



FINANSTILSYNET

THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

Høringsnotat

Forslag til endring av risikostyringsforskriften

SAKSNUMMER:

20/1148

11.05.2020

1. Innledning

De fleste foretak underlagt Finanstilsynets tilsyn er omfattet av forskrift om risikostyring og internkontroll (risikostyringsforskriften)¹, med enkelte unntak. Eksempelvis er ikke finansforetak underlagt risikostyringsforskriften fordi reguleringen som følger av finansforetaksloven går lenger enn de overordnede kravene som følger av risikostyringsforskriften.

Gjeldsinformasjonsforetakene er underlagt Finanstilsynets tilsyn, men er ikke omfattet av risikostyringsforskriften. Finanstilsynet foreslår at risikostyringsforskriften også gjøres gjeldende for gjeldsinformasjonsforetak.

2. Nærmere om gjeldsinformasjonsforetak

Et gjeldsinformasjonsforetak har tillatelse til å motta, innhente, registrere og utlevere gjeldsopplysninger.² Definisjonen omfatter både foretak som benytter tradisjonelle dataregistre og foretak som benytter spørretjenester eller portaler. Per i dag er det tre gjeldsinformasjonsforetak med konsesjon; Experian Gjeldsregister AS, Gjeldsregisteret AS og Norsk Gjeldsinformasjon AS. Disse foretakene oppbevarer og behandler opplysninger om enkeltpersoners usikrede gjeld eller ubenyttet kreditt.³ Formålet med opprettelsen av gjeldsinformasjonsforetak var å bidra til bedre og mer fullstendige kredittvurderinger, noe som kan bidra til å forebygge og begrense gjeldsproblemer blant enkeltpersoner.⁴ Gjeldsinformasjonslovens formål er å legge til rette for sikker, ordnet og effektiv registrering og utlevering av gjeldsopplysninger.⁵

Gjeldsinformasjonsforetakene innhenter og oppbevarer opplysninger om usikret gjeld og ubenyttet kreditt på personnivå, og utleverer disse til en nærmere definert krets i forbindelse med kredittvurderinger.⁶ Eksempelvis vil et finansforetak innhente opplysninger fra gjeldsinformasjonsforetakene i forbindelse med en konkret søknad om kreditt for å sikre at søkerens totale økonomiske situasjon er kartlagt. I tillegg kan opplysningene utleveres til bl.a. Norges Bank, Finanstilsynet, SSB og annen offentlig myndighet til analyse-, overvåknings-, statistikkformål, eller til andre for forskningsformål.⁷

Gjeldsinformasjonsloven har krav til internkontroll, som pålegger styret å fastsette retningslinjer for internkontroll og kontrollere at internkontrollen etableres, gjennomføres og dokumenteres på en forsvarlig måte i samsvar med styrets retningslinjer og pålegg.⁸ Videre skal daglig leder sørge for at internkontroll etableres og gjennomføres i henhold til lov og forskrifter. Det samme gjelder for styrets vedtatte retningslinjer og pålegg. I forarbeidene til gjeldsinformasjonsloven⁹ ble det vist til at formålet med loven og konsesjonsordningen i hovedsak var å ivareta personvern hensyn. Det ble videre vist til at kravet om bl.a. internkontroll skal bidra til å sikre en forsvarlig og trygg forvaltning av gjeldsopplysningene, som hindrer misbruk, kopling eller spredning av opplysninger til uvedkommende. Internkontrollkravet er ment å sikre at det etableres tilfredsstillende rutiner og klare ansvarsforhold for drift og organisering av foretakene. Det er imidlertid ingen krav til risikovurderinger med tilhørende dokumentasjon, avvikshåndtering, internrevisjon mv.

I tillegg er gjeldsinformasjonsforetak underlagt IKT-forskriften.¹⁰ Utover reguleringen av plikter knyttet til registrering og utlevering av gjeldsopplysninger, samt til taushetsplikt og sletting av opplysninger, er det ingen regulering av utøvelsen av gjeldsinformasjonsvirksomheten.

¹ FOR-1997-06-20-1057

² Gjeldsinformasjonsloven § 2 a).

³ Jf. § 2 d)

⁴ Prop. 87 L (2016-2017) pkt. 1

⁵ jf. § 1

⁶ jf. § 12 første ledd

⁷ jf. § 12 tredje og fjerde ledd

⁸ jf. gjeldsinformasjonsloven § 8 og gjeldsinformasjonsforskriften § 7

⁹ Prop. 87 L (2016-2017) pkt. 4.3.8.2

¹⁰ Gjeldsinformasjonsforskriften § 8

3. Om risikostyringsforskriften

Foretak under tilsyn skal innrette sin internkontroll etter de bestemmelser tilsynet fastsetter.¹¹ Finanstilsynet har med hjemmel i finanstilsynsloven gitt forskrift om gjennomføring av risikovurderinger og internkontroll, rapportering, krav om dokumentasjon mv. (risikostyringsforskriften).

Etter forskriften har styret det overordnede ansvaret for internkontrollen.¹² Dette samsvarer med kravene i gjeldsinformasjonsloven. Videre skal styret – etter risikostyringsforskriften – påse at foretaket har hensiktsmessige systemer for risikostyring og internkontroll. Styret skal fastsette prinsipper for risikostyring og internkontroll, og påse at risikostyringen og internkontrollen er gjennomført og overvåket. I forskriften er det fastsatt plikter for daglig leder, blant annet at vedkommende skal etablere en forsvarlig risikostyring og internkontroll på basis av en vurdering av aktuelle risikoer etter retningslinjer fastsatt av styret og påse at denne er dokumentert, gjennomført og overvåket på en forsvarlig måte.¹³ Minst én gang årlig skal det foretas en gjennomgang av vesentlige risikoer for alle virksomhetsområder, og det skal minst én gang årlig foretas en oppsummerende vurdering av om internkontrollen har vært gjennomført på en tilfredsstillende måte.¹⁴ Vurderingene skal dokumenteres og være tilgjengelige for Finanstilsynet i minst tre år.

Risikostyringsforskriften utdyper styrets og ledelsens ansvar utover det som følger av gjeldsinformasjonsregelverket, og fastsetter i tillegg minimumskrav til foretakets prosesser for – og dokumentasjon av – risikostyring og internkontroll.

4. Finanstilsynets vurdering

Finansforetakene plikter å rapportere opplysninger om enkeltpersoners usikrede gjeld og kredittrammer til gjeldsinformasjonsforetakene.¹⁵ Dette innebærer at gjeldsinformasjonsforetakene oppbevarer og behandler en vesentlig mengde sensitive opplysninger om enkeltpersoners økonomiske forhold. Det er i denne sammenheng helt avgjørende for forsvarlig virksomhetsstyring at foretakene identifiserer konkrete og generelle risikoer knyttet til denne virksomheten. Spesielt er det viktig at opplysningene behandles i samsvar med de strenge og omfattende reglene som følger av personopplysningsloven og personvernforordningen. Foruten det åpenbare behovet for korrekt behandling med tanke på personvern, er det også helt nødvendig for en forsvarlig kredittvurdering at mottakere av informasjonen kan stole på at denne er korrekt, tidsriktig og komplett.

Det er i denne forbindelse en rekke risikoer for feil. Foruten større sikkerhetsbrudd i IT-systemene, er det risiko for brudd på taushetsplikt, at sletting ikke skjer i samsvar med reglene, at opplysninger gis på feil grunnlag eller til feil mottaker, feilregistrering av opplysninger, at foretakene driver annen virksomhet som er egnet til å svekke tilliten til foretakets uavhengighet mv. Disse risikoene er det viktig at foretakene identifiserer, og at det opprettes hensiktsmessige systemer, rutiner og tiltak for å forebygge dem.

Det er dermed gode grunner til å innlemme gjeldsinformasjonsforetakene i risikostyringsforskriften. Etter Finanstilsynets vurdering bør det, i tillegg til krav om risikovurderinger, være krav til å fastsette adekvat avvikshåndtering der risikoer forekommer. Det bør også være krav til internrevisjon/revisorbekreftelse for å påse at gjeldsinformasjonsforetakenes internkontroll fungerer etter sin hensikt. For foretakene vil dette innebære at internkontrollen blir plassert i et større og mer detaljert rammeverk for en helhetlig risikostyring, med klare ansvarsfordelinger. Etter Finanstilsynets syn vil dette redusere risikoen for avvik og bidra til forsvarlig virksomhetsutøvelse. Fra et tilsynsmessig ståsted vil dokumentasjonskravene bety at Finanstilsynet får tilgang på verdifull informasjon om bl.a. hvordan foretaket vurderer eksisterende og nye risikoer, om hvilke typer avvik og feil som avdekkes og hvordan virksomheten følger opp og behandler dette.

¹¹ Finanstilsynsloven § 4 første ledd nr. 2

¹² Risikostyringsforskriften § 3

¹³ Risikostyringsforskriften § 4

¹⁴ Risikostyringsforskriften §§ 7 og 8

¹⁵ Gjeldsinformasjonsloven § 10

Det er Finanstilsynets erfaring at risikostyringsforskriften i de fleste tilfeller gir en hensiktsmessig og fleksibel regulering av risikostyringen og internkontrollen i foretakene under tilsyn. Kravene innebærer at foretakene gis et bedre grunnlag for å avdekke svakheter og feil i virksomhetsutøvelsen for derigjennom å iverksette forebyggende eller korrigerende tiltak. Det foreligger lang tilsynspraksis med denne reguleringen, og sammen med dokumentasjonskravene som følger av forskriften, bidrar dette til å effektivisere tilsynsarbeidet. Det er derfor Finanstilsynets oppfatning at gjeldsinformasjonsforetakene bør være underlagt reguleringen i risikostyringsforskriften.

5. Økonomiske og administrative konsekvenser

Det er vanskelig å forutse hvilke konsekvenser forslaget vil ha for foretakene. På den ene siden fordrer det allerede eksisterende kravet til internkontroll at foretakene har gjort forutgående risikovurderinger for å vite hvordan internkontrollen skal være utformet og gjennomføres. Dette bør tilsi at forslaget om å omfatte foretakenes virksomhet i risikostyringsforskriften ikke medfører større endringer for foretakene.

På den andre siden vil de mer detaljerte reglene til risikostyringen kunne bety at gjeldsinformasjonsforetakene må innhente kompetanse utenfra. Dette vil kunne medføre økte kostnader, som Finanstilsynet ikke har forutsetninger for å tallfeste. I tillegg legger Finanstilsynet til grunn at krav om internrevisjon/revisorbekreftelse vil medføre en kostnad, men at denne er av mindre vesentlig størrelse.

6. Forslag til endring i forskrift 20. juni 1997 nr. 1057 om risikostyring og internkontroll

§ 1 skal lyde:

§ 1. Virkeområde

Forskriften gjelder for

1. Regulerte markeder
2. Verdipapirforetak
3. Forvaltningsselskaper for verdipapirfond
4. Pensjonsforetak
5. Oppgjørssentraler
6. Verdipapirregistre
7. Betalingsforetak og opplysningsfullmektiger
8. E-pengeforetak
9. Forsikringsformidlingsvirksomhet
10. Eiendomsmeglingsforetak
11. Inkassoforetak
12. Regnskapsførerselskaper
13. *Gjeldsinformasjonsforetak.*

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]