FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

NORSK GJELDSINFORMASJON AS
Postboks 1343 Vika
0113 OSLO

VÅR REFERANSE	DERES REFERANSE		DATO
21/4834			29.11.2021

Tilsynsrapport

1. Generelt

Norsk Gjeldsinformasjon AS ("foretaket") har hatt tillatelse til å drive gjeldsinformasjons-virksomhet siden 26. juni 2021. Foretaket har tre ansatte.

Virksomheten reguleres av gjeldsinformasjonsloven med tilhørende forskrifter. Barne- og familiedepartementet har i tillegg gitt en veiledning om praktisering av gjeldsinformasjons-forskriften (31. januar 2019). Virksomheten er også omfattet av risikostyringsforskriften og IKT-forskriften. Gjeldsinformasjonsforetak skal kunne utlevere gjeldsopplysninger til den opplysningen gjelder (privatpersoner), til finansforetak og kommuner, til kredittopplysningsforetak for kredittvurderinger og kredittscoremodeller og til myndigheter for analyse- og statistikkformål.

Finanstilsynet har gjennomført tilsyn i foretaket. Hensikten med tilsynet var å vurdere foretakets IKT- og risikostyrings-systemer med særlig vekt på sikkerhet for at persondata ikke kommer på avveie og at gjeldsinformasjonen til enhver tid er korrekt og tilgjengelig for de som skal motta den.

Til grunn for denne tilsynsrapporten ligger Finanstilsynets foreløpige rapport datert 26. august 2021 og foretakets svar på denne av 23. september 2021.

2. IT-virksomheten

Forskrift nr. 147 / 2019 om bruk av informasjons- og kommunikasjonsteknologi (IKT).

IKT-forskriften omfatter IKT-systemer som er av betydning for foretakets virksomhet. For eksterne brukere av foretakets IKT-systemer skal det foreligge avtaler som sikrer at forskriftens krav til sikkerhet og dokumentasjon ivaretas.

IKT-forskriften § 5 stiller krav til at foretaket skal utarbeide prosedyrer som skal sikre beskyttelse av utstyr, systemer og informasjon av betydning for foretakets virksomhet mot skader, misbruk,

FINANSTILSYNET
Revierstredet 3
Postboks 1187 Sentrum
0107 Oslo

Telefon 22 93 98 00

post@finanstilsynet.no
www.finanstilsynet.no

Saksbehandler
Geir Haatveit
Dir. tlf **22 93 98 03**

uautorisert adgang og endring, samt hærverk. Videre skal prosedyrene inneholde retningslinjer for tildeling, endring, sletting og kontroll med autorisasjon for tilgang til IKT-systemene.

IKT-forskriften § 8 stiller krav til at drift av IKT-virksomheten skal være basert på dokumenterte prosedyrer, som sikrer fullstendig, rettidig og korrekt behandling og oppbevaring av data. IKT-systemer skal ha dokumenterte driftsløsninger som sikrer en tilgjengelighet i tråd med foretakets dokumenterte krav.

IKT-forskriften § 9 stiller krav til at foretaket skal sikre at prosedyrer for avviks- og endringshåndtering foreligger og følges. Prosedyrene for avvikshåndtering skal omfatte alle avvik som oppstår i driften av IKT-systemene. Operasjonelle hendelser eller sikkerhetshendelser som medfører vesentlig reduksjon i funksjonalitet som følge av brudd på konfidensialitet, integritet eller tilgjengelighet til IKT-systemer og/eller data skal uten ugrunnet opphold rapporteres til Finanstilsynet.

Det skal etableres prosedyrer som skal sikre at driftsavbrudd og katastrofeberedskap blir ivaretatt i samsvar med krav i IKT-forskriften § 11. Virksomheten skal ha egne kriseplaner, og det skal minst en gang årlig gjennomføres test for å sikre at kriseløsningen fungerer som forutsatt. Resultatet av testen skal dokumenteres, slik at det er mulig å kontrollere.

2.1 Kontroll av tilganger hos leverandør

I foreløpig rapport påpekte Finanstilsynet at foretakets rutiner for tilgangsstyring ikke beskriver handlinger for regelmessig kontroll av tilgangene til egne medarbeidere eller til medarbeidere hos leverandører, herunder priviligerte tilganger. For medarbeidere hos leverandører bør rutinen beskrive hvordan foretaket sikrer, gjennom bekreftelse eller rapportering fra leverandøren, at leverandøren regelmessig følger opp at medarbeideres tilgang til foretaket er i henhold til tjenstlig behov og minste privilegium.

Det kommer fram av foretakets tilsvar at foretakets rutiner for tilgangsstyring er oppdatert. Det er nå presisert i rutinene hvordan kontrollene skal utføres, herunder hyppighet, for å sikre at medarbeideres tilgang internt og eksternt er i henhold til tjenstlig behov.

2.2 Kvalitetskontroller

Finanstilsynet pekte i foreløpig rapport på at det er viktig at de daglige kvalitetskontrollene foretaket utfører for å avdekke manglende, mangelfulle eller feil data i leveransene fra finansforetakene, er dokumentert slik at flere kan være i stand til å utføre dem, og nøkkelmannsrisikoen reduseres. Finanstilsynet viste videre til at det er viktig at dokumentasjonen oppdateres i takt med at kompetansen på området øker og kontrollene justeres.

Foretaket har i sitt svar bekreftet at de har oppdatert rutinen som dokumenterer kontrollene av datakvaliteten og at rutinen vil bli oppdatert ved endringer i kontrollene. Foretaket har videre bekreftet at det har et høyt fokus på arbeidet med å videreutvikle kvalitetskontrollene for å styrke overvåkningen ytterligere.

I foreløpig rapport ba Finanstilsynet også foretaket redegjøre for om resultatet av de daglige kontrollene dokumenteres og lagres slik at man har en logg over avvik i datakvalitet.

Finanstilsynet har fra foretakets svar merket seg at all historikk lagres og er enkel å finne fram i. Foretaket har en dedikert e-postkasse for support som fungerer som en logg for dialogen med finansforetakene om feilhendelser.

2.3 Hendelsesrapportering til Finanstilsynet

Finanstilsynet pekte i foreløpig rapport på at foretaket ikke har beskrevet sin rapporteringsplikt etter IKT-forskriften § 9, i sine rutiner for driftsavvik eller avvikshåndtering.

Finanstilsynet har merket seg fra foretakets svar at hendelsesrapporteringen var beskrevet i noen av foretakets rutiner, men manglet i enkelte, og at disse nå er oppdatert.

3. Risikostyring og internkontroll

Forskrift nr. 1080 / 2008 om risikostyring og internkontroll.

Styret er ansvarlig for å påse at foretaket har en forsvarlig risikostyring og internkontroll i samsvar med forskrift nr. 1080 / 2008 om risikostyring og internkontroll. De viktigste elementene i et forsvarlig internkontrollsystem er *risikovurdering* med angivelse av konkrete risikoer, *rutiner* basert på risikovurderingen, og et system for *kontroll* av at rutinene følges, samt dokumentasjon av dette.

Etter forskrift om risikostyring og internkontroll § 6 skal foretaket løpende vurdere hvilke vesentlige risikoer som er knyttet til virksomheten. Risikovurdering er en systematisk identifisering og vurdering av konkrete risikoer, hvilken sannsynlighet det er for at forholdet inntreffer, og hvilken konsekvens dette vil ha for foretaket. Risikovurderingen danner grunnlaget for de rutiner foretaket må etablere, og brukes for å vurdere om eksisterende tiltak er gode nok, og for å identifisere områder hvor ytterligere tiltak må iverksettes for å redusere risikoen.

På bakgrunn av risikovurderingen skal det etableres rutiner. Videre skal daglig leder etter risikostyringsforskriften § 4 påse at risikostyringen og internkontrollen blir *gjennomført og overvåket* på en forsvarlig måte. Dette innebærer at det skal foreligge skriftlige rutiner for å kontrollere at arbeidsrutinene er blitt fulgt (*kontrollrutiner*). Kontrollrutinene skal angi hva som skal kontrolleres og kontrollens intensitet, og hvordan kontrollen skal gjennomføres. Rutinene kan være dynamiske, for eksempel slik at avvik på et område vil medføre forsterket kontroll i en periode. Avvik skal rapporteres til styret. Dokumentasjon av denne kontrollen og rapporteringen til styret må forefinnes skriftlig.

Foretakets risikovurdering og arbeidsrutiner ble mottatt i forbindelse med tilsynet, men foretaket ikke hadde etablert kontrollrutiner. Foretaket har i etterkant av tilsynet utarbeidet og oversendt kontrollrutiner. Finanstilsynet tar dokumentasjonen til etterretning.

For Finanstilsynet

Anne-Kari Tuv
Seksjonssjef

Olav Johannessen
seksjonssjef

Dokumentet er godkjent elektronisk og har derfor ikke håndskrevne signaturer.