FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

Veiledning i etterlevelse av IKT-forskriften for eiendomsmeglingsforetak

DATO:
15.04.2016

MOTTAKERE:
EIENDOMSMEGLINGSFORETAK

Innhold

1 Innledning

Finanstilsynet har i 2016 laget en ny veiledning for eiendomsmeglingsforetakene. Samtidig er det laget en tilsynsmodul med kontrollspørsmål spesielt rettet mot eiendomsmeglingsforetakene. Veiledningen erstatter Finanstilsynets veiledning for etterlevelse av IKT-forskriften for mindre foretak fra 2006.

2 Veiledning til paragrafene i IKT-forskriften

2.1 § 2. Planlegging og organisering

"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.

Foretaket skal ha retningslinjer som skal sikre at utkontraktert IKT-virksomhet oppfyller kravene i § 12.

Det skal oppnevnes 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."

Eiendomsmeglingsforetakets IKT-strategi skal vise hvordan IKT-virksomheten understøtter forretningsvirksomheten i å nå foretakets mål. IKT-strategien skal beskrive valg av systemløsninger og utkontrakteringspartnere. Dette gjelder både meglersystem og oppgjørssystem, samt driftsløsninger lokalt og for eksterne kontraktsmedhjelpere. Valg av strategisk og operasjonelt samarbeid med system- og driftsleverandørene er en sentral del av IKT-strategien.

Foretaket skal utnevne ansvarlige for IKT-virksomheten. IKT-ansvarlig skal ha en stillingsbeskrivelse som beskriver oppgaver og ansvar. Aktuelle ansvarsområder for IKT-ansvarlig er oppfølging av system- og driftsleverandører, oppfølging ved nye systemversjoner, oppgaver knyttet til tilgangsstyringen, IKT-sikkerhet og lokal drift.

2.2 § 3. Risikoanalyse

"Foretaket skal fastsette kriterier for akseptabel risiko forbundet med bruk av IKT-systemene.

Foretaket skal ha en dokumentert prosess for gjennomføring av risikoanalyser av IKT-virksomheten. Prosessen skal blant annet definere klare ansvarsforhold og omfatte oppfølging av tiltak som iverksettes som et resultat av den gjennomførte risikoanalysen.

Foretaket skal minst en gang årlig, eller ved endringer som har betydning for IKT-sikkerheten, gjennomføre risikoanalyser for å påse at risiko styres innenfor akseptable grenser i forhold til foretakets virksomhet. Resultatet av risikoanalysen skal dokumenteres."

Når risiko skal identifiseres og vurderes, bør det tas utgangspunkt i begrepene tilgjengelighet, konfidensialitet og integritet:

- systemløsningene skal være driftssikre
- saksbehandlingen skal være riktig i henhold til juridisk regelverk, egne rutiner og avtalen med kunden
- dataene skal være beskyttet mot uautorisert innsyn og endring

Det er nyttig å stille seg spørsmålene Hvilke sårbarheter og hvilke trusler kan ramme tjenestene? Hva er konsekvensene hvis de rammes?

Det kan være organisatoriske risikoer, systemmessige risikoer og tekniske risikoer.

Det er eiendomsmeglingsforetaket selv som skal vurdere risikoen knyttet til IKT-virksomheten. Dette kan ikke overlates til en leverandør. Det vil imidlertid være nødvendig å innhente leverandøren(e)s risikoanalyse slik at den kan inngå som en del av grunnlaget for den samlede risikoanalysen av IKT-virksomheten i foretaket.

Resultatet av risikoanalysen skal dokumenteres. For identifiserte tiltak må det fremgå hvem som er ansvarlig for å iverksette dem og frister for å utføre dem. Det bør benyttes et skjema som er enkelt å følge opp.

Risikoanalysen i henhold til IKT-forskriften kan inngå som en del av risikoanalysen i henhold til internkontrollforskriften[1].

Eksempel på risiko for ikke å etterleve juridiske krav:

Nytt krav i eiendomsmeglingsloven fra 2014 om skriftlig dokumentasjon av alle bud, initierte utvikling av app'er for budgivning. Imidlertid er løsningen avhengig av at nettverk m.m. fungerer, og det er korte marginer for forsinkelse. Det er en risiko knyttet til at bud ikke blir formidlet fordi app'en ikke fungerer som den skal.

2.3 § 4. Kvalitet

"Foretaket skal fastsette kvalitetsmål for de enkelte deler av IKT-virksomheten knyttet opp mot foretakets øvrige mål. Foretaket skal ha dokumenterte prosedyrer for oppfølging av fastsatte kvalitetsmål."

IKT-virksomheten skal fungere tilfredsstillende som støtte for beslutninger, kundebehandling, saksbehandling og rapportering, og opereres i samsvar med internt regelverk, lov og forskrifter.

Konkrete kvalitetsmål kan være:

- at tjenester gjennom selvbetjeningskanalen er tilgjengelige 24/7
- at saksbehandlingssystemene er tilgjengelige i arbeidstiden
- at IT-systemene ikke inneholder feil etter oppgraderinger og versjonsendringer
- at tilgangskontrollen til IT-systemene hindrer uautorisert tilgang til systemer og data
- at sikkerhetsbeskyttelsen hindrer vellykkede ondsinnede angrep mot systemer og data

Faste rapporteringer fra system- og driftsleverandørene, foretakets egen avvikslogg og resultatet av periodiske kontroller av tilgangsrettighetene er eksempler på måter å følge opp kvalitetsmålene på.

[1] https://lovdata.no/dokument/SF/forskrift/2008-09-22-1080/KAPITTEL_1#KAPITTEL_1

2.4 § 5. Sikkerhet

"Foretaket skal utarbeide prosedyrer som skal sikre beskyttelse av utstyr, systemer og informasjon av betydning for foretakets virksomhet, jf. § 1, 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. Kravene til IKT-sikkerhet skal så langt det er praktisk mulig være målbare. Oppfyllelse av kravene til informasjonssikkerhet for personopplysninger etter forskrift av 15. desember 2000 nr. 1265 til personopplysningsloven skal anses som oppfyllelse av kravene i paragrafen her."

2.4.1 Tilgangsstyring

Tilgangsstyring er et viktig og sammensatt område. Retningslinjer for dette skal være dokumenterte slik at der er mulig å kontrollere at retningslinjene følges.

Tilganger
Det kan være flere typer tilganger til samme system. En tilgang kan være lese-rettigheter til systemet, en annen lese- og skrive-rettigheter, og en tredje lese-, skrive- og slette-rettigheter.

Rollebasert tilgangsstyring.
Ansatte har ulike oppgaver og roller. Den ansatte kan være daglig leder, fagansvarlig, ansvarlig megler, fullmektig, medhjelper, eller ansvarlig for oppgjør, eventuelt oppgjørsmedhjelper. Ansatte skal ha tilgang til nødvendige filområder og støttesystemer. Det kan være ulike driftsoperatører for driftsplattformen og selve saksbehandlingssystemet. Tilgangsstyringen bør være rollebasert med tilganger definert for hver rolle.

Ansvar for tildeling av tilganger og dokumentasjon
Selskapet må dokumentere hvem som har ansvar for tilgangsstyringen. Ofte vil det være nærmeste leder som har ansvar for tilgangsstyringen til de han/hun leder, men det kan også være at ulike ledere har ansvar for tilgangsstyringen til ulike systemer. Den enkelte ansatte blir da tildelt tilganger fra flere ledere. Det må finnes en samlet oversikt over hva den enkelte ansatte har tilgang til.

Rutiner for tilgangsbestillinger
Foretaket skal ha rutiner for tilgangsbestillinger. Tilgangsbestillinger kan være oppretting, endring eller sletting av tilganger. Endring av tilganger er aktuelt når den ansatte får nytt ansvar og arbeidsoppgaver. Selve utførelsen av tilgangsbestillingen kan være delt mellom foretaket selv og drifts-/systemleverandør(er). Rutinene må beskrive 'tjenesteveien' med 'blankett'-støtte gjennom hele løpet.

Periodiske kontroller av tilgangsrettigheter
Det bør gjøres halvårlige kontroller av tilgangsrettighetene. Det må kunne tas ut lister både på applikasjonsnivå og på driftsnivå som viser hva den enkelte ansatte har tilgang til. IKT-ansvarlig vil ofte ha ansvar for å produsere listene mmens den som har ansvaret for å tildele tilgangene, også har ansvaret for å kontrollere tilgangene.

2.4.2 Lagring av data i skyløsninger

Skyløsninger baseres på deling av ressurser og lagring i en sky. Finanstilsynet vurderer skyløsninger på lik linje med annen utkontraktering og stiller de samme kravene som til annen utkontraktering i henhold til IKT-forskriftens § 12, se kapittel 2.9. Før en skyløsning velges for lagring av data, må skyleverandøren derfor svare tilfredsstillende på minimum følgende spørsmål:

- Er skyen lokalisert i Norge, Europa eller utenfor Europa?
- Hvordan arkiveres og slettes dataene?
- Kan dataene hentes ut igjen ved eventuelt bytte av leverandør?
- Hvilken backup tas av dataene?
- Lagres backup i et annet land enn skyen?
- Er risikoanalyser gjennomført og sikkerhetsløsninger dokumenterte?

- Hvordan er tilgangsstyringen organisert og fulgt opp?
- Er foretaket sikret adgang til å kontrollere og revidere skyleverandørens aktiviteter i henhold til kravene i IKT-forskriftens § 12 1.ledd og gir den tilsynsmyndighetene tilsvarende rett iht. §12 2. ledd?
- Hva slags hendelsesstatistikk har skyleverandøren?
- Hvilke underleverandører bruker skyleverandøren?

Personvernloven stiller krav til databehandleravtale. Personopplysningsloven gir også restriksjoner for lagring av personopplysninger utenfor Norge ref. personopplysningsloven § 29 og § 30.

2.5 § 6. Utvikling og anskaffelse og § 7. Systemvedlikehold

"Foretaket skal ha skriftlige prosedyrer for anskaffelse, utvikling, videreutvikling og testing av IKT-systemer. IKT-systemene skal ikke settes i ordinær drift før ansvarlig har godkjent dette."

"Foretaket skal sikre at IKT-systemene vedlikeholdes og forvaltes på en måte som gir en stabil, planlagt og forutsigbar drift. Det skal foreligge dokumenterte prosedyrer for systemvedlikeholdet."

Siden majoriteten av eiendomsmeglingsforetakene bruker et leverandørutviklet saksbehandlersystem, vil systemutvikling og systemvedlikehold i de fleste tilfeller utføres av leverandøren. Foretaket har likevel selv ansvar for at systemene ivaretar tilgjengelighet, konfidensialitet og integritet på en tilfredsstillende måte. Foretaket må ha kompetanse til å beskrive krav til systemet og til å kontrollere systemleveransene. I kapitlene om endringshåndtering og utkontraktering er dette nærmere beskrevet.

For å sikre at foretaket kan tåle en situasjon der systemleverandøren får problemer, kan foretaket, evt. foretakene i en kjede i samarbeid, sikre eierskap til kildekoden gjennom en Escrow-avtale[2]. Foretaket kan også vurdere å inngå avtale med en alternativ leverandør om at denne skal bistå i en situasjon der primær-leverandøren får problemer.

2.6 § 8. Drift

"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. 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."

Det er nyttig å rangere IKT-løsningene etter hvor viktige de er og hvilke krav det er til tilgjengelighet til systemene. Noen systemer er det tilstrekkelig at er tilgjengelig mellom kl. 08 og 16 på hverdager. Andre systemer må være tilgjengelige 24/7 som eksempelvis portalen mot publikum. Driftsløsningene må tilpasses kravene til tilgjengelighet.

For å sikre høy tilgjengelighet til systemene, kan det etableres dupliserte løsninger som er likeverdige. En sekundær løsning overtar automatisk for den primære og sikrer kontinuitet på en måte som gjør at sluttbrukeren i liten grad vil merke et avbrudd. Driftsløsninger som sikrer kontinuitet kan etableres for ulike komponenter i driftsmiljøet som databaser, disker, programvareservere og nettverk. Større eiendomsmeglingsforetak har ofte utkontraktert driften til profesjonelle driftsleverandører som tilbyr denne typen løsninger.

I avtalen med driftsleverandøren må foretakets krav til tilgjengelighet fremgå og hvordan leverandøren skal levere i henhold til dette. Videre må foretaket avtalefeste at leverandøren skal rapportere

[2] Escrow-avtale: Avtale om at kunden får tilgang til kildekoden hvis en kritisk situasjon skulle oppstå.

regelmessig og minimum halvårlig om hvordan kravene er oppfylt.

2.7 § 9. Avviks- og endringshåndtering

2.7.1 Endringshåndtering

"Prosedyrene for endringshåndtering skal omfatte alle endringer som kan påvirke IKT-systemene og skal sikre forsvarlig, formell behandling og dokumentering av endringene. Foretaket skal sikre at prosedyrene for endringshåndtering gir en stabil, planlagt og forutsigbar drift."

Systemendringer
Majoriteten av eiendomsmeglingsforetakene bruker et leverandørutviklet saksbehandlersystem, og systemleverandøren spiller en viktig rolle i endringshåndteringen. Leverandøren leverer nye versjoner av systemet et visst antall ganger i året. Endringene i nye versjoner består gjerne av en kombinasjon av forbedret funksjonalitet og feilretting fra forrige versjon, sammen med helt ny funksjonalitet. Siden mange eiendomsmeglingsforetak bruker samme saksbehandlersystem, har foretakene i ulik grad vært med på å spesifisere endringene i de nye versjonene.

Endringshåndtering defineres som hele løpet fra en endring kravspesifiseres til den settes i produksjon. Enten foretaket har vært med på å definere endringene i utgangspunktet, eller det iverksetter endringene gjennom en ny versjon av systemet, skal foretaket innarbeide endringene i eget system. Dette innebærer følgende:

- ha kunnskap om hva endringene innebærer,
- sikre at funksjonaliteten i systemet er i henhold til lover og regelverk,
- brukeropplæring,
- dokumentasjon av endringene,
- test av endringene og
- formell godkjennelse av at akseptansetest av endringene med tilfredsstillende resultat er utført

Først deretter kan den nye versjonen av systemet settes i produksjon.

Driftsendringer
Ofte har eiendomsmeglingsforetakene også utkontraktert driften. Driftsendringer spesifiseres da av driftsleverandøren som har detaljkunnskap om driftsmiljøet.

Endringer i nettverk, brannmurer, disker, databaser, sertifikater, lisenser med mer initieres av løpende driftsovervåking av kapasitetsgrenser og andre terskelverdier eller av nye systemversjoner.

Det kan være hensiktsmessig å skille mellom standardendringer og normale driftsendringer. Standardendinger er endringer som rutinemessig utføres og som medfører lavere risiko enn andre endringer. Standardendringer kan derfor behandles gjennom en enklere endringshåndteringsprosedyre enn normale driftsendringer. Eiendomsmeglingsforetaket må sikre at driftsleverandøren har dokumentert hvilke typer endringer som sorterer under standardendringene. Listen over standardendringer bør godkjennes av foretaket, og gjennomgås sammen med leverandøren årlig.

Eiendomsmeglingsforetaket skal informeres om og godkjenne driftsendringer. Unntaket er standardendringer som leverandøren kan gjennomføre uten samme krav til formell godkjenning.

2.7.2 Avvikshåndtering

"Prosedyrene for avvikshåndtering skal omfatte alle avvik som oppstår i driften av IKT-systemene. Avviksbehandlingen skal ha som formål å gjenopprette normal tilstand i IKT-virksomheten. Avviksbehandlingen skal identifisere årsaken til avvik, hindre gjentagelser og sikre forsvarlig og formell behandling av avviket. Avvikene skal dokumenteres. Prosedyrene for avvikshåndtering skal inneholde retningslinjer for eskalering."

Avvik kan oppstå etter endringer eller som følge av svikt i overvåkningen av systemene.
Hvor mange feil som oppstår etter nye systemversjoner, er en god parameter på hvor godt endringshåndteringen fungerer. Overskridelse av terskelverdier som definerte max-verdier eller utløpsdato på sertifikater, lisenser eller systempatcaher kan føre til avbrudd. Dersom driften er utkontraktert, er det oftest driftsleverandør som overvåker terskelverdier og systemparametere.

Foretaket skal ha et system for registrering av avvik, klassifisering av avvik og oppfølging av avvik. Avvikshåndteringen skal inneholde alle avvik som berører foretaket uavhengig av om avviket oppstår i egen IT-organisasjon eller hos en av leverandørene. Faste oppfølgingspunkt på møter med leverandørene er gjennomgang av avvik og oppfylling av definerte krav i serviceavtaler.

Håndtering av sikkerhetshendelser
Det er viktig å ha dokumenterte rutiner for håndtering av sikkerhetshendelser. En sikkerhetshendelse kan være en situasjon der selskapet blir utsatt for eksponering eller manipulering av data. Årsaken kan være eksterne angrep mot selskapets elektroniske systemer, eksempelvis mot url/domenenavn, eller at kunder eller egne ansatte bryter regler eller interne krav. Det kan være nødvendig å stenge ned systemet for å avgrense skaden og avklare omfanget av og årsaken til hendelsen. For å håndtere en sikkerhetssituasjon mest mulig effektivt, bør eiendomsmeglingsforetaket ha beskrevet varslingsveier, beslutningspunkter og mediestrategi. Det er naturlig å knytte denne dokumentasjonen til kriseplanen, se neste kapittel.

2.8 § 11. Driftsavbrudd og kriseberedskap

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

Kriseplanen skal minst omfatte

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

Det skal minst en gang årlig gjennomføres opplæring, øvelse og testing av at kriseløsningen virker som forutsatt. Resultatet av testen skal dokumenteres."

IKT-forskriften stiller krav til at eiendomsmeglingsforetaket skal ha en dokumentert kriseplan. Kriseplanen skal beskrive hvordan en situasjon der driften ikke kan opprettholdes med normalt tilgjengelige ressurser, skal håndteres.

I arbeidet med å lage kriseplanen kan det være nyttig med en scenariobasert tilnærming.

Driftsavbrudd kan oppstå hos driftsleverandør eller i den lokale systemstøtten. Feil i saksbehandlingssystemet etter nye systemversjoner kan medføre feil i datagrunnlaget. Eksterne angrep kan blokkere tilgangen til systemene eller manipulere eller eksponere data.
Foretaket må definere hva som er en krise for foretaket, hvilke hendelser som kan utløse slike situasjoner og hvilke tiltak som skal iverksettes hvis en slik situasjon oppstår.
Håndtering av sikkerhetshendelser som beskrevet i kapittelet over inngår i dette.

Stikkord for håndteringen i en krisesituasjon er kommunikasjon med leverandør, varslingsveier, informasjon internt og eksternt, og iverksettelse av reserveløsninger enten de er elektroniske eller manuelle. En dokumentert kriseplan sikrer en rasjonell og effektiv håndtering av en krisesituasjon.

2.8.1 Test av kriseløsningen

IKT-forskriften sier at det minst årlig skal gjennomføres opplæring, øvelse og testing i et omfang som gir tilstrekkelig trygghet for av at kriseløsningen virker som forutsatt. Resultatet av testen skal dokumenteres slik at det er mulig å kontrollere.

Den årlige testen av kriseløsningen involverer både eiendomsmeglingsforetaket og driftsleverandøren. Foretaket må gjennom avtalen med leverandøren sikre at denne forplikter seg til årlig test av sine beredskapsløsninger. Leverandøren skal dokumentere resultatet av testen og rutinemessig rapportere dette til eiendomsmeglingsforetaket.

Eiendomsmeglingsforetakets egen test av kriseløsningen vil ofte bestå i å sikre at det foreligger testresultater fra leverandøren, kontrollere at varslingslister er oppdaterte, gjennomgå egne reserveløsninger og øve de ansatte i kriseløsningen.

2.9 § 12. Utkontraktering

"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 kontrollere, herunder revidere de av leverandørens aktiviteter som er knyttet til avtalen. Avtalen skal også sikre håndtering av taushetsbelagt informasjon.

Avtalen skal videre sikre at Finanstilsynet gis tilgang til opplysninger fra og tilsyn hos IKT-leverandøren der Finanstilsynet finner det nødvendig som et ledd i tilsynet med foretaket.

Foretaket skal sikre, i egen regi eller gjennom et formalisert samarbeid med andre foretak enn IKT-leverandøren, at organisasjonen besitter tilstrekkelig kompetanse til å forvalte utkontrakteringsavtalen."

Det er viktig å merke seg at det er foretaket med konsesjon til å drive eiendomsmegling, som har ansvaret for at virksomheten drives i samsvar med kravene i IKT-forskriften. Dette gjelder også der IKT-løsningene er utkontraktert. I praksis betyr dette at eiendomsmeglingsforetaket må sikre at leverandøren(e) oppfyller kravene i IKT-forskriften. Så vel systemleverandør som driftsleverandør må i avtalen med foretaket forplikte seg til å etterleve IKT-forskriften. Dette innebærer blant annet at eiendomsmeglingsforetaket gis rett til å kontrollere og revidere de av leverandørens aktiviteter som er knyttet til avtalen og at Finanstilsynet gis tilgang til opplysninger fra og tilsyn hos IKT-leverandøren der Finanstilsynet finner det nødvendig som et ledd i tilsynet med foretaket. Det samme gjelder for leverandørens eventuelle underleverandører.

Eiendomsmeglingsforetaket må selv ha kompetanse til å stille krav til systemløsningene, følge opp leveransene, teste og akseptere/godkjenne systemendringer. Det må avtales faste møteplasser og faste rapporteringer med leverandørene som foretaket må ha rutiner for å følge opp.

For møter med og rapportering fra systemleverandøren vil kravspesifikasjoner og testresultater stå på agendaen. For møter med og rapportering fra driftsleverandør, skal bl.a. oppfølging av serviceavtaler på tilgjengelighet og håndtering av IKT-sikkerhet stå på agendaen.

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