Finansdepartementet
Postboks 8008 Dep
0030 Oslo

Vår ref.: VMA

Oslo, 19.04.2024

Høringssvar – nye regler om digital operasjonell motstandsdyktighet i finanssektoren (DORA)

Innledning

Finansforbundet viser til Finansdepartementets høring av 23.01.2024 om behovet for endringer i norsk rett for å gjennomføre forventede EØS-forpliktelser som svarer til DORA (Digital Operational Resilience Act).

Finansforbundet er største fagforbund i finansnæringen, med over 35.000 medlemmer. Vi er opptatt av å sikre gode og forutsigbare rammebetingelser for finansnæringen, og ivareta ansattes rettigheter.

Finansforbundet er positiv til departementets forslag om å implementere de felleseuropeiske reglene som følger av DORA, gjennom en ny lov om digital operasjonell motstandsdyktighet i finanssektoren. Finansmarkedene er internasjonale og tett integrert, og vi mener det er en fordel med et harmonisert felleseuropeisk regelverk også knyttet til digital motstandsdyktighet og IKT-sikkerhet.

Finansforbundets hovedsynspunkter knytter seg til

- Behandling av ansattes personopplysninger
- Kompetansebehov og utkontraktering
- Håndhevelse av proporsjonalitetsprinsippet
- Avklaringer om implementering og virkeområde
- Avklaringer om sanksjonering

Behandling av ansattes personopplysninger

Finansforbundet ser behovet for et felleseuropeisk regelverk om IKT-risiko i finanssektoren. Digital Operational Resillience Act (DORA) stiller betydelige krav til blant annet testing, risikovurdering, hendelseshåndtering og overvåkning. Dette innebærer samtidig en omfattende behandling av

ansattes personopplysninger. Finansdepartementet omtaler ikke konsekvensene for ansattes personvern i sitt høringssvar. Dette er problematisk.

Allerede i dag kan datasikkerhetstiltak i praksis føre til en totalregistrering av ansattes arbeidshverdag. Eksempler er overvåkning av inn- og utgående e-poster, fiktive phishingforsøk, «flagging» av uvanlig aktivitet eller språk, loggføring av aktivitet på internett og registrering av IP-adresser. I tillegg kommer overvåkning i medhold av annet regelverk virksomhetene er underlagt, deriblant lydopptak av telefonsamtaler og lagring av elektronisk kommunikasjon i tilknytning til investeringstjenester etter verdipapirhandelloven. Med DORA vil datasikkerhetstiltakene øke og behovet for beskyttelse av ansattes personvern forsterkes.

Dagens lovverk har omfattede og konkrete krav til arbeidsgiver for å ivareta sikkerheten, men få og upresise regler som skal ivareta personvernet. Dette gir en ubalanse som går på bekostning av ansatte. I arbeidslivet generelt er det et skjevt styrkeforhold mellom arbeidsgiver og arbeidstaker. I finans hvor sikkerhetstiltakene er spesielt omfattende er behovet for tiltak som ivaretar ansattes personvern stort.

Personvernforordningen er vanskelig tilgjengelig og utfordrende å omsette i praksis. Den har et stort virkeområde og baserer seg på generelle prinsipper. I tillegg skiller regeloppbygningen og språket seg fra annen norsk lovgivning. Dette er krevende å forholde seg til for arbeidsgivere, og gjør det vanskelig for ansatte å forstå sine rettigheter.

I tillegg reguleres innsyn i ansattes e-post og annet elektronisk materiale i e-postforskriften. E-postforskriften er av eldre dato, og gjenspeiler ikke behovet for vern som ansatte har i dagens teknologiske samfunn.

Finansforbundet etterlyser en særskilt lovgivning for behandling av personopplysninger i arbeidslivet. Vi fremhever personvernforordningen art. 88 som åpner for å fastsette nærmere regler for behandling av arbeidstakeres personopplysninger i ansettelsesforhold.

Kompetansebehov og utkontraktering

Det framgår at DORA vil gi vesentlige mer omfattende og detaljerte krav til norske foretaks risikostyring, hendelseshåndtering og bruk av IKT-leverandører. Finansforbundet mener det er helt avgjørende at ansatte som skal følge opp etterlevelse av regelverket også tilbys tilstrekkelig kompetanseheving. Dette ansvaret ligger særlig til finansinstitusjonene som må legge til rette for nødvendig kompetanseheving. Det må også utvikles relevante kompetansetilbud fra utdanningsinstitusjonene. Vi vil i den forbindelse bemerke at det som del av bransjeprogram for finansnæringen er tildelt midler til Nord universitet i Bodø får å utvikle et emne innen digital bekjempelse mot finansiell kriminalitet. Dette er en god start, som vi mener det kan bygges videre på.

Gitt finansnæringens rolle som en grunnleggende nasjonal funksjon, vil angrep på leverandørkjeder av IKT-tjenester med store kundebaser kunne få omfattende konsekvenser. Finansforbundet har tidligere kritisert utflagging av tjenester, blant annet grunnet tap av kompetanse. Utfordringen med å ha for lite kompetanse er at vi mister verdifull bestiller-, innkjøps- og kontrollkompetanse, noe Finansmarkedsmeldingen også belyser. Finansforbundet har videre merket seg at totalberedskaps-kommisjonen mener det er avgjørende at finansnæringen har et bevisst forhold til hvilken kompetanse som ikke bør utkontrakteres. Vi vil understreke at det er avgjørende med god oppfølging når det gjelder dette området. Det er positivt at Finanstilsynet har vedtatt forskrift om meldeplikt

ved utkontraktering av virksomhet og utarbeidet et eget rundskriv om utkontraktering. Vi mener videre det er grunnlag for å undersøke nærmere hvilke erfaringer næringen har gjort seg med det å legge IKT-funksjoner til land utenfor Norge, for å kartlegge hvilke konsekvenser dette har med hensyn til å kunne ivareta kritisk kompetanse i Norge.

Håndhevelse av proporsjonalitetsprinsippet

Etter forordningens artikkel 4 skal foretak gjennomføre reglene i henhold til et proporsjonalitetsprinsipp, og skal ta hensyn til foretakets størrelse og samlede risikoprofil, samt virksomhetens type, omfang og kompleksitet. Høringsnotatet understreker at norske foretak lenge vært underlagt krav som langt på vei svarer til forordningen. Økte rapporteringskrav og krav til oppfølging av rapporteringen innebærer likevel at foretakene må påregne vesentlig innsats særlig i overgangen til nytt regelverk. Tilsvarende vil krav om penetrasjonstesting medføre behov for administrasjon og oppfølging.

Basert på høringsnotatet er det utfordrende å ta stilling til hvordan proporsjonalitetsprinsippet er tenkt å fungere i praksis. Slik vi oppfatter det, er det ikke klargjort hvilke deler av forordningen som gjelder for ulike aktører. Finansforbundet mener proporsjonalitetsprinsippet må implementeres og håndheves med aktsomhet med tanke på påvirkning av konkurransesituasjon for små og mellomstore aktører. Disse strever allerede med høyere kapitalkrav og omfattende compliance- og rapporteringskrav. Det er en styrke for norsk økonomi og næringsliv at finansmarkedet i Norge består av både internasjonale og nasjonale aktører, både stor og små.

Implementering og virkeområde

Implementeringen av DORA må koordineres med implementering av digital sikkerhetslov. Digital sikkerhetslov ble vedtatt i Stortinget i 2023 og vil tre i kraft i 2024 eller 2025. Loven skal løfte virksomheter innenfor samfunnsområder som har en særlig viktig rolle for opprettholdelsen av samfunnsmessig og økonomisk aktivitet, herunder bank, finansmarkedsinfrastruktur og digital infrastruktur. DORA vil, som en såkalt lex specialis, gå foran digital sikkerhetslov.

Finansforbundet er kjent med at ettersom tidspunkt for ikrafttredelse for DORA og Digitalsikkerhetslov ikke er avklart, er det en utfordring for finansnæringen å vite hvilket lovverk man skal forholde seg til. Det kan f.eks. være et spørsmål om man først må ivareta digitalsikkehetsloven og så DORA. I implementeringen av DORA og Digitalsikkerhetsloven bør det derfor komme klart fram hvordan finansnæringen skal håndtere overgangen til nytt lovverk.

For en del selskap som er underlag finansforetaksloven er det uklart om de også vil være underlagt DORA. Finansdepartementet bør her avklare virkeområdet til DORA når det gjelder bl.a. morselskap i finanskonsern. Morselskap er å anse som finansforetak, men det fremgår ikke av listen i høringsnotatet (kap. 2.2.1) om hvorvidt de også omfattes av virkeområdet for DORA.

Sanksjoner

Gjennomføring av DORA som en ny lov om digital operasjonell motstandsdyktighet i finanssektoren, åpner for at Finanstilsynet vil kunne ilegge administrative sanksjoner i form av overtredelsesgebyr. Finansforbundet vil påpeke at det allerede er et omfattende lovverk som muliggjør sanksjoner knyttet til digital sikkerhet, herunder digitalsikkerhetsloven, finansforetaksloven og finanssikkerhetsloven. Slik vi forstår det vil dette kunne innebære at finansvirksomheter kan få ilagt

sanksjoner for samme overtredelse i henhold til flere lovverk. Det bør foretas en gjennomgang av sanksjonsordningene i de ulike lovverkene med henblikk på at de innskrenkes for ikke å overlappe. Vi understreker at det særlig for små aktører er hensiktsmessig med forutsigbarhet med hensyn til hvilke regler som vil gjelde for ulike overtredelser.

Med vennlig hilsen
FINANSFORBUNDET

Vigdis Mathisen
forbundsleder