilde og tekniske og forretningsmessige krav. Løsning for nøkkelhåndtering må velges ut fra krav til effektivitet, tilgjengelighet, forsinkelse og sikkerhet.

SPHF skal ansvarliggjøre skyleverandør når det kommer til kryptering og nøkkelhåndtering.

SPHF skal stille krav til skyleverandør slik at infrastrukturen som benyttes, samt de kryptografiske algoritmene, er i samsvar med:

- Internasjonalt/nasjonalt lovverk
- Nasjonale føringer
- Regionale føringer og anbefalinger

Den nasjonale tilsynsmyndigheten for tillitstjenester er Nasjonal kommunikasjonsmyndighet (NKOM), og deres liste over kvalifiserte tillitstjenester kan sees til hvis tjenesten skal behandle person- og helseopplysninger. Skyleverandørens sertifiseringer mht. kryptering og nøkkelhåndtering skal dokumenteres.

Berørte forretningsdrivere: BD1, BD2, BD3

7.16 Mobilsikkerhet

Skyleverandørens bruk av mobile enheter for administrasjon, drift eller vedlikehold av sine tjenester skal dokumenteres, og skyleverandøren skal dokumentere at nødvendige sikkerhetstiltak for sine mobile enheter er implementert.

Informasjonen på en mobil klient skal som minimum sikres like godt som ved bruk av en ordinær klient, men på grunn av økt risiko ved tap av enhet under transport eller lignende, må det som minimum¹⁶:

- vurderes om tiltak for å redusere sannsynlighet for informasjonstap må implementeres
- følge prinsipper om at personopplysninger ikke lagres på mobilt ukryptert medium

Bruk eller innføring av mobile enheter skal alltid risikovurderes, og konsekvenser for personvernet må vurderes.

Berørte forretningsdrivere: BD2

7.17 Human Resource-sikkerhet

Det er viktig å sikre at ansatte hos skytjenesteleverandøren forstår sin rolle og sitt ansvar og har kompetansen de trenger til å utføre sine arbeidsoppgaver slik at risikoen for (menneskelige) feil minimeres. Skytjenesteleverandøren skal kunne dokumentere hvordan de driver opplæring når det

¹⁶ Helse Sør-Øst Sikkerhetsstrategi punkt 4.2.26

kommer til sikkerhet, og hvordan personell opprettholder sin kompetanse.

Skyleverandøren skal forholde seg til følgende:

- Awareness/opplæring
 - o Alle ansatte hos skytjenesteleverandøren skal få opplæring i informasjonssikkerhet, tilpasset den enkelte rollen. Skytjenesteleverandøren skal ha et dokumentert opplæringsprogram som de ansatte oppdateres på jevnlig.
- Sikkerhetsinstruks/taushetserklæring/NDA
 - o Der mulig skal ansatte hos en skyleverandør underskrive sikkerhetsinstruks, ellers må dette søkes ivaretatt gjennom kontrakt som inngås for tjenesten (Non-Disclosure Agreement eller tilsvarende). Der det er relevant skal ansatte hos skyleverandøren signere taushetserklæring med gjeldende HF.
 - o Alle hos skyleverandøren som utfører arbeid for, eller arbeid i, helseforetakenes systemer, skal ha fått informasjon om og være kjent med, konsekvensene ved brudd på sikkerhetsreguleringer.
- Identifisering av leverandører¹⁷

Berørte forretningsdrivere: BD1, BD4, BD8, BD12

7.18 Infrastruktur og virtualisering

Infrastruktur skal deles inn i flere sikkerhetsnivåer i henhold til ny «Policy for Regional Sonemodell» og informasjonsklassifiseringsmodellen. Det skal foreligge sikkerhetskontroller som detekterer og forhindrer ikke godkjente tjenester, uønskede handlinger og eksterne trusselagenter.

Nettverkstrafikk skal overvåkes. Dette inkluderer til og fra skytjenester og leverandørtilgang, som alltid skal realiseres gjennom godkjent løsning.

Skytjenestene må kunne skalere for å håndtere økt bruk, krav til datalagring, prosesseringskapasitet med mer som kan oppstå gjennom tjenestenes levetid. Prosesseringskapasitet og lagringskapasitet må være tilgjengelig for skytjenestene når det er nødvendig. Bruk av skytjenester skal kunne utvides til å kunne supportere nye krav til sikkerhetsarkitektur og tjenester etter behov.

Sikkerhetsarkitekturen må kunne utvides og skalere for å ta høyde for nye brukergrupper (interne og eksterne), klientenheter og samhandlingsmønstre.

Bruk av virtualiseringsteknologi skal følge fastlagte prinsipper i henhold til beste praksis, leverandørens anbefalinger, regionens ledelsessystem for informasjonssikkerhet, samt kontrollrammeverk som beskrevet i Regional sikkerhetspolicy for skytjenester og øvrige tilknyttede dokumenter.

Berørte forretningsdrivere: BD9

7.19 Applikasjonssikkerhet

Bruk av skyteknologi driver frem endringer og nye muligheter for utvikling av og sikkerhet i applikasjoner. Skyteknologi kan gi et bedre sikkerhetsgrunnlag, mer automatisering, isolerte miljø og –virtuelle maskiner samt elastisitet. Det gir også noen utfordringer for applikasjonssikkerhet som må vurderes, som begrenset synlighet, logging og monitorering, og endret trusselbilde. Derfor er det viktig at SPHF forstår kapasiteten til leverandør på sikkerhet, og stiller krav til at leverandør:

¹⁷ Iht. eIDAS-forordningen

- Integrerer sikkerhet inn i applikasjonsdesign-prosessen
- Integrerer sikkerhetstesting i utviklingsprosessen
- Automatiserer sikkerhetstiltak og –kontroller
- Bruker de iboende egenskapene og mulighetene i skytjenester til å dele opp mellom produksjons- og utviklingsmiljø

Krav til applikasjonssikkerhet i sky kan trekkes ut fra CCM og CAIQ. Disse kommer i tillegg til applikasjonssikkerhetskrav som stilles for alle applikasjoner i regionalt ISMS.

Berørte forretningsdrivere: BD4, BD9, BD11.

7.20 Interoperabilitet og portabilitet

Skytjenestene skal være designet, implementert og driftet for å tilfredsstille regionens tekniske og operasjonelle standarder. Dette slik at leverandør i så liten grad som mulig benytter proprietære løsninger, filformat og lignende, all den tid det foreligger risiko for at skyleverandørens tjeneste rammes av bortfall eller andre hendelser som hindrer eller stopper tjenesteleveransen. Det er ønskelig for en dataansvarlig å ha mulighet til å flytte hele løsninger til annen leverandør relativt sømløst. Dette er viktig for å ivareta det respektive helseforetaks eierskap til dataene og slippe avhengighet til proprietære løsninger hvor leverandøren eksempelvis kan rammes av konkurs eller oppkjøp.

I henhold til personopplysningsloven og personvernforordningen¹⁸ har den registrerte rett til dataportabilitet – altså at data kan flyttes fra en leverandør eller et system over til en annen, og at dataene er lesbare både hos gammel og ny leverandør.

Skytjenester skal kunne samhandle med tjenester i eget datasenter slik at alle krav til sikkerhet er ivaretatt. Dette gjelder tilgang til tjenester internt, henting av data fra API, synkronisering av data og kommunikasjonstjenester.

Berørte forretningsdrivere: BD4, BD5, BD8, BD9, BD10.

¹⁸ [Lovdata - Personvernforordningen artikkel 20](#)