Erhvervs- og Vækstministeriet
Att.: Departementschef Michael Dithmer
Slotsholmsgade 10-12
1216 København K

Sektorinitiativer for beskyttelse af fortrolige kundeoplysninger

4. september 2015

Finanssektorens Hus
Amaliegade 7
1256 København K

Telefon 3370 1000

mail@finansraadet.dk
www.finansraadet.dk

I brev af 18. september 2014 angav daværende direktør Jørgen A. Horwitz blandt andet, at sektoren havde defineret to initiativer for at styrke sektorens håndtering af fortrolige kundeoplysninger. Initiativerne blev beskrevet som udarbejdelse af sektorfælles retningslinjer for:

1. Håndtering af adgangsstyring og kontrol.
2. Gennemførelse af "awareness"-indsatser over for medarbejderne.

Endelig blev det anført, at Finansrådet – når retningslinjerne forelå – ville henstille til medlemmerne, at retningslinjerne blev fulgt.

Journalnr. 466/05
Dok. nr. 541433-v1

Som opfølgning på ovenstående har Finansrådet i et konstruktivt samarbejde med bankernes it-sikkerhedsspecialister arbejdet på at udarbejde retningslinjerne. Sideløbende har der fra bankernes side også været arbejdet med deres interne opfølgning på implikationerne af "Se & Hør-sagen".

Opfølgningen på "Se & Hør-sagen" er blevet behandlet med største alvor af både bankerne og Finansrådet. Således har bankerne – som anført i ovenstående – i forlængelse af sagen gennemgået egne procedurer og vurderet, om der eventuelt skulle justeres i disse. Tilbagemeldingen fra bankerne har været, at de eksisterende procedurer generelt er tilfredsstillende.

I forhold til selve retningslinjerne, der gennemgås i nedenstående, og som **vedlægges** som bilag, er det vigtigt at være opmærksom på de omfattende regler, som bankerne allerede er underlagt i blandt andet Lov om Finansiel Virksomhed og Persondataloven. Disse regler udmøntes på forskellig vis i bankerne og har betydet, at der allerede er en række procedurer, som bliver efterlevet. Ikke desto mindre har Finansrådet – i samarbejde med medlemmerne – fundet det hensigtsmæssigt at udfærdige disse retningslinjer for derved at understrege sagens vigtighed.

Det skal endelig bemærkes, at retningslinjerne i sagens natur er relativt overordnede. Finansrådet kan som interesseorganisation ikke stille egentlige krav til sine medlemmer om at overholde retningslinjer eller lignende. Det kan tilføjes, at det i denne sag i øvrigt heller ikke ville give særlig god mening, hvis Finansrådet kastede sig ud i detaljerede retningslinjer, blandt andet fordi der blandt de danske pengeinstitutter er væsentlige forskelle i størrelse, forretningsprocesser, systemdesign mv., hvilket betyder, at de

individuelle pengeinstitutter bedre vil kunne udfærdige detaljerede retningslinjer.

Retningslinjerne
I forhold til *retningslinjerne om håndtering af adgangsstyring og kontrol* (bilag 1) er der i forhold til adgangsstyring blandt andet fokus på, at der skal være et arbejdsbetinget behov for at få adgang til fortrolige data, og at der bør foreligge en risikovurdering i forbindelse hermed. Derudover også, at administrationen af adgange bør ske systematisk og sikre styring og dokumentation af de tildelte adgange. Endelig bør der ske en løbende opfølgning på, hvorvidt de oprindelige kriterier for tildeling af adgange til stadighed er valide og aktuelle.

Med hensyn til kontrol af adgangsstyring fokuseres der på logning af anvendelsen, der bør sikre, at man til enhver tid kan se, ikke blot registreringer og transaktioner, men også opslag på kundedata. Det bør således være muligt at undersøge en given system- og dataanvendelse. Derudover bør der ske en løbende kontrol i form af stikprøver på disse aktiviteter. Således vil medarbejderne også være bevidste om, at de kan blive stillet til ansvar for de opslag, registreringer eller transaktioner, de måtte foretage, og at de skal kunne begrunde enhver systemaktivitet som værende arbejdsbetinget.

I forhold til *retningslinjer om sikring af medarbejderes awareness om behandling af fortrolige kundedata* (bilag 2) er fokus på, at alle medarbejdere, eksterne konsulenter med flere bør underskrive en tavshedserklæring, inden de får adgang til fortrolige data. I den forbindelse bør de blive gjort opmærksomme på de gældende regler både internt i virksomheden og den bagvedliggende lovgivning samt de mulige konsekvenser ved overtrædelse af disse.

Det er Finansrådets opfattelse, at det er nødvendigt med en løbende ajourføring af medarbejdernes opmærksomhed på dette område for at sikre, at medarbejdernes opmærksomhed på disse regler ikke svækkes hen over tid. Der bør derfor med passende mellemrum iværksættes awareness-indsatser eller lignende, som sikrer, at alle, der er omfattet af tavshedspligten, bliver gjort opmærksom på dette vigtige område. Endelig bør bankerne kunne dokumentere deres awareness-indsats.

Videre proces
Som nævnt indledningsvist i brevet vil Finansrådet – efter fremsendelsen af dette brev – henstille til pengeinstitutterne, at retningslinjerne følges. Derudover stiller Finansrådet sig selvfølgelig til rådighed for uddybning af retningslinjerne og eventuelle spørgsmål, som retningslinjerne måtte afstedkomme.

Med venlig hilsen

Michael Busk-Jepsen

Direkte +45 3370 1068
mbj@finansraadet.dk

Bilag 1

Retningslinjer om håndtering af adgangskontrol og logning for medarbejdere med fleres adgang til fortrolige kundedata

Journalnr. 466/05
Dok. nr. 541433-v1

Oplysninger om kunder og deres engagement har pengeinstitutter pligt til at beskytte, jf. både Lov om Finansiel Virksomhed og Persondataloven, og sektoren har traditionelt haft stor opmærksomhed på området. Disse oplysninger opfattes af kunderne og omverdenen generelt som værende personlige, og de forventes behandlet med en høj grad af fortrolighed. Derfor bør adgang til kundedata i pengeinstitutter kun gives, hvor der foreligger et arbejdsbetinget behov.

Disse retningslinjer omfatter følgende forhold:

1 **Adgangskontrol**
1.1 Arbejdsbetinget behov
1.2 It-drifts- og supportpersonale, inkl. eksterne samarbejdspartnere
1.3 Administration

2 **Logning og kontrol**
2.1 Logning
2.2 Kontrol og opfølgning
2.3 Tilrettelæggelse af kontroller

1 Adgangskontrol

1.1 Arbejdsbetinget behov

Arbejdsbetinget behov findes i mange forskellige afskygninger, og det er ikke muligt at give præcise retningslinjer for, hvorledes dette skal tolkes. Der er behov for betjening af kunder i blandt andet tværgående servicecentre, ligesom der i dag ikke findes geografiske skel imellem de steder, kunderne skal kunne betjenes. I alle tilfælde bør der dog foreligge en vurdering og risikovurdering i forbindelse med definitionen. Det kan i denne sammenhæng ligeledes være vigtigt at skelne imellem midlertidigt behov og behov af mere permanent karakter.

Det mest åbenlyse behov findes umiddelbart hos de medarbejdere, der til dagligt møder kunderne direkte enten fysisk eller via elektroniske kanaler. Derudover findes behovet i forskellige supportfunktioner samt specielle centrale funktioner som eksempelvis intern revision, inkassoafdelinger etc. Der findes desuden en række funktioner, hvor der egentlig ikke er behov for direkte adgang til kundeoplysninger, men hvor arbejdets karakter nødvendiggør, at man i forbindelse med udførelse af det daglige arbejde vil få adgang til kundedata.

Omvendt vil teknisk personale, rengøringspersonale, bankbetjente og itudviklere normalt ikke have et permanent arbejdsbetinget behov for adgang.

1.2 It-drifts- og supportpersonale, inkl. eksterne samarbejdspartnere

It-drifts- og supportpersonale med flere kan have behov for at få adgang til kundedata i forbindelse med deres daglige arbejde. Dette gælder, uanset om de er ansat internt eller eksternt hos eksempelvis samarbejdspartnere, outsourcingpartnere eller serviceleverandører.

1.3 Administration

Administrationen af adgange bør ske systematisk og sikre styring og dokumentation af de tildelte adgange. Dokumentationen for tildeling af adgang bør begrunde det arbejdsbetingede behov og godkendes af en ledende medarbejder. Der bør foretages en periodisk vurdering af, hvorvidt de oprindelige kriterier for de tildelte rettighedsadgange til stadighed er valide og aktuelle.

2 Logning og kontrol

2.1 Logning

Udover kontrollen med tildeling og generel håndtering af tildelte rettigheder bør der ske logning af anvendelsen. Logningen bør således sikre, at man til enhver tid kan se ikke blot registreringer og transaktioner, men også opslag på kundedata.

2.2 Kontrol og opfølgning

Denne logning bør kunne dokumentere, hvem der har foretaget opslag, registreringer eller transaktioner og på hvilke kunder, således at det vil være muligt at undersøge en given system- og dataanvendelse. Udover undersøgelse af konkrete hændelser bør der ske en løbende kontrol i form af stikprøver på disse aktiviteter. Det vil også betyde, at medarbejderne ved, at de kan blive stillet til ansvar for de opslag, registreringer eller transaktioner, de måtte foretage, og at de skal kunne begrunde enhver aktivitet som værende arbejdsbetinget.

Hvor forholdene tilsiger det, kan der foretages skærpet monitorering af transaktioner i forhold til udvalgte kunder og eventuelt etablere særlig notifikation ved mistanke om overskridelse af beføjelser.

2.3 Tilrettelæggelse af kontroller

Alle ovennævnte kontroller bør tilrettelægges med udgangspunkt i en konkret risikovurdering og tilpasses pengeinstituttets forhold og organisation i øvrigt.

Bilag 2

Retningslinjer om sikring af medarbejderes awareness om behandling af fortrolige kundedata

Journalnr. 466/05
Dok. nr. 541433-v1

Ansatte med flere i en virksomhed omfattet af Lov om Finansiel Virksomhed (FIL) er ifølge lovens § 117 pålagt en tavshedspligt om fortrolige oplysninger, herunder oplysninger om kunders personlige forhold. Denne tavshedspligt er hele fundamentet for finansielle institutioners samarbejde med kunderne, idet kunderne skal kunne stole på, at deres personlige oplysninger ikke videregives uberettiget eller på anden måde udnyttes. Tillid er med andre ord en nøglefaktor i dette samarbejde.

Disse retningslinjer omfatter følgende forhold:

1. Tavshedserklæring
2. Awareness af medarbejdere
3. Awareness-indsats
4. Indhold af indsats
5. Dokumentation

1. Tavshedserklæing

Alle medarbejdere, eksterne konsulenter med flere bør underskrive en tavshedserklæring, inden de får adgang til fortrolige data. I den forbindelse bør de blive gjort opmærksomme på de gældende regler både internt i virksomheden og den bagvedliggende lovgivning samt de mulige konsekvenser ved overtrædelse af disse.

2. Awareness af medarbejdere

Der bør være fokus på, at medarbejdernes opmærksomhed på disse regler hen over tid kan svækkes. Derfor bør der ske en løbende ajourføring af medarbejdernes opmærksomhed på området.

3. Awareness-indsats

Der bør med passende mellemrum gennemføres awareness-indsatser eller lignende, som sikrer, at alle, der er omfattet af tavshedspligten, er opdateret med de seneste regler og politikker på området.

Måden, hvorpå det enkelte pengeinstitut gennemfører indsatsen, kan variere, men det bør sikres, at formen er tilpasset den konkrete målgruppe, således at den bedst mulige effekt opnås.

4. Indhold af indsats

Indholdet bør omhandle relevante regler på persondatalovens område og FIL § 117 samt konsekvenserne ved overtrædelse af disse bestemmelser. Derudover kan der være specielle forhold i den enkelte virksomhed, der påkalder sig særlig opmærksomhed i denne anledning, hvorfor de naturligvis også skal behandles. Nogle af de emner, der kan berøres, er eksempelvis:

- Ud over finansielle ydelser er tillid den vigtigste vare, et pengeinstitut tilbyder sine kunder, og den tillid må ikke svigtes.

- Nej, det er ikke ok at bruge systemerne til at slå kunder og kollegaers fødselsdage op – det vil typisk ske ved et opslag for at finde et CPR-nummer, som er en fortrolig kundeoplysning.
- Man må ikke tilgå fortrolige oplysninger, som man ikke har et arbejdsbetinget behov for at tilgå.
- Det er ikke ok "bare" at tilegne sig oplysninger, som man ikke har et arbejdsbetinget behov for.
- Kommer man utilsigtet i besiddelse af viden, som falder ind under ovenstående, så skal man tale med sin chef om det.
- Vær opmærksom på, at i finanskoncerner gælder FIL måske for nogle, men ikke nødvendigvis alle selskaber, og dermed er der forskellige lovkrav på området. Uagtet dette vil virksomhedens overordnede sikkerhedspolitik normalt altid være gældende.
- Det er ikke ok at diskutere kundeforhold med andre kollegaer, for hvem det ikke er arbejdsmæssigt relevant.
- Det er selvfølgelig helt uacceptabelt – og strafbart - at lade fortrolige kundeoplysninger tilgå 3. mand, herunder pressen, uanset typen af information.

Ovenstående er ikke en udtømmende liste, men blot eksempler til inspiration.

5. Dokumentation

Både den initiale indføring i reglerne og awareness-indsatserne bør kunne dokumenteres gennemført på en måde tilpasset de konkrete forhold i pengeinstituttet.

6. Opfølgning

Finansrådet vil – i samarbejde med bankerne - efter 1 år gøre status for awareness-indsatserne og i samarbejde med bankerne overveje, om det vil være hensigtsmæssigt at udarbejde en erfaringsbaseret best practice for, hvordan en medarbejderrettet awareness-indsats i forhold til behandling af fortrolige kundeoplysninger kan udformes med størst mulig effekt.