

**FINANSTILSYNET**THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAYVIPPS MOBILEPAY AS
v/styret
Postboks 9236 Grønland
0134 OSLOVår referanse
25/6268
Deres referanse

13.10.2025

Tilsynsrapport

1. Innledning

Finanstilsynet gjennomførte IKT-tilsyn 19. og 20. juni 2025 i Vipps MobilePay AS (heretter omtalt "foretaket"). Formålet med tilsynet var å gjøre en vurdering av hvordan foretaket administrerer, utvikler, drifter, vedlikeholder og sikrer IKT-systemer og -tjenester. For dette området så tilsynet på styring med og kontroll av IKT-virksomheten. Tilsynet vektla systemløsninger som støtter foretakets kjernevirksomhet og prioriterte IKT-systemer som foretaket har utkontraktet.

Til grunn for disse merknadene ligger Finanstilsynets foreløpige rapport datert 2. juli 2025 og styrets kommentarer til rapporten i brev av 10. september 2025. Tilsynsrapporten er utarbeidet med utgangspunkt i IKT-forskriften, som var gjeldende regelverk for foretaket på tilsynstidspunktet. Fra 1. juli 2025 skal foretaket etterleve DORA-forordningen med tilhørende delegerte kommisjonsforordninger, jf. DORA-loven § 1.

2. Finanstilsynets oppsummering

Tilsynet avdekket ingen vesentlige mangler ved foretakets styring med og kontroll av IKT-virksomheten. Foretakets risikostyring har noen mindre påpekninger, blant annet knyttet til uklarheter i overordnet styringsdokumentasjon, endringshåndtering, oppfølging av utkontraktet IKT-virksomhet og testing av beredskapsplaner.

3. Finanstilsynets vurderinger

3.1. Overordnet styringsdokumentasjon

Foretaket skal ha klare og hensiktsmessige styrings- og kontrollsystemer samt hensiktsmessige retningslinjer og rutiner for å styre, overvåke og rapportere risiko foretaket er eller kan bli eksponert for, jf. finansforetaksloven § 13-5 første ledd. IKT-forskriften § 2 første ledd stiller videre krav til at foretaket skal fastsette overordnede mål, strategier og sikkerhetskrav for IKT-virksomheten.

Finanstilsynet pekte i foreløpig tilsynsrapport på at det synes å være uklarhet i forholdet mellom prinsipp- og policydokumentene, og ba foretaket sikre at foretakets styrende dokumenter for IKT på prinsipp- og policynivå samlet gir mer hensiktsmessig styring av IKT-virksomheten.

Styret skriver i sitt svar at foretaket tar innspillet fra Finanstilsynet til etterretning, og vil gjennomgå dokumentasjonsstrukturen for å tydeliggjøre sammenhengen mellom prinsipp- og policynivå, slik at dette samlet legger til rette for god styring av IKT-virksomheten.

Finanstilsynet tar styrets svar til etterretning.

3.2. Virksomhetens konsekvensanalyse

Det skal foreligge oppdatert dokumentasjon av det enkelte IKT-system, som er av betydning for foretakets virksomhet, ifølge IKT-forskriften § 13. Hensiktsmessige planer og tiltak for tilgjengelighet og kontinuitet bør etableres med utgangspunkt i konsekvensanalyser for foretakets kritiske forretningsprosesser. Virksomhetens konsekvensanalyse skal bidra til å sikre at foretakets beredskapsplaner utarbeides med basis i forretningsmessig kritikalitet. Planene skal basere seg på foretakets prioriteringer for gjenoppbygging av forretningskritiske tjenester og prosesser. Prioriteringene for gjenoppbygging skal basere seg på resultatene fra analysen, hvor det også skal framgå hva som er akseptabel nedetid for det enkelte IKT-system. Beredskapsplanene, som viser foretakets prioriteringer for gjenoppbygging, bør formidles til relevante leverandører. For å verifisere at det er etablert fungerende planer og løsninger må det foretas regelmessig opplæring, øvelse og testing, jf. IKT-forskriften § 11.

Finanstilsynet bemerket i foreløpig tilsynsrapport at virksomhetens konsekvensanalyse anses som et sentralt styringsdokument og at den, gitt dens flerfunksjonelle anvendelse utover beredskapsområdet, bør forankres i en overordnet standard i foretakets dokumentasjonsstruktur. Dette for å sikre at konsekvensanalysen tydelig identifiserer og prioriterer Vipps MobilePays produkter, tjenester og støttende infrastruktur, og ikke eksklusivt knyttes til beredskapsstandarden.

Styret skriver i sitt svar at foretaket erkjenner forbedringsbehov knyttet til den gjeldende konsekvensanalysen, særlig når det gjelder vurdering og dokumentasjon av gjenoppbyggingsmål og avbruddstoleranser (RPO, RTO og MTPD), og at foretaket vil oppdatere relevant styrende dokumentasjon for å inkludere kravene. Videre merker Finanstilsynet seg at Vipps MobilePay samtidig vil vurdere hvordan konsekvensanalysen best kan forankres i foretakets dokumenthierarki og virksomhetsstyring.

Finanstilsynet tar styrets svar til etterretning.

3.3. Kontrollfunksjoner

I finansforetaksloven § 13-5 andre ledd stilles det krav om at et finansforetak skal ha uavhengige kontrollfunksjoner med ansvar for risikostyring, etterlevelse, internrevisjon og aktuarfaglige oppgaver. Foretakets uavhengige kontrollfunksjoner i andre forsvarslinje skal ha tilstrekkelig kompetanse tilpasset risikoen ved og omfanget av virksomheten i foretaket. Det framgår av CRR/CRD-forskriften § 38 og § 39.

Finanstilsynet pekte i foreløpig tilsynsrapport på at det i tilsynsmøtet ble opplyst at første og andre forsvarslinje utfører sine oppgaver og kontroller basert på rapportering fra IKT-tjenesteleverandør, men at det ikke rapporteres på oppfyllelse av styregodkjente dokumenter. Finanstilsynet presiserte at det anser det som vesentlig at foretaket regelmessig rapporterer til styret om etterlevelsen av de styrende dokumentene som styret har vedtatt for IKT-området.

Styret skriver i sitt svar at foretakets første og andre forsvarslinje gjennomfører kontroller og oppfølging av IKT-området, inkludert for utkontraktert virksomhet. Videre opplyses det at foretaket fortløpende og risikobasert vil vurdere om de etablerte kontrollene er tilstrekkelige for å sikre forsvarlig leverandøroppfølging. Foretaket bekrefter at det framover vil styrke styrerapporteringen ved å inkludere en vurdering av etterlevelsen av de styrende dokumentene for IKT-området.

Finanstilsynet tar styrets svar til etterretning.

3.4. IKT-drift – endringshåndtering

IKT-forskriften § 9 stiller krav om prosedyrer for avviks- og endringshåndtering. Prosedyrene for håndtering av endringer skal omfatte alle endringer som kan påvirke IKT-systemene og skal sikre forsvarlig, formell behandling og dokumentering av disse. Foretaket skal sikre at prosedyrene for endringshåndtering gir en stabil, planlagt og forutsigbar drift.

Finanstilsynet skrev i foreløpig tilsynsrapport at det bør rapporteres på utvikling i antall forhåndsgodkjente endringer og sammenheng med driftsstabilitet, samt at kontrollfunksjonene bør utføre kontroller for å sikre at kriterier for forhåndsgodkjenning er oppfylt. Finanstilsynet pekte videre på at foretakets endringsprosess bør inkludere kontroll av om en endring kan medføre behov for justering av beredskapsplanene.

Styret skriver i sitt svar at foretaket tar innspillene fra Finanstilsynet til etterretning og vil inkludere rapportering om utviklingen i antall forhåndsgodkjente endringer, samt sammenhengen mellom endringene og driftsstabiliteten. I forlengelsen av dette vil foretaket styrke oppfølgingen av forhåndsgodkjente endringer og påse at kontrollfunksjonene gjennomføre kontroller for å verifisere at kriteriene for forhåndsgodkjenning er oppfylt. Styret opplyser videre at foretakets endringshåndteringsprosess vil bli oppdatert, slik at vurdering av behov for justering av beredskapsplaner inngår i vurderingen.

Finanstilsynet tar styrets svar til etterretning.

3.5. Utkontraktering

I henhold til IKT-forskriften § 2 skal foretaket ha retningslinjer for å sikre at utkontraktert IKT-virksomhet oppfyller kravene i § 12. Dette gjelder blant annet krav til skriftlig avtale, der avtalen skal sikre foretakets rett til å kontrollere, herunder revidere leverandørens aktiviteter, samt Finanstilsynets tilgang til opplysninger og mulighet for å føre tilsyn hos IKT-leverandøren. Videre framgår det av § 12 at foretaket har ansvar for at IKT-virksomheten oppfyller alle krav som stilles i forskriften, og at dette også gjelder der hele eller deler av IKT-virksomheten er utkontraktert. Av bestemmelsene i § 13 framgår det at foretaket skal sikre at det har en samlet oppdatert dokumentasjon over organisasjon, utstyr, IKT-systemer og vesentlige forhold i IKT-virksomheten.

Finanstilsynet pekte i foreløpig tilsynsrapport på at desentralisert oppfølging av IKT-tjenester kan medføre ulik grad og kvalitet på oppfølging av den utkontraktede virksomheten, og at det derfor må sørges for at det er tilstrekkelig kompetanse og ressurser hos kontrakteier for å sikre god kvalitet på oppfølging av leverandører.

Styret skriver i sitt svar at foretaket anerkjenner viktigheten av tilstrekkelig kompetanse og ressurser for å sikre god kvalitet på oppfølging av utkontraktert IKT-virksomhet. Foretaket vil utvide standarder og rutiner for leverandørstyring for å sikre vurdering av når ansvar for utkontraktering av IKT bør sentraliseres. Styret opplyser videre at denne vurderingen skal gjennomføres ved avtaleinngåelse og deretter minst én gang årlig.

Finanstilsynet tar styrets svar til etterretning.

3.6. Beredskap

I IKT-forskriften § 11 framgår kravene til at foretaket skal ha en dokumentert kriseplan som skal kunne iverksettes dersom IKT-driften ikke kan opprettholdes som følge av en krise. Det skal minst

årlig gjennomføres opplæring, øvelse og testing av at kriseløsningen virker som forutsatt. Resultatet av testen skal dokumenteres.

Finanstilsynet pekte i foreløpig rapport på at ved testing av beredskapsplaner, både for foretakets egne og for utkontrakterte IKT-tjenester, må relevante informasjonssikkerhetsscenarioer inngå, der også verstefallsscenarioer er inkludert i beredskapstesting. Videre legges det til grunn at planverk for gjenoppbygging og alternativ drift testes og utføres i henhold til interne instruksjoner.

Styret presiserer i sitt svar at det er gjennomført grundige scenarioanalyser og stresstester av operasjonell risiko. Foretaket erkjenner imidlertid at det i mindre grad er gjennomført tester som spesifikt omfatter konsekvenser av alvorlige hendelser hos leverandører, og at sammenhengen mellom virksomhetens konsekvensanalyse og oppdatering av beredskapsplaner kan tydeliggjøres. Foretaket tar innspillene fra Finanstilsynet til etterretning og vil styrke beredskapstester ved å inkludere leverandørrelaterte scenarioer og vurdere behovet for testing av verstefallsscenarioer og gjenoppbyggingsevne. Foretaket vil også sikre at beredskapsplaner oppdateres i tråd med og at testgjennomføring fastsettes basert på virksomhetens konsekvensanalyse.

Finanstilsynet tar styrets svar til etterretning.

4. Videre oppfølging

Finanstilsynet ber om å motta kopi av protokollen fra styremøtet hvor Finanstilsynets tilsynsrapport blir behandlet.

Vi ber foretaket sende kopi av dette brevet til valgt revisor.

For Finanstilsynet

Olav Johannessen
seksjonsleder

Irene Støback Johansen
senior tilsynsrådgiver

Dokumentet er godkjent elektronisk.