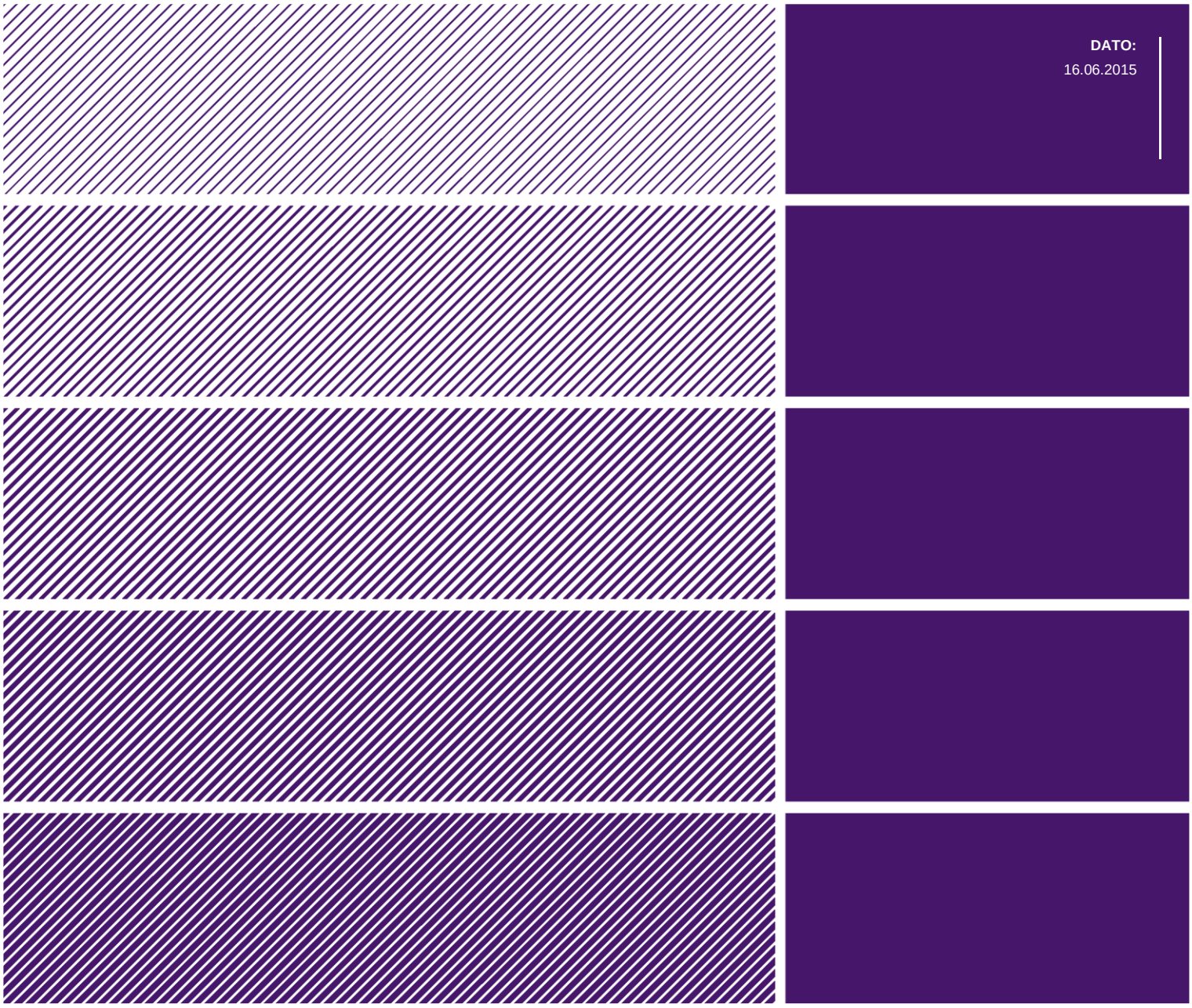
FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

Forslag til nytt regelverk på området for betalingstjenester og finansforetakenes bruk av informasjons- og kommunikasjonsteknologi (IKT)

Høringsnotat og forskriftsforslag



DATO:
16.06.2015

1. Innledning

Etter finanstilsynsloven er det med virkning fra 1. juli 2014 gitt regler om utkontraktering av IKT-virksomhet fra foretak under tilsyn samt Finanstilsynets mulighet til å gripe inn mot dette. Da Finanstilsynet foreslo denne regelendringen overfor Finansdepartementet, ble det også vist til at tilsynet i medhold av betalingssystemloven, ville vurdere å stille nærmere krav til sikkerhet i systemene for betalingstjenester.

Utviklingen på betalingssystemområdet og finansforetakenes bruk av IKT-tjenester gjør det krevende for foretakene å opprettholde og sikre et akseptabelt risikonivå. Kriminell aktivitet rettet mot betalingstjenester som er distribuert digitalt, utgjør del av risikobildet. Økt kompleksitet, både når det gjelder grunnleggende IKT-infrastruktur og betalingstjenester som baseres på ulike teknologier og operatører, kan være utfordrende.

Også innenfor EU har disse utviklingstrekkene fått oppmerksomhet, og EBA (European Banking Authority) har etablert retningslinjer for sikkerhet for internettbetalinger som vil bli gjort gjeldende fra 1. august 2015. Retningslinjene bygger på retningslinjer utarbeidet av SecuRe Pay[1] .

På dette grunnlag mener Finanstilsynet det er behov for å styrke generelle system- og sikkerhetskrav til betalingssystemer. Det foreslås derfor forskriftsbestemmelser om dette. Det vises til nærmere omtale i punkt 2.2.

Finanstilsynet har gjennom tilsynsvirksomheten erfart at iverksettelse og utkontraktering av IKT-prosjekter med vesentlig betydning for foretakenes virksomhet og med potensielt stor risiko har vært gjennomført uten at foretakets styre har vært direkte involvert i beslutningen. Dette anses ikke å være i samsvar med god virksomhetsstyring. På denne bakgrunn foreslås det en ny bestemmelse i forskrift om bruk av informasjons- og kommunikasjonsteknologi (IKT-forskriften) om at styret skal behandle avtaler om utkontraktering av IKT-virksomhet og endringer i slike avtaler.

I tillegg foreslås det at unntak for hendelsesrapportering etter IKT-forskriften oppheves for pensjonskasser og inkassoselskaper samt enkelte redaksjonelle endringer i forskriften for øvrig. Forslaget er nærmerer omtalt i punkt 2.1.

[1] European Forum on the Security of Retail Payments etablert i 2011 av ECB (The European Central Bank) som et frivillig samarbeidsforum for tilsynsmyndigheter på betalingssystemområdet. (http://www.ecb.europa.eu/press/pr/date/2014/html/pr140204.en.html)

2. Forslag til regelverksendringer

2.1 Forskrift om bruk av informasjons- og kommunikasjonsteknologi (IKT-forskriften)

IKT-forskriften § 2 omhandler utkontraktering av IKT-virksomhet, og lyder:

> *Foretaket skal fastsette overordnede mål, strategier og sikkerhetskrav for IKT-virksomheten. Det skal foreligge beskrivelse av den enkelte prosess og hvordan ansvaret for administrasjon, anskaffelse, utvikling, drift, systemvedlikehold, sikring av informasjon og avvikling utføres på en betryggende måte.*
>
> *Ved utkontraktering av deler eller hele IKT-virksomheten skal foretaket ha egne retningslinjer som skal sikre leveransen.*
>
> *Det skal oppnevnes en ansvarlig i foretaket for de ulike deler av IKT-virksomheten. Med ansvarlig menes en funksjon eller stilling.*

Finanstilsynet foreslår at bestemmelsen utvides med et krav om at utkontraktering av IKT-virksomhet, eller endring av denne, skal godkjennes av styret før gjennomføring. Erfaring fra tilsynvirksomheten har avdekket at utkontraktering av IKT-aktiviteter er gjennomført uten styrets involvering, også for aktiviteter som Finanstilsynet mener representerer høy risiko for virksomheten. Etter forslaget skal styret forelegges planer for utkontrakteringen med risikovurdering, og en beskrivelse av hvordan leveransene skal kontrolleres. Styrets behandling skal sikre at beslutninger om utkontraktering av viktig virksomhet er forankret i foretakets øverste ledelse. IKT-forskriften omfatter kun systemer av betydning for foretakets virksomhet. Det vises for øvrig til de nye bestemmelsene i finansieringsvirksomhetsloven § 2-17a og finanstilsynsloven § 4c.

IKT-forskriften definerer krav når det gjelder foretakenes IKT-virksomhet. Siden den trådte i kraft i 2003, har forskriften vært et viktig verktøy for foretakene under tilsyn og i Finanstilsynets oppfølging av foretakene. Utviklingen innenfor IKT siden 2003 har medført et behov for å oppdatere forskriftens formuleringer til dagens praksis. Dette gjelder særlig forholdet mellom forskriftens § 8 Drift og § 10 Krav til kontinuitet. Tilgjengelighet, eller kontinuitet, til systemene vurderes å være en integrert del av kravene som stilles til den ordinære driften av systemene. For å bedre gi forskriften en struktur som er tilpasset dagens syn på oppbygning av IT-systemer, foreslås det at forskriftens § 10 utgår og erstattes med et nytt ledd i § 8 om driftskrav. Endringen innebærer ingen materielle endringer i de krav som stilles til foretakens systemer.

I tillegg foreslås det en mindre endring i § 9 om avviks- og endringshåndtering, ved at unntaket for foretak som nevnt i § 1 første ledd nr. 5 (Private, kommunale og fylkeskommunale pensjonskasser) og inkassoselskaper om rapportering av hendelser fjernes. Begrunnelsen for dette er at alvorlige IKT-hendelser også for denne typen foretak er viktig å bli kjent med for tilsynsmyndigheten, både for å vurdere risiko, men også for å sikre nødvendige korrektive tiltak.

Videre foreslås det at betalingsforetak omfattes av forskriften. Det antas at det er en inkurie som har medført at denne foretaksgruppen ikke tidligere er ført opp på listen over foretak som omfattes av IKT-forskriften

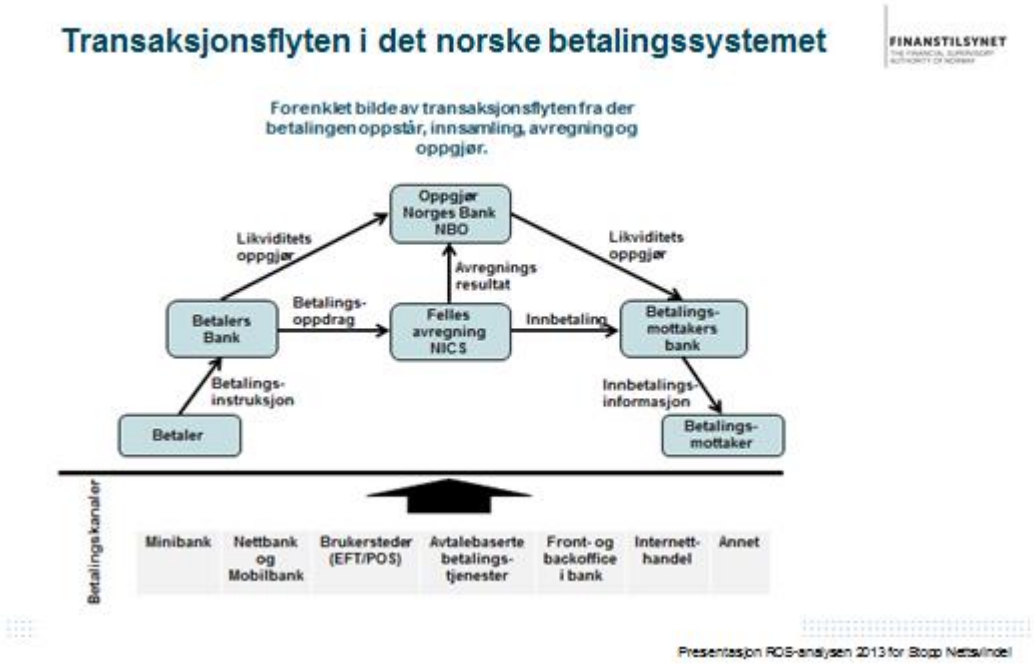
Samtidig foreslås også enkelte språklige presiseringer og endringer uten materiell betydning i forskriften for øvrig. Særskilt nevnes at det i ny § 11 (tidligerer § 12) presiseres at foretakene

skal ha anledning til å gjennomføre revisjon av leverandør. Dette antas imidlertid å være dekket av gjeldende ordlyd om adgang til å gjennomføre inspeksjon og kontroll.

2.2 Betalingssystemloven mv. (bsl.)

Betalingssystemloven er et rammeverk for bl.a. etablering av og tilsyn med betalingssystemer. Som systemer for betalingstjenester regnes systemer for overføring av penger fra eller mellom banker eller andre som kan yte betalingstjenester etter, jf. lovens § 1-1.

Systemer for betalingstjenester omfatter de tjenester som fremgår under den sorte horisontale streken i figuren under:



Kun institusjoner med konsesjon til å yte betalingstjenester kan drive systemer for betalingstjenester. Forskriftsforslaget retter seg derfor til banker og andre kredittinstitusjoner, betalingsforetak, e-pengeforetak mv., jf. finansieringsvirksomhetsloven § 4b-1 første ledd. I tillegg til norske foretak, mener Finanstilsynet at kravene bør omfatte norske filialer av EØS-foretak. Allmenne hensyn tilsier at alle systemer for betalingstjenester i Norge har felles, høy grad av sikkerhet. Anvendelsen av slike krav også for utenlandske foretak som driver virksomhet i Norge anses derfor i samsvar med "general good-læren" i EU.

Drift av betalingssystemene (den IT-teknisk delen) har tradisjonelt vært utkontraktert til særselskaper, men slik at den konsesjonspliktige betalingstjenesten ble utført av bankene. Foretakene som opererer den tekniske delen av systemer for betalingstjenester er ikke underlagt tilsyn, men betalingssystemet som sådan er under tilsyn av Finanstilsynet. Finanstilsynet har hjemmel til å gi pålegg om retting overfor den institusjon som driver systemet, dersom tilsynet finner at systemet ikke innrettes eller drives i samsvar med bestemmelser fastsatt i eller i medhold av lov.

Betalingssystemloven oppstiller visse overordnede krav om sikkerhet og effektivitet i betalingssystemene. Den nærmere reguleringen av felles systemer på betalingsområdet har

tradisjonelt foregått gjennom avtaler i banksektoren. Denne selvreguleringen er dokumentert i den såkalte "Blåboka", og omfatter en rekke områder knyttet til felles operativ infrastruktur (FOI) og felles betalingstjenester, for eksempel BankAxept.

Selvregulering kan være et effektivt virkemiddel, både for å sikre lik håndtering av felles tjenester, men også for å sikre utvikling av regelverk der endringene skjer hyppig og samtidig være tilstrekkelig detaljerte utover det som det kan være hensiktsmessig i en myndighetsfastsatt regulering.

Det har imidlertid vist seg, blant annet gjennom erfaringer fra tilsynvirksomheten, at det ikke i tilstrekkelig grad er etablert kontroll med etterlevelse av selvreguleringen (Blåboka). Det er derfor etter Finanstilsynets vurdering nødvendig å stille enkelte krav for å sikre etterlevelse av regelverket, samtidig som visse minstekrav til sikkerhetsløsninger for betalingstjenester bør etableres for å ivareta den økte risikoen som følge av utviklingen på betalingssystemområdet, jf. over.

Forslaget vil også ivareta retningslinjer for sikkerhet for internettbetalinger som EBA (European Banking Authority) har utarbeidet og som vil bli gjort gjeldende fra 1. august 2015[2]. Retningslinjene er ment for nasjonale tilsynsmyndigheter for å kunne følge opp anbefalinger utarbeidet av SecuRe Pay, et forum under den Europeiske sentralbanken, om sikkerhet for elektroniske betalingsløsninger.

Finanstilsynet foreslår derfor at det med hjemmel i bsl. § 3-3 fastsettes systemkrav til betalingssystemer som beskrives nedenfor.

Infrastruktur og felles betalingstjenester

Krav om sikker og effektiv betaling følger av bsl. § 3-1. Vesentlige endringer i risikobildet for felles infrastruktur (i bankenes egenregulering definert som felles operativ infrastruktur (FOI)) og/eller felles betalingstjenester avtalt mellom foretakene kan representere en økt risiko og med fare for alvorlige konsekvenser. Eksempel på endringer kan være etablering av ny betalingstjeneste, vesentlig endring av nåværende betalingstjeneste, flytting av prosessering, endret lagring av data eller flytting av infrastruktur ut av Norge. Slik endring skal meldes Finanstilsynet som følge av meldeplikten, jf. bsl. § 3-2.

Meldeplikten etter bsl. § 3-2 er nærmere beskrevet i Finanstilsynets rundskriv nr. 17/2004. Det vises i denne sammenheng til ny § 4c i Finanstilsynsloven om meldeplikt ved utkontraktering av tjenester fra institusjoner under tilsyn, som særlig på betalingsområdet vil overlappe med det som omfattes av meldeplikten etter lov om betalingssystemer. Unntak fra meldeplikt er gitt i forskrift av 5. juni 2015 nr 613[3].

Det foreslås at risikovurderinger skal gjennomføres som en del av beslutningsgrunnlaget før ny teknologi introduseres. IKT-forskriften § 3 inneholder krav om årlig risikovurdering. Det foreslåtte kravet går lenger enn IKT-forskriften ved å kreve løpende risikovurderinger, men kun for betalingssystemer, for at for eksempel sikkerhetshull skal kunne oppdages så tidlig som mulig etterhvert som de måtte oppstå.

[2] http://www.eba.europa.eu/regulation-and-policy/consumer-protection-and-financial-innovation/guidelines-on-the-security-of-internet-payments/-/regulatory-activity/press-release

[3] http://www.finanstilsynet.no/no/Artikkelarkiv/Aktuelt/2015/2_kvartal/Unntak-fra-meldeplikt-ved-utkontraktering-av-virksomhet-/

Krav til betalingsløsninger betjent av kunde
Betalingstjenester er i dag i vesentlig omfang distribuert ut til kunder enten via lukkede eller åpne nett til bl.a. egen datamaskin og mobile enheter, til fysiske betjeningssteder tilknyttet banken (minibanker), til betalingsterminaler på fysiske brukersteder (POS) og brukersteder på nettet.

Finanstilsynet foreslår at foretakene skal gjennomføre løpende risikoanalyser, jfr over, for å sikre at løsningene foretaket tilbyr kundene har et tilstrekkelig sikkerhetsnivå og at transaksjoner som utføres over nettet er tilstrekkelig sikret med hensyn til konfidensialitet, integritet og tilgjengelighet.

Ved selvbetjening av betalingstjenester foreslås det at foretaket skal sørge for en sikker påloggingsmekanisme, og det skal etableres en sterk autentiseringsløsning med bruk av flere uavhengige faktorer. Trafikk som går over åpne nett, skal være kryptert. Kryptografien som brukes skal være av internasjonalt akseptert standard.

Foretaket skal etter forslaget ha etablert overvåkning og måling av trafikken av betalingstjenestene som tilbys elektronisk for å kunne oppdage uønsket trafikk eller manipulering så tidlig som mulig for å avverge kriminalitet og alvorlige hendelser. Foretaket skal også sikre at mobile betalingsløsninger skal ha minst tilsvarende sikkerhet som for tradisjonell nettbaserte løsninger.

Det er viktig at foretaket sikrer at det er tilstrekkelig sikkerhet i kortbetalingsløsninger og nettverket som benyttes. Det foreslås derfor en presisering i forskriften av at minibanker og betalingsterminaler skal ha løsninger som skal sikre mot uautorisert bruk, for eksempel forsøk på å avlese koder ved hjelp av ulovlig påmonterte enheter. Videre skal utstyret i størst mulig grad skjerme inntasting av kode mot uønsket innsyn. Løsningene skal minimum følge internasjonale anerkjente standarder.

Etterlevelse av regelverk
Det må etableres system for å sikre etterlevelse av gjeldende regelverk, både egenregulering og myndighetsregulering gjennom foretakets internkontroll.

3 Vurdering av økonomiske og administrative konsekvenser av forslagene

EBA har i 2015 kommet med retningslinjer for sikkerhet for internettbetalinger, som vil tre i kraft 1. august 2015, og disse vil få anvendelse for norske foretak. Den foreslåtte forskrift er i tråd med EBA sine retningslinjer.

Det er Finanstilsynets vurdering at etablerte betalingsløsninger i stor grad oppfyller kravene som foreslås forskriftsfestet. Forskriftsbestemmelsen vil særlig ha betydning for nye betalingstjenester og/eller nye tjenesteleverandører. Nettbutikker som ikke har "3D Secure"-løsninger (2-faktor identifisering) vil indirekte måtte tilpasse seg gjennom bankene som omfattes av forslaget. Tilsvarende må tilbydere som bare har betalingskort med magnetstripe heve sikkerhetsnivået.

Kostnader ved økt sikkerhetsnivå vil etter tilsynets vurdering oppveies av ulempene og kostnadene som kan oppstå som følge av et økende trusselbilde / kriminell virksomhet. I

tillegg til den løpende tilsynsvirksomheten, er det vanskelig å se andre alternative tiltak som er bedre egnet for å sikre kvaliteten og tilliten til betalingssystemene.

Forslaget til endring av IKT-forskriften antas ikke å ha vesentlige økonomiske og administrative konsekvenser. Styrets arbeidsbelastning vil kunne øke, men antas å bidra til å forebygge risiko for alvorlig svikt i sentral infrastruktur.

4 Forslag til forskrift og forskriftsendringer

I

Endringer i IKT-forskriften

§ 1, nytt punkt 13 skal lyde:

13. Betalingsforetak

Tidligere punkt 13 blir nytt punkt 14 osv.

§ 2, skal lyde:

Foretaket skal fastsette overordnede mål, strategier og sikkerhetskrav for IKT-virksomheten. Det skal foreligge beskrivelse av den enkelte prosess og hvordan ansvaret for administrasjon, anskaffelse, utvikling, drift, systemvedlikehold, sikring av informasjon og avvikling utføres på en betryggende måte.

~~Ved utkontraktering av deler eller hele IKT-virksomheten skal~~ F~~f~~oretaket skal ha ~~egne~~retningslinjer som skal sikre at utkontraktert IKT-virksomhet oppfyller kravene i § 12.~~leveransen.~~

Det skal oppnevnes ~~en~~ansvarlige i foretaket for de ulike deler av IKT-virksomheten. Med ansvarlig menes en funksjon eller stilling.

Avtaler om utkontraktering av IKT-virksomhet og endringer i slike avtaler skal behandles av styret. Styret skal forelegges planer for utkontrakteringen, med risikovurdering, og en beskrivelse av hvordan foretaket skal sikre leveransen.

§ 8 skal lyde:

Drift~~en~~ av IKT-virksomheten skal være basert på dokumenterte prosedyrer, som sikrer fullstendig, rettidig og korrekt ~~dataproduksjon,~~ behandling og oppbevaring av ~~produksjons~~data ~~samt tilgjengelighet av IKT-systemene.~~

IKT-systemer skal ha dokumenterte driftsløsninger som sikrer en tilgjengelighet i tråd med foretakets dokumenterte krav. Det skal gjennomføres regelmessige analyser og tiltak for å motvirke avvik i IKT-systemene eller deres omgivelser, som påvirker oppnåelse av foretakets dokumenterte krav.

Foretaket skal teste og dokumentere at driften fungerer i henhold til foretakets dokumenterte krav.

§ 9, tredje ledd, siste punktum, skal lyde:

Foretak som nevnt i § 1 første ledd ~~nr. 5 (Private, kommunale og fylkeskommunale pensjonskasser og pensjonsfond), nr. 11 (Inkassoforetak) og~~ nr. 12 (Eiendomsmeglerforetak) omfattes ikke av kravet til hendelsesrapportering.

§ 10 oppheves

§ 11 blir ny § 10 som skal lyde:

§ 10 Driftsavbrudd og krise~~atastrofe~~beredskap

Foretaket skal ha en dokumentert krise~~atastrofe~~plan som skal iverksettes dersom IKT-driften ikke kan opprettholdes som følge av en krise~~atastrofe~~. Med krise~~atastrofe~~ menes hendelser som forårsaker driftsavbrudd slik at foretakets IKT-drift ikke kan fortsette med normalt tilgjengelige ressurser.

krise~~atastrofe~~planen skal minst omfatte

- oversikt over IKT-systemer som inngår i ~~katastrofe~~planen
- beskrivelse av krise~~atastrofe~~løsningen
- klare kriterier for oppstart av krise~~atastrofe~~løsningen
- akseptabel lengde på et driftsavbrudd før krise~~atastrofe~~løsningen iverksettes
- prosedyrer som inneholder de nødvendige aktiviteter for å gjenopprette IKT-driften
- oversikt over ansvarsforhold og prosedyrer ved oppstart av krise~~atastrofe~~løsningen
- informasjon til berørte ansatte, leverandører, kunder, offentlige myndigheter og media.

Det skal minst en gang årlig gjennomføres opplæring, øvelse og testing ~~i et omfang som gir tilstrekkelig trygghet for~~ av at krise~~atastrofe~~løsningen virker som forutsatt. Resultatet av testen skal dokumenteres ~~slik at det er mulig å kontrollere~~.

§ 12 blir ny § 11. § 11 første ledd skal lyde:

Foretaket har ansvar for at IKT-virksomheten oppfyller alle krav som stilles etter denne forskrift. Dette gjelder også der hele eller deler av IKT-virksomheten er utkontraktert. Det skal foreligge en skriftlig avtale som sikrer dette. Avtalen må sikre at foretak under tilsyn også gis rett til å ~~inspisere og~~ kontrollere, *herunder revidere* de av leverandørens aktiviteter som er knyttet til avtalen. Avtalen skal også sikre håndtering av taushetsbelagt informasjon.

II

Forskrift om systemer for betalingstjenester med hjemmel i betalingssystemloven § 3-3:

§ 1 virkeområde

Forskriften gjelder for banker, kredittinstitusjoner, e-pengeforetak, betalingsforetak og filialer av slike foretak med hovedsete i annen stat som omfattes av Det europeiske økonomiske samarbeidsområde (EØS).

§ 2 Risikovurdering og etterlevelse av regelverk

Foretak som tilbyr elektroniske betalingstjenester skal løpende gjennomføre risiko- og sårbarhetsanalyser for å sikre tilstrekkelig sikkerhetsnivå. Risiko- og sårbarhetsanalyser skal gjennomføres som en del av beslutningsgrunnlaget før en ny betalingstjeneste lanseres og ved hendelser eller endringer av betydning for sikkerhetsnivået.

Foretaket skal etablere system for å sikre etterlevelse av gjeldende regelverk, bransjens selvregulering og interne rutiner.

§ 3 Sikkerhetskrav

Foretaket som tilbyr elektroniske betalingstjenester skal etablere tiltak for å sikre nødvendig konfidensialitet, integritet og tilgjengelighet for tjenestene. Gjeldende nasjonale standarder og internasjonalt anerkjente standarder skal følges.

Foretaket skal beskytte tjenesten i sin helhet (ende til ende) ved hjelp av logiske og fysiske sikringstiltak. Kommunikasjon over åpne nett, herunder internett og telenett, skal være kryptert. Foretakets risiko- og sårbarhetsvurdering skal legges til grunn for å avklare behov for tiltak.

For autentisering av kunden skal foretaket ha en sikker påloggingsmekanisme.

Foretaket skal sikre at utlevering av identitetskjennetegn skjer på betryggende måte. Videre skal foretaket sikre at kunden på en hensiktsmessig måte kan beskytte sine identitetskjennetegn, og foretaket skal etablere løsninger som gjør at kunden kan sperre videre bruk av identitetskjennetegnene.

Foretaket skal overvåke og måle datatrafikk for betalingstjenester for å kunne avdekke og hindre uautorisert bruk av tjenesten.

FINANSTILSYNET
Postboks 1187 Sentrum
0107 Oslo
POST@FINANSTILSYNET.NO
WWW.FINANSTILSYNET.NO