



Gjeldsregisteret AS
Postboks 4
1330 FORNEBU

VÅR REFERANSE
21/2981

DERES REFERANSE

DATO
29.11.2021

Tilsynsrapport

1. Generelt

Gjeldsregisteret AS ("foretaket") er heleiet av TietoEvry AS, og har hatt tillatelse til å drive gjeldsinformasjonsvirksomhet siden 26. juni 2018. Foretaket har fire ansatte.

Virksomheten reguleres av gjeldsinformasjonsloven med tilhørende forskrifter. Barne- og familiedepartementet har i tillegg gitt en veiledning om praktisering av gjeldsinformasjonsforskriften (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 risikostyringssystemer 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 21. 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, 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 Kvalitetskontroller

Finanstilsynet pekte i foreløpig rapport på at foretaket manglet dokumentasjon på hvordan de utfører de daglige kvalitetskontrollene for å avdekke manglende, mangelfulle eller feil data i leveransene fra finansforetakene. Slik dokumentasjon er viktig for at flere kan være i stand til å utføre kontrollene, og for å redusere nøkkelmansrisikoen.

Foretaket har i sitt svar vist til at de har hatt daglige- og månedlige kontrollrutiner siden etableringen, og at det nå har utvidet sin rutinebeskrivelse med konkrete beskrivelser av hvordan de utfører den daglige kontrollen.

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.

Det fremgår av foretakets svar at daglig dokumentasjon av resultatet av kvalitetskontrollene foreligger siden etableringen, og at all kommunikasjon relatert til datakvalitet som foretaket har med finansforetakene, lagres.

2.2 Krise- og beredskapsplaner

Finanstilsynet påpekte i foreløpig rapport at foretaket ikke hadde gjennomført egen beredskapstest i 2020, og noterte seg at det skulle gjennomføres test i 2021 opp mot tjenesteleverandøren.

I svaret har foretaket bekreftet at det er planlagt å gjennomføre en krise- og beredskapsøvelse i oktober/november 2021. Finanstilsynet ber om å bli informert når foretaket har gjennomført krise- og beredskapsøvelsen i 2021.

2.3 Hendelsesrapportering

Finanstilsynet påpekte i foreløpig rapport at foretaket ikke har beskrevet sin rapporteringsplikt etter IKT-forskriften § 9 i sin rutine for avvikshåndtering. Finanstilsynet pekte videre på at det ikke er mottatt noen rapporter om IT-hendelser fra foretaket. Basert på foretakets innsendte dokumentasjon og informasjon som kom frem under tilsynsmøtet, oppfattet Finanstilsynet at det kan ha vært hendelser som kvalifiserer for rapportering til Finanstilsynet.

Foretaket har opplyst i sitt svar 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.

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 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.

Foretakets risikovurdering, rutiner, og kontrollrutiner ble oversendt i forkant av tilsynet, samt gjennomgått under tilsynsmøtet. Finanstilsynet tar dokumentasjonen og gjennomgangen til etterretning.

For Finanstilsynet

Anne-Kari Tuv
seksjonssjef

Olav Johannessen
seksjonssjef

Dokumentet er godkjent elektronisk og har derfor ikke håndskrevne signaturer.