FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

Styret i Sparebanken Møre
Postboks 121
6001 ÅLESUND

VÅR REFERANSE	DERES REFERANSE	UNNTATT OFFENTLIGHET	DATO
19/2720		Offl. § 13 1. ledd, jf. fvl. § 13 1. ledd nr. 2 Merket tekst er unntatt offentlighet	11.06.2020

Tilsynsrapport

Finanstilsynet gjennomførte stedlig tilsyn med Sparebanken Møre (banken) 5. juli 2019.

Formålet med tilsynet var å gjennomgå og vurdere Sparebanken Møres styring og kontroll innen IKT-området med fokus på IKT-sikkerhet, herunder bankens oppfølging av IKT-leverandører.

Til grunn for tilsynsrapporten ligger Finanstilsynets foreløpige rapport datert 16. desember 2019 og styrets kommentarer til denne rapporten datert 29. januar 2020.

Finanstilsynet har følgende merknader etter det stedlige tilsynet:

Styring og kontroll med IKT-virksomheten

Internkontrollrapportering
Finanstilsynets vurdering i foreløpig rapport er at det er mangler i bankens internkontroll innen IKT-sikkerhet. Mangler i kontrollfunksjonene medfører risiko for at brudd på interne og eksterne krav ikke fanges opp og svekker ledelsens og styrets evne til å iverksette nødvendige tiltak. Etter Finanstilsynets vurdering er det behov for å systematisere og dokumentere kontrollene.

Finanstilsynet anbefalte i foreløpig rapport at det avsettes ressurser og iverksettes tiltak for å identifisere hvilke kontroller innen IKT-sikkerhet som er nødvendige å etablere, både internt i banken og i relasjon til IKT-leverandører. Dette er nødvendig for at bankens tre forsvarslinjer kan synliggjøre den faktiske kontrollsituasjonen ovenfor ledelsen og styret.

Finanstilsynet har fra styrets svar merket seg at styret tar anbefalingene til etterretning og at styret vil påse at nødvendige kontroller identifiseres og vil inngå i bankens rapportering.

Finanstilsynet understreker styrets ansvar for at tilstrekkelige kontroller etableres og følges opp.

Roller og ansvar innen IKT-sikkerhet
Finanstilsynet konstaterte i foreløpig rapport at banken ikke har beskrevet hvordan de ulike rollene innen IKT-sikkerhet skal ivareta sitt ansvar, og hvilke kontrollaktiviteter som skal foretas for å

FINANSTILSYNET
Revierstredet 3
Postboks 1187 Sentrum
0107 Oslo

Telefon 22 93 98 00

post@finanstilsynet.no
www.finanstilsynet.no

Saksbehandler
Tommie Gallefoss
Dir. tlf 22 93 98 00

verifisere at ansvaret ivaretas etter intensjonen. Finanstilsynet anbefalte at banken tydeliggjør dette gjennom instrukser.

Finanstilsynet har fra styrets svar merket seg at styret vil påse at ansvaret for gjennomføring og verifikasjon av kontrollaktivitetene beskrives i bankens IKT-kvalitetssystem.

Finanstilsynet tar styrets opplysning til etterretning.

Ressurser og kompetanse
Finanstilsynet anbefalte i foreløpig rapport at banken foretar en kartlegging av kompetanse- og ressurssituasjonen innen IKT-sikkerhet, og av IKT-området for øvrig. Bankens bestiller-kompetanse er særskilt viktig, både for å sikre at bankens egne krav gjenspeiles i avtaler med leverandører, og at leverandørstyringen utøves i tråd med bankens egne krav til styring og kontroll.

Finanstilsynet har fra styrets svar merket seg at banken vil sikre nødvendig kompetanse for IKT-området gjennom egne ansatte eller gjennom partnerskap. Styret vil påse at kompetanseplanen revideres basert på en kartlegging av kompetanse- og ressurssituasjonen innen IKT-sikkerhet og IKT-området for øvrig.

Finanstilsynet tar styrets opplysning til etterretning.

Risikostyring innen IKT-området
Finanstilsynet anbefalte i foreløpig rapport at bankens funksjoner, i samarbeid med risikostyringsfunksjonen, foretar en gjennomgang av hvilke områder og temaer som skal inngå i risikovurderingen. Basert på dette bør banken etablere og dokumentere prosedyrer som sikrer en årlig og helhetlig risikovurdering av IKT-området. Som et ledd i en helhetlig risikostyring, er det viktig å identifisere hvilke områder og funksjoner i banken som skal involveres i dette arbeidet.

Finanstilsynet har fra styrets svar merket seg at banken har etablert et prosjekt som vil påse at det etableres og dokumenteres prosedyrer og rutiner som sikrer helhetlig risikovurderinger på IKT-området minimum årlig. Videre fremgår det av styrets svar at sentrale funksjoner og områder skal identifiseres og involveres i risikovurderingene for å sikre samhandling, og at konsekvensene ved alvorlige hendelser skal bli belyst.

Finanstilsynet understreker styrets ansvar for at banken løpende følger med på risikobildet innen IKT-området.

IKT-Sikkerhet
Finanstilsynet oppfattet at sikkerhetsansvarlig/sikkerhetssjef i banken har det overordnede ansvaret for informasjonssikkerheten i banken, og at dette omfatter både fysisk sikkerhet og IKT-sikkerhet. Samtidig er ansvaret for IKT-sikkerhet lagt til IT-avdelingen. Bankens sikkerhetsansvarlig er organisatorisk plassert som en funksjon under Risikostyring og Compliance, men det var uklart for Finanstilsynet om rollen er definert som en andrelinjefunksjon. For å styrke internkontrollen anbefalte Finanstilsynet at det etableres et tydelig skille mellom første- og andreforsvarslinje innen området IKT-sikkerhet. Andreforsvarslinje bør, i samarbeid med Compliancefunksjonen, overvåke og følge opp førstelinjens styring og kontroll og bistå risikofunksjonen i arbeidet med operasjonell risiko innen IKT-sikkerhet.

Finanstilsynets vurdering var også at en sterkere knytning mellom funksjonene i førstelinjen og andrelinjen innen IKT-området vil styrke bankens internkontroll og anbefalte banken å etablere en dedikert samhandlingsplass for dette.

Finanstilsynet har fra styrets svar merket seg at banken gjennom et pågående prosjekt sikrer at det etableres et tydelig skille mellom første- og andreforsvarslinje innen området IKT-sikkerhet. Videre vil styret vurdere en dedikert samlingsplass for funksjonene i førstelinjen og andrelinjen innen IKT-området for styrking av bankens internkontroll på området.

Finanstilsynet understreker styrets ansvar for velfungerende funksjoner i bankens tre forsvarslinjer.

Internrevisjon
Finanstilsynets stilte i foreløpig rapport spørsmål ved internrevisjonens bruk av ressurser til arbeidet med risikovurdering og identifisering av aktuelle revisjonsområder innen IKT-området, som etter Finanstilsynets oppfatning er for begrenset.

Finanstilsynet har fra styrets svar merket seg at banken i revisjonsplanen for 2020 har satt av mer ressurser til internrevisjonsgjennomganger av IKT-området i forhold til tidligere år.

Finanstilsynet tar styrets opplysning til etterretning.

Styrende dokumenter

Kvalitetssystemets struktur
Finanstilsynet anbefalte i foreløpig rapport at det etableres et tydeligere skille mellom policy (førende) og prosedyrer/instrukser/rutiner (instruerende) dokumenter.

Finanstilsynet har fra styrets svar merket seg at styret vil påse at banken foretar en gjennomgang av etablerte dokumenter for å sikre et tydeligere skille mellom førende og instruerende krav.

Finanstilsynet tar styrets opplysning til etterretning.

Kontroll på etterlevelse
Finanstilsynet anbefalte at banken vurderer i hvilken grad de etablerte kontrollene dekker behovet for bekreftelse på etterlevelse av kontrollmål og krav slik disse fremgår av bankens policyer innen IKT-sikkerhet. Finanstilsynet anbefalte at banken etablerer de kontrollene banken mener er nødvendige for at kontrollfunksjonene i bankens forsvarslinjer skal kunne utøve sitt ansvar i tråd med ledelsen og styret sine forventinger og behov. Dette omfatter rutiner for andrelinjens oppfølging og kontroll med at besluttede kontroller gjennomføres, og rutiner for internrevisjonens vurdering av om kontrollene, internt i banken og hos IKT-leverandører, utføres som forventet. Finanstilsynet påpekte også at banken bør beskrive kontrollmål og kontroller som skal legges til grunn for bekreftelse på etterlevelse av de krav som er beskrevet, både internt i banken og hos IKT-leverandører, jf. eksempelvis kontrollmålene og kontrollene i ISO 27001/27002.

Finanstilsynet har fra styrets svar merket seg at styret anser det som hensiktsmessig å ytterligere beskrive kontrollmålene og hvilke kontroller som skal utføres. Styret vil påse at beskrivelser blir inkludert i relevante interne dokumenter.
Finanstilsynet tar styrets opplysning til etterretning.

Risikovurderinger innen IKT-området

Forretningsområdenes involvering
Finanstilsynet pekte i foreløpig rapport på at forretningsområdene bør involveres i arbeidet med risikovurderinger. Forretningsprosessene må inngå i grunnlaget for risikoidentifisering, analyse og evalueringen innen IKT-området for å synliggjøre forretningsmessige konsekvenser av de identifiserte risikoene. Dette bør være førende for bankens arbeid med risikoreduserende tiltak og vil også inngå som en viktig del av bankens arbeid med forretningsmessige konsekvensanalyser og kontinuitetsplaner. Finanstilsynet understreket i foreløpig rapport viktigheten av at forretningssiden tar eierskap til risikoer innen IKT-sikkerhet som utgjør en risiko for egne forretningsprosesser.

Finanstilsynet har fra styrets svar merket seg at styret vil sikre at forretningssiden involveres i arbeid med risikovurderinger innen IKT-området.

Finanstilsynet tar styrets opplysning til etterretning.

Risiko knyttet til bankens interne styring og kontroll
Finanstilsynet påpekte i foreløpig rapport at bankens risiko- og sårbarhetsanalyse i hovedsak dekker de generelle IKT-risikoene. Finanstilsynet etterlyste vurderinger av risikoer knyttet til ressurssituasjonen i IT-avdelingen, tekniske og organisasjonsmessige endringer og vurderinger knyttet til leverandørstyringen.

Finanstilsynet har fra styrets svar merket seg at styret vil påse at IKT-risikoene fra 2020 vil omfatte de påpekte forhold.

Finanstilsynet tar styrets opplysning til etterretning.

Risiko knyttet til tredjepart
Finanstilsynet påpekte i foreløpig rapport viktigheten av at risikovurdering av IKT-leverandørene inngår som en sentral del av bankens risikostyring. Finanstilsynet anbefalte banken å etablere en prosedyre som legger føringer og instrukser for en løpende/periodisk risikovurdering av IKT-leverandørene, jf. IKT forskriften § 3. Dette bør blant annet omfatte risikoer knyttet til leverandørens organisering, kompetanse og samhandling, samt forhold som gjelder tjenester til banken som leverandøren har utkontraktert.

Finanstilsynet har fra styrets svar merket seg at styret vil påse at bankens dokumenterte prosedyre for utkontrakterte IKT-systemer revideres, og vil omfatte gjennomføring av løpende/periodisk risikovurdering av IKT-leverandører.

Finanstilsynet understreker styrets ansvar for at risikoer knyttet til IKT-leverandørene identifiseres og inngår i bankens helhetlige risikovurdering.

Leverandørstyring

Leverandøravtaler
Finanstilsynet pekte i foreløpig rapport på at relevante krav til IKT-sikkerhet som er beskrevet i bankens kvalitetssystem, ikke fremkommer i avtalen med leverandøren, og at banken sammen med

leverandøren må identifisere nødvendige kontrollmål og kontroller som skal legges til grunn for leverandørens bekreftelse på etterlevelse av kravene.

Finanstilsynet har fra styrets svar merket seg at styret vil påse at aktuell SLA-avtale oppdateres i henhold til dette.

Finanstilsynet tar styrets opplysning til etterretning.

Uavhengige erklæringer og uttalelser fra leverandører
Finanstilsynet pekte i foreløpig rapport på at leverandørens ISAE 3402 revisjon er viktig for bankens internkontroll, men at ISAE3402-erklæringen ikke kan anses som en fullverdig bekreftelse på leverandørens etterlevelse av bankens krav. Det er ingen garanti for at bankens kritiske systemer og nettverk inngår i testutvalget som ligger til grunn for testene i ISAE 3402-revisjonen.

Finanstilsynet har fra styrets svar merket seg at styret vil sikre at banken formaliserer periodisk gjennomgang og behandling av uavhengige erklæringer fra leverandører gjennom tydelige kontrollmål og gjennomføringer av kontroller.

Finanstilsynet tar styrets opplysning til etterretning.

Samhandling med leverandører
Finanstilsynet anbefalte banken i foreløpig rapport å vurdere behovet for en utvidelse av samhandlingsmodellen innen IKT-sikkerhet, som kan knyttes direkte til etterlevelse av bankens egne policyer, kontrollmål og kontroller, slik dette er regulert i avtalen med leverandøren. Finanstilsynet understrekte at intensjonen med en slik modell i hovedsak er å innhente en kortfattet skriftlig bekreftelse fra leverandørens førstelinje på at kontroller er gjennomført, og med mulighet for å innhente dokumentasjon som underbygger bekreftelsen. Dette vil også åpne for at bankens internrevisjon kan gå gjennom leverandørens bekreftelser og vurdere om kontrollene som er utført har nødvendig kvalitet. Finanstilsynet mente dette vil bidra til å styrke bankens internkontroll ved at leverandørens kontrollsituasjon innen IKT- sikkerhet i større grad synliggjøres.

Finanstilsynet har fra styrets svar merket seg at styret vil vurdere behovet for en utvidelse av samhandlingsmodellen med leverandøren.

Finanstilsynet understreker styrets ansvar for at banken har en samhandlingsmodell med IKT-leverandørene som tilfredsstiller bankens behov for styring og kontroll.

Sikkerhetskultur og opplæring

Opplæring
Finanstilsynet ba i foreløpig rapport banken bekrefte at det er etablert kontroller for å følge opp at alle ansatte gjennomgår bankens opplæringstiltak for sikker bruk av bankens systemer.
Finanstilsynet har fra styrets svar merket seg at styret vil sikre at det blir etablert og dokumentert kontroller som sikrer at alle ansatte, inklusive nyansatte, gjennomfører web-basert eller annen obligatorisk opplæring.

Finanstilsynet understreker styrets ansvar for at bankens ansatte har kompetanse som er nødvendig for sikker bruk av bankens systemer.

Medarbeidere
Finanstilsynet etterspurte i foreløpig rapport behovet for kontrolltiltak for å bekrefte at det ved alle relevante ansettelser blir gjennomført bakgrunnssjekk, herunder krav om vandelsattest og politiattest, slik bankens rutiner for ansettelse tilsier.

Finanstilsynet har fra styrets svar merket seg at styret bekrefter at det ikke gjennomføres kontroll av at bakgrunnssjekk gjennomføres ved ansettelse, og at styret vil vurdere behovet for å etablere slike kontrolltiltak.

Etter Finanstilsynets vurdering er et slikt kontrolltiltak nødvendig.

Tilgangsstyring

Finanstilsynet ble opplyst på stedlige tilsyn at banken ikke har etablert kontroller for å verifisere at tilganger for ansatte som har sluttet er slettet i systemene, og ba i foreløpig rapport banken om å sikre at periodisk gjennomgang av tilganger utføres med bekreftelse fra ledere, og at det etableres rutine for dette.

Finanstilsynet har fra styrets svar merket seg at banken utfører årlig kontroll for å verifisere at tilganger for ansatte som har sluttet er slettet i systemene, og at det vil bli tilrettelagt instruks og rutiner for gjennomføring av nevnte kontroll mer enn en gang pr år. Styret vil sikre at nevnte rutine vil inkludere at ledere med personalansvar skal bekrefte periodisk gjennomgang av tilganger for sine ansatte.

Finanstilsynet tar styrets opplysning til etterretning.

Utvidede tilgangsrettigheter

Finanstilsynet påpekte i foreløpig rapport at banken må sikre at leverandøren bekrefter at det gjennomføres periodisk kontroll med utvidede tilgangsrettigheter.

Det fremgår av styrets svar at banken, i henhold til prosedyrer, gjennomfører årlig kontroll av tilgangsrettigheter til ansatte i banken og hos leverandører som har utvidede tilgangsrettigheter (operatøraksess). Videre fremgår det at for en av leverandørene er bankens kontroll av etterlevelse basert på ISAE 3402-erklæringen fra denne, og at styret tar Finanstilsynets bemerkning om at ISAE 3402-erklæringen ikke kan anses som en fullverdig bekreftelse på leverandørens etterlevelse av bankens krav, til orientering.

Finanstilsynet tar styrets opplysning til etterretning.

Informasjonssikkerhet

Segmentering av nettverk
Finanstilsynet påpekte i foreløpig rapport at det er viktig at banken etablerer rutiner som til enhver tid sikrer at bankens nettverk er etablert med segmentering i tråd med bankens krav, og at dette innføres som en del av bankens kontroller.

Finanstilsynet har fra styrets svar merket seg at banken vil sikre at kontrollmål, samt hvilke kontroller og tester av infrastruktur og nettverk som skal gjennomføres, spesifiseres, herunder at bankens nettverk er etablert med segmentering i tråd med bankens krav.

Finanstilsynet tar styrets opplysning til etterretning.

Konfigurasjonsstyring
Finanstilsynet understrekte i foreløpig rapport at det er bankens ansvar, i tråd med krav i IKT-forskriftens §12, å sikre at leverandøren har etablert tilstrekkelige rutiner og kontroller for konfigurasjonsstyring av de tjenester som inngår i leveransene til banken.

Finanstilsynet har fra styrets svar merket seg at styret vil sikre at kontrollmål og kontroller inkluderer sikkerhetsstatus på komponentene i infrastrukturen.

Finanstilsynet tar styrets opplysning til etterretning.

Herding
Finanstilsynets anbefalte i foreløpig rapport at banken stiller krav til IKT-leverandørene om regelmessig rapportering, for eksempel månedlig, av status på herding og patching. Dette er også i tråd med kravene i bankens policy og vil være en av bankens kontroller.

Finanstilsynet har fra styrets svar merket seg at banken vil sikre at kontrollmål og kontroller inkluderer status på herding og patching.

Finanstilsynet tar styrets opplysning til etterretning.

Sikkerhet i applikasjoner
Følgende krav er beskrevet i bankens policy: "Applikasjoner/systemer i desentral plattform som behandler konfidensiell informasjon (personopplysninger, finansiell informasjon etc.) skal ha et høyt sikkerhetsnivå og testet for sikkerhetshull minimum i henhold til OWASP topp 10 eller tilsvarende."

Finanstilsynet ba banken i foreløpig rapport utdype hvordan dette etterleves, og anbefalte at banken i sine rutiner etablerer nødvendige kontroller.

Finanstilsynet har fra styrets svar merket seg at banken forutsetter at leverandører som gjennomfører utviklingsoppdrag, etterlever kravene i bankens sikkerhetspolicy og prinsippene "Security by design" og "Privacy by design". Banken forutsetter også at leverandøren foretar en kodegjennomgang. Styret tar Finanstilsynets anbefalinger til etterretning og vil sikre at bankens rutineverk også dekker testing og dokumentasjon av bankens kontroller knyttet til sikkerhet i applikasjoner.
Finanstilsynet tar styrets opplysning til etterretning.

Datalekkasje gjennom epost og eksterne medier
Finanstilsynet påpekte i foreløpig rapport at banken ikke har etablert tilstrekkelige kontroller for å oppdage eller forhindre datalekkasje gjennom uautorisert epostutveksling eller uautorisert lagring til eksterne medier. Finanstilsynet kommenterte at dagens praksis utgjør en høy risiko for at konfidensiell informasjon kan komme på avveie som følge av ubevisste eller bevisste handlinger fra ansatte eller ansatte hos leverandører, og at kontroller bør etableres for å redusere denne risikoen.

Finanstilsynet har fra styrets svar merket seg at styret vil sikre at banken ytterligere vurderer risikoen for at konfidensiell informasjon kan komme på avveie. Nødvendige tiltak som nye kontrollfunksjoner og tekniske løsninger vil vurderes og eventuelt innføres.

Finanstilsynet understreker styrets ansvar for at det etableres kontroller som minimerer risikoen for at konfidensiell informasjon kommer på avveie.

Sikring mot sosial manipulering
Finanstilsynet kommenterte i foreløpig rapport at banken hadde besluttet å innføre løsninger for å avdekke falske avsendere av epost og for å avdekke misbruk av bankens domener, men at dette ennå ikke var gjennomført.

Finanstilsynet har fra styrets svar merket seg at banken er i ferd med å etablere løsninger for å avdekke falske avsendere av epost og for å avdekke misbruk av bankens domener. Styret vil sikre at implementeringen av nevnte løsninger ferdigstilles.

Finanstilsynet tar styrets opplysning til etterretning.

Skjerming av ansatte med fullmakter
Finanstilsynet konstaterer at banken ikke har etablert særskilte tiltak, utover opplæringen som nevnt, for å redusere risikoen for at informasjon om ansattes roller [redacted] ikke kommer uvedkommende i hende. Dette medfører en økt risiko for en målrettet sosial manipulering fra kriminelle miljøer. Finanstilsynet anbefalte at ansatte i banken, og hos tredjepart, som inngår i målgruppen, instrueres særskilt, og at det etableres instrukser for dette som del av bankens sikkerhetspolicy.

Finanstilsynet har fra styrets svar merket seg at styret vil gjøre en vurdering av hvordan banken på en hensiktsmessig måte kan skjerme ansatte med fullmakter.

Finanstilsynet tar styrets opplysning til etterretning.

Overvåking av aktiviteter i nettverket og systemer
Finanstilsynet pekte i foreløpig rapport på at det er viktig å overvåke aktiviteten til ansatte med utvidede tilgangsrettigheter og ansatte som sitter på informasjon som kan utgjøre en spesielt stor trussel for bankens drift om tilliten som er gitt misbrukes. Slik overvåking vil også kunne avdekke om kriminelle har lykkes i å etablere et digitalt fotfeste på innsiden av bankens nettverk. Samtidig kan overvåking av ansatte være en utfordring med hensyn til personvernet. Finanstilsynet pekte i foreløpig rapport på at banken bør vurdere behovet for å etablere overvåking av ansatte med utvidede tilgangsrettigheter og som et minimum, etablere kontroller for periodiske gjennomganger av loggede aktiviteter i kritiske systemer.

Finanstilsynet har fra styrets svar merket seg at banken har gjennomført en vurdering av personvernkonsekvenser, hvor bankens personvernombud og hovedtillitsvalgt var involvert. Styret vil påse at det gjøres vurderinger av eventuelle kontrollfunksjoner og tekniske løsninger.

Finanstilsynet tar styrets opplysning til etterretning.

Endringsstyring

Finanstilsynets påpekte i foreløpig rapport at bankens styrende dokumenter for endringshåndtering i for liten grad er instruerende, og det mangler beskrivelse av hvilke kontroller som skal utføres for å verifisere etterlevelse både når det gjelder endringer som utføres av banken selv, og for endringer som utføres av leverandører.

Finanstilsynet har fra styrets svar merket seg at styret vil sikre at bankens kvalitetssystem også beskriver hvilke kontroller som skal utføres for å verifisere etterlevelse både når det gjelder endringer som utføres av banken selv, og for endringer som utføres av leverandører.

Finanstilsynet understreker styrets ansvar for at endringsstyring internt i banken og hos bankens IKT-leverandører er underlagt tilstrekkelig styring og kontroll.

Kontinuitetsledelse

Finanstilsynet konstaterer at banken selv har signalisert, gjennom lederrapporteringen av internkontrollen for 2018, at det er behov for å forbedre bankens håndtering av krisesituasjoner og testing av bankens beredskapsplaner.

Finanstilsynet oppfordret i foreløpig rapport banken å rette en spesiell oppmerksomhet mot sikkerhetshendelser, og vurdere om banken sammen med sine IKT-leverandører er tilstrekkelig forberedt på å håndtere hendelser av alvorlig karakter, for eksempel Cyber-angrep.

Finanstilsynet har fra styrets svar merket seg at styret vil påse at eksisterende planverk vil bli oppdatert i henhold til etablerte tiltak og i samsvar med rulleringsplan for beredskapsplaner [redacted]

Finanstilsynet understreker styrets ansvar for at banken er rustet til å kunne håndtere alvorlige hendelser.

Kopi av tilsynsrapporten bes sendt intern og ekstern revisor.

For Finanstilsynet

Olav Johannessen
seksjonssjef

Tommie Gallefoss
tilsynsrådgiver

Dokumentet er godkjent elektronisk og har derfor ikke håndskrevne signaturer.