FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

EXPERIAN GJELDSREGISTER AS
Postboks 5275 Majorstuen
0303 OSLO

VÅR REFERANSE	DERES REFERANSE		DATO
21/5133			29.11.2021

Tilsynsrapport

1 Generelt

Experian Gjeldsregister AS ("foretaket") er en del av Experian-gruppen. Foretaket har fire ansatte, og har siden 19. oktober 2018 hatt tillatelse til å drive gjeldsinformasjonsvirksomhet.

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 Finanstilsynet foreløpige rapport datert 26. august 2021 og foretakets svar på denne av 18. oktober 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, uautorisert adgang og endring, samt hærverk. Videre skal prosedyrene inneholde retningslinjer for tildeling, endring, sletting og kontroll med autorisasjon for tilgang til IKT-systemene.

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**

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

Finanstilsynet pekte i foreløpig rapport på at det ikke fremkommer av foretakets rutiner for tilgangsstyring at det gjøres regelmessig kontroll av tilgangene til egne medarbeidere eller medarbeidere hos leverandører, herunder privilegerte tilganger. For medarbeidere hos leverandører bør rutinen beskrive hvordan foretaket sikrer, gjennom bekreftelse eller rapportering fra leverandøren, at leverandøren regelmessig følger opp at medarbeideres tilganger er i henhold til tjenstlig behov og minste privilegium.

Foretaket har i sitt svar opplyst at det endrer sine rutiner i tråd med Finanstilsynets påpekning. Videre fremgår det at foretaket har avtalt med leverandørene at disse forplikter seg til regelmessig oppfølging av tilganger og rapportering av resultatet av oppfølgingen.

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.

Fra foretakets svar har Finanstilsynet merket seg at foretaket har dokumenterte beskrivelser av kvalitetskontrollene og logger fra kvalitetsoppfølgingen. Foretaket har nå utvidet dokumentasjon med frekvens og ansvarlig rolle slik at kontrollene ved behov enklere kan utføres av andre. Ved behov for nye eller forbedrede kvalitetskontroller, vil foretaket utvide eksisterende kontroller med disse fortløpende.

2.3 Hendelsesrapportering til Finanstilsynet

Finanstilsynet påpekte i foreløpig rapport at foretaket ikke har beskrevet sin rapporteringsplikt etter IKT-forskriften § 9 i sin rutine for avvikshåndtering.

Foretaket har i svaret opplyst at de aktuelle rutinene er oppdaterte og inkluderer nå rapportering til Finanstilsynet.

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.

3.1 Risikovurdering

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.

Risikovurderingen må utarbeides individuelt og konkret for virksomheten. Dersom foretaket benytter maler fra konsernledelse, franchisegiver, bransjeforeninger eller andre leverandører, skal risikovurderingen tilpasses virksomheten. Risikovurderingen skal være skriftlig, jf. forskrift om risikostyring og internkontroll § 8.

Finanstilsynet påpekte i den foreløpige rapporten at foretakets risikovurdering var mangelfull.

Finanstilsynet ba i varselet om dokumentasjon av foretakets internkontroll. Slik dokumentasjon ble ikke sendt inn, og foretaket hadde på tilsynstidspunktet ikke utarbeidet slik dokumentasjon.

Foretaket har i etterkant av det stedlige tilsynet utarbeidet ny risikovurdering for virksomheten, og en risikoanalyse av IKT-virksomheten. Finanstilsynet tar disse til etterretning.

3.2 Rutiner

På bakgrunn av risikovurderingen skal det etableres rutiner. For virksomheten til et gjelds-informasjonsforetak vil dette eksempelvis være rutiner for håndtering av henvendelser fra privatpersoner, rutiner for å avdekke og rapportere feil, oppfølging av leverandører, driftsrutiner osv.

Finanstilsynet påpekte i den foreløpige rapporten at det ikke forelå skriftlige arbeidsrutiner.

I sitt svar til den foreløpige rapporten har foretaket opplyst at det har hatt arbeidsrutiner som dekker sentrale forhold ved virksomheten, men at det på utvalgte områder er behov for å dokumentere disse i større grad. Imidlertid forstår Finanstilsynet foretakets kommentar slik at det fortsatt ikke er etablert skriftlige arbeidsrutiner.

3.3 Kontroll

Etter risikostyringsforskriften § 4 skal daglig leder 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 ett område vil medføre forsterket kontroll i en periode. Avvik skal rapporteres til styret. Dokumentasjon av denne kontrollen og rapporteringen til styret må forefinnes skriftlig, og kan f.eks. være kontrollrapporter hvor det fremgår hva som er kontrollert, om det er funnet avvik, samt dokumentasjon på hvordan eventuelle avvik er blitt fulgt opp.

Foretaket opplyste under det stedlige tilsynet at det ikke hadde skriftlige kontrollrutiner. Det ble gjennomført enkelte kontroller, men det var ikke skriftlig nedfelt *hva* som skulle kontrolleres, *hvor ofte* kontrollen skulle skje, eller *resultatet av kontrollen*.

Foretaket har i svaret til den foreløpige rapporten opplyst at det har etablert strukturert risikostyring, at det arbeides med å systematisere kontrollene ytterligere, og at dokumentasjon av kontrollen og rapportering til styret vil skje skriftlig. Finanstilsynet forstår imidlertid foretakets kommentar slik at arbeidet med å utarbeide skriftlige kontrollrutiner ikke er ferdigstilt.

3.4 Oppsummering, risikostyring og internkontroll

Finanstilsynet vurderte i den foreløpige rapporten at foretakets etterlevelse av risikostyrings-forskriften var mangelfull, og at foretaket ikke oppfylte kravene til risikoanalyse i IKT-forskriftens § 3. Finanstilsynet finner den manglende etterlevelsen på disse områdene kritikkverdig.

Foretaket har i etterkant av det stedlige tilsynet utbedret flere av manglene som ble påpekt under tilsynet og i den foreløpige rapporten. Ut fra foretakets svar forstår vi det likevel slik at dette arbeidet ikke er ferdigstilt.

Finanstilsynet forventer at foretaket ferdigstiller arbeidet med å oppfylle kravene i risikostyringsforskriften senest innen utgangen av året, og Finanstilsynet vil følge opp dette overfor foretaket tidlig i 2022, herunder be om å få oversendt revisors årlige bekreftelse til styret i medhold av risikostyringsforskriften § 10.

Kopi av tilsynsrapporten er sendt foretakets valgte revisor.

For Finanstilsynet

Anne-Kari Tuv
seksjonssjef

Olav Johannessen
seksjonssjef

Dokumentet er godkjent elektronisk og har derfor ikke håndskrevne signaturer.