FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

Kommunalbanken AS
Att: Styret
Postboks 1210 Vika
0110 OSLO

VÅR REFERANSE	DERES REFERANSE		DATO
19/8411			05.08.2021

Tilsynsrapport

Finanstilsynet gjennomførte stedlig tilsyn i Kommunalbanken AS (KBN) med møter avholdt 27. september 2019 og 30. oktober 2019. Tilsynet hadde som formål å gjøre en vurdering av hvordan KBN sikrer administrasjon, drift, vedlikehold og sikkerhet for foretakets IKT-virksomhet, herunder utkontrakterte IKT-tjenester knyttet til foretakets styreportal levert som en SaaS-løsning (Software as a Service).

Til grunn for disse merknadene ligger Finanstilsynets foreløpige rapport datert 1. mars 2021 og styrets kommentarer til rapporten i brev av 30. april 2021.

Som en innledende kommentar til KBNs svar på Finanstilsynets foreløpige rapport, så er det Finanstilsynets vurdering at sertifiseringer etter ISO/IEC 27001 eller revisjoner etter SOC-2 (Service Organization Control) ikke nødvendigvis er dekkende for å sikre etterlevelse av IKT-forskriftens bestemmelser.

Finanstilsynet har følgende merknader etter det stedlige tilsynet:

FORHOLD KNYTTET TIL STYRING OG KONTROLL

Endringshåndtering

Finanstilsynet ble under tilsynet informert om at leverandør av KBNs styreportal ikke har en dokumentert og etablert prosess for å håndtere endringer. Finanstilsynets vurdering er at leverandør av IKT-tjenester knyttet til KBNs styreportal skal oppfylle IKT-forskriftens bestemmelser. Det legges derfor til grunn at KBN gjennom oppfølging av leverandørens IKT-tjenesteleveranse sikrer at det etableres prosedyrer for endringshåndtering iht. gjeldende regelverk.

Det fremgår av KBNs svar på foreløpig tilsynsrapport at leverandør av styreportal har dokumenterte prosesser for endringshåndtering som etter KBNs vurdering tilfredsstiller kravene i IKT-forskriften §9 avviks- og endringshåndtering. Videre fremgår det av svaret at prosessene er dokumentert, og rutiner for endringshåndtering er gjenstand for årlig revisjon dokumentert i SOC 2-rapporter.

Det er Finanstilsynets vurdering av dokumentasjonen det vises til gir en beskrivelse av at endringshåndtering skal utføres, men at dokumentasjonen ikke i tilstrekkelig grad dokumenterer prosessen for endringshåndtering og hvordan denne skal utføres.

FINANSTILSYNET
Revierstredet 3
Postboks 1187 Sentrum
0107 Oslo

Telefon 22 93 98 00

post@finanstilsynet.no
www.finanstilsynet.no

Saksbehandler
Stig Ulstein
Dir. tlf 22 93 99 66

Tilgangsstyring

Finanstilsynet ble under tilsynet informert om at KBN ikke gjennomfører revisjoner av brukertilganger for personell hos leverandøren som utfører tjenester knyttet til KBNs styreportalløsning. Foretakets styredokumentasjon kan inneholde data som vil kunne misbrukes om de kommer på avveie. Finanstilsynet mener derfor det er viktig at KBN følger opp leverandørens bruk av tilganger ved at data som blir aksessert i systemet blir overvåket. Videre må KBN ha kontroll med hvilke av leverandørens brukere som har tilgang til sensitive data, og kunne loggføre dette.

I KBNs svar på foreløpig tilsynsrapport vises det til at det er inngått tjenesteavtale som sikrer behandling av KBNs sensitive data hos leverandøren. I avtalen kreves det skriftlig tillatelse fra KBN dersom leverandørens ansatte må aksessere KBNs informasjon, med unntak for i nødsfall. I slike tilfeller skal KBNs kontaktperson varsles umiddelbart etter at KBN informasjon er aksessert. Behandling av personopplysninger er regulert i egen databehandleravtale.

Videre vises det i svaret til at leverandøren leverer systemet som SaaS og dermed har behov for tilgangsrettigheter som kan innebære innsyn i kundens data. Kontroll med tilgangsrettigheter er etter KBNs vurdering underlagt forsvarlige prosedyrer gjennom at leverandøren har dokumentert og implementert tilgangsstyring iht. ISO 27002-9 Aksesskontroll, med rollebaserte tilganger etter «least privilege» -prinsippet. Rutinene og etterlevelsen er omfattet av revisjonen fra Deloitte og dokumentert i årlige SOC 2-rapporter (Deloitte 2018) (Deloitte 2019) (Deloitte 2020) med beskrivelse i pkt. 3.3 og verifisert i kontrollpunktene CA.29 til CA.34 og CA.36 til CA.39 uten avvik.

Etter Finanstilsynets vurdering er behovet for styring og kontroll av tilgangsrettigheter viktig, særlig på grunn av at løsningen er levert som en SaaS-løsning.

Styring og kontroll

Finanstilsynet ble under tilsynet informert om at leverandøren av styreportalløsningen ikke har etablert en funksjon som er ansvarlig for styring og kontroll av IKT-virksomheten. Det er Finanstilsynets vurdering at styring og kontroll med IKT-virksomheten er sentralt i arbeidet med å etablere en effektiv internkontroll. Finanstilsynets vurdering i foreløpig rapport er at KBN i sin oppfølging av leverandøren må sikre at nødvendige kontroller blir etablert, og at det etableres rutiner for oppfølging av kontrollene.

I KBNs svar på foreløpig tilsynsrapport ble det vist til at "*forskrift om IKT-systemer i banker mv og Finanstilsynets rundskriv 3/2020 samt EBAs retningslinjer for utkontraktering (EBA 2021) begrenset av finansforetaksloven setter krav til risikostyring og internkontroll for IKT-virksomheten og utkontraktert IKT-virksomhet for foretak som er under tilsyn*".

Av svaret fremgår det videre at KBNs styret mener regelverket kun gjelder for KBN og at leverandør av styreportalløsningen, som tjenesteleverandør til KBN, ikke er underlagt dette regelverket. Videre fremgår det av svaret at KBN mener de har tilstrekkelig innsyn i tjenesteleverandørs virksomhet, herunder styringssystem, sikkerhet, kvalitetssikring, tekniske løsninger, mv. som gjør at KBN kan sikre etterlevelse av regelverket.

Finanstilsynets vil peke på at etter IKT-forskriftens krav i § 12 er KBN ansvarlig for at IKT-virksomheten oppfyller alle krav som stilles etter forskriften, også der hele eller deler er

utkontraktert, og at det skal foreligge en avtale som sikrer dette. Finanstilsynet fastholder at for å kunne ivareta ovenfornevnte krav må KBN påse at IKT-tjenesteleverandør har tilstrekkelig organisering og rapportering når det gjelder leverandørens styring og kontroll.

Avtale

Ved gjennomgang av mottatt dokumentasjon er det Finanstilsynet vurdering at avtalen, som KBN har signert med leverandør for kjøp av IKT-tjenester ifm. styreportal, ikke er iht. gjeldende regelverk KBN er underlagt. Blant annet fremgår det ikke av avtalen at leverandøren skal etterleve IKT-forskriftens bestemmelser på en slik måte at KBN etterlever forskriftens krav. Videre fremgår det heller ikke av avtalen at KBN, og også Finanstilsynet, gis rett til å kontrollere, herunder revidere, de av leverandørens aktiviteter som er knyttet til avtalen, jf. forskriftens § 12 Utkontraktering.

Av KBNs svar på foreløpig tilsynsrapport fremgår det at avtalen mellom KBN og leverandøren er en abonnementsavtale for SaaS-løsningen «styreportal» og at ny avtale ble oversendt Finanstilsynet ifm. det stedlige tilsynet. Videre vises det i svaret til at ny avtale sikrer KBN rett til å foreta revisjon hos leverandøren og sikrer Finanstilsynets rett til å motta informasjon fra og kontrollere leverandøren som ledd i sitt tilsyn med KBN.

Finanstilsynet tar bankens opplysning til etterretning.

Kopi av rapporten bes sendt valgt revisor.

For Finanstilsynet

Olav Johannessen
seksjonssjef

Stig Ulstein
senior tilsynsrådgiver

Dokumentet er godkjent elektronisk og har derfor ikke håndskrevne signaturer.