Danske Revisorer
NR. 1
Januar 2016
42. årgang

Foreningen
Danske Revisorer

Tema:
IT sikkerhed

UDGIVER:

Foreningen Danske Revisorer

Munkehatten 32
5220 Odense SØ
Telefon 65 93 25 00
fdr.dk
fdr@fdr.dk

Danske Revisorers målsætning er at bringe kortfattede, relevante og faglige artikler.
Synspunkter, der kommer til udtryk i Danske Revisorer, behøver ikke nødvendigvis at være udtryk for foreningens eller bestyrelsens standpunkt.

REDAKTION
SUSANNE HOLM, Odense
HENRIK WILSON, Måløv
CHARLOTTE ELWAIN, Kerteminde

ABONNEMENTSPRIS
Pris pr. årgang kr. 125,- inkl. moms og forsendelse.
Løssalg kr. 35,- pr. stk.

ANNONCEPRISER
1/1-side 180 x 263,5..... kr. 7.150,-
1/2-side 180 x 130..... kr. 5.500,-
1/3-side 180 x 85..... kr. 4.400,-
1/4-side 180 x 63..... kr. 3.850,-
Bagside 160 x 205..... kr. 7.700,-
Omslag side 2
180 x 263,5..... kr. 7.700,-
Gentagelsesrabat på 10% for 4 indrykninger.

Annoncemateriale leveres digitalt.
Indleveringsfristen er 4 uger før udgivelse.
Danske Revisorer udkommer marts, juni, september og december. Der tages forbehold for forsinkelser i udgivelsestidspunktet.

LAYOUT, PRODUKTION OG TRYK
Erhverv-fyn.dk
OPLAG
1.200 eksemplarer

NR. 1 - JANUAR 2016

Indhold


Carsten Hvid Challet


Jens Sørensen


Kåre Olsen


Sune Bielefeldt

It-sikkerhed – et ansvar, vi skal tage på os

Antallet af databedragerier er mellem seks- og syvdoblet siden 2009

Af næstformand Henrik Wilson, Foreningen Danske Revisorer

Temaet i dette nummer af Danske Revisorer har for en gangs skyld ingen forbindelse til revision eller regnskaber. Det handler derimod om it-sikkerhed, et emne der bliver mere og mere påtrængende for os alle.

Vi har alle hørt om mennesker og virksomheder, der har fået knækket deres kodeord, krypteret indholdet på deres computere, mistet mange timer og tusindvis af kroner på at retablere deres mistede data – og måske endda været ude af stand til det, fordi de havde været sløsede med deres sikkerhedskopiering.

Nu tager vi emnet op, til gavn for os selv og vore klienter.

En række artikler på de følgende sider belyser it-kriminalitet fra forskellige vinkler. Du vil kunne læse, at antallet af databedragerier er mellem seks- og syvdoblet siden 2009. Professionel hacking bliver et stadig alvorligere problem.

Måske har vi og vore klienter ikke været tilstrækkeligt opmærksomme på, hvor vigtigt det er at sikre vores data mod misbrug. En ting er, når vi kan læse i medierne, at vores personnumre på grund af grov sjusk hos myndighederne eller deres betroede rådgivere pludselig er offentligt tilgængelige. Men vi må ikke komme i samme båd med vore klienters og egne data.

Der er to vigtige ting, vi kan gøre, for at sikre os selv og vore klienter. Den ene er at benytte nogle virkeligt sikre passwords. I dette nummer af Danske Revisorer kan du lære at skabe dig et sikkert password. Den anden er at foretage sikkerhedskopiering, så du aldrig kan miste mere end maksimalt otte timers data, nemlig dagens.

Vi benytter en standarderklæring, når vi reviderer vore klienters indsats med hensyn til it-sikkerhed. Men er det nok? Jeg vil anbefale alle medlemmer, at man ved næste revision går mere i dybden med klienternes it-sikkerhed og tjekker, om deres indsats er tilstrækkelig. På den måde vil vi få strammet op på sikkerheden i mere end 25.000 danske virksomheder.

Det kan også være en god idé at tjekke, om vore egne og klienternes erhvervsansvarsforsikringer dækker ikke bare omkostninger til genskabelse af data, men også ansvar for manglende sikkerhed af personfølsomme data.

Når alt dette er sagt, går livet jo videre. Jeg tror, det er sikkert nok at spå, at 2016 bliver lige så turbulent som det år, vi netop har forladt. Jeg ønsker alle medlemmer af Foreningen Danske Revisorer et udfordrende, spændende og sikkert nyt år.

Næstformand for Foreningen Danske Revisorer, Henrik Wilson.

Når en hackerstorm rammer dit firma

**Sådan arbejder it-verdenens Store Stygge Ulv.
Og så mange sikkerhedssystemer puster den omkuld i Danmark.**

Af kommunikationsrådgiver Michael Eisenberg, Intercom

Forestil dig et lille kontor i en trist industribygning i udkanten af en millionby i Kina, Rusland, USA eller – Danmark! En flok computere arbejder for fuldt tryk, nogle knækker passwords, andre sender mails ud til millioner af uskyldige brugere om, at de har vundet en iPhone 6S, og nu skal de bare klikke på et link, så er telefonen på vej.

En computer har knækket 60 koder inden for den sidste time og er i gang med at sprede ødelæggelse hos 60 firmaer. Næste computer i rækken har i efterhånden fem timer kæmpet med at knække et password, men endnu forgæves.

"Stop det bras, vi kan ikke bruge mere tid på det," siger chefen og vinker en medarbejder hen til sig. "Slet det password og lad os komme videre."

Det var dit password, de ikke kunne knække. De opgav, fordi du havde været for snedig og valgt at benytte et password, som selv enorm datakraft ikke kan knække på 24 timer.

Dit password er med andre ord ikke navnet på din ægtefælle eller "1234" eller "password". Eller er det? Er dit svar på det sidste spørgsmål et ja, så er din og dine kunders sikkerhed i farezonen.

Truslen i virkelighedens verden

Men er der nu så megen ondskab i verden. Svaret er ja – og mere endnu. Lad os se på to meget forskellige eksempler på organiseret it-kriminalitet, som kan ramme både store og små firmaer.

I Danmarkshistoriens største hackersag stadfæstede et enigt nævningeting ved Østre Landsret i juni i år byrettens dom over svenskeren Gottfrid Svartholm Warg for at have hacket CSC igennem en længere periode i 2012. Straffen blev 3½ års fængsel.

CSC er et stort computerfirma, der hoster en række offentlige registre, herunder CPR-registret. Ved hackerangrebene blev der kopieret data fra en række registre som CPR-registret, Rigspolitiets kørekort-register og et register over efterlyste personer inden for Schengen-samarbejdet. Datatilsynet har siden rettet en yderst alvorlig kritik af Rigspolitiet, fordi det havde tilsidesat helt enkle grundprincipper for datasikkerhed. Tilsynet kalder det "overordentligt kritisabelt." Hertil kommer, at politiet allerede i 2012 midt under angrebene var blevet advaret af SÄPO, det svenske sikkerhedspoliti, om, at hackerangreb fandt sted. Men man tog det ikke alvorligt nok.

Hos den ramte virksomhed, CSC, tog man heller ikke alvorligt nok på tingene. Ikke nok med at deres sikkerhedssystemer var fulde af huller, man tjekkede heller ikke løbende sin egen sikkerhed.

"I CSC-skandalen gik der 232 dage, før den blev opdaget," oplyser direktør Carsten Hvid Challet, TDC Sikkerhed.

Også angreb mod små firmaer

Angrebet fra den svenske hacker var klart nok rettet mod et stort firma, fordi man kunne få fat i oplysninger om mange personer og firmaer, og informationerne kunne udnyttes økonomisk.

Men også små firmaer er i søgelyset hos it-kriminelle. Mange danskere har i det seneste halve års tid oplevet at få en mail fra Post Nord, hvor man fik at vide, at en pakke var undervejs. Man blev bedt om at klikke på et link for at se, hvor langt pakken var kommet. Uheldigvis var der ingen pakke undervejs, i stedet fik man, når man klikkede på linket, malware ind på computeren, hvorved alle ens data blev krypteret. De var nu ikke længere tilgængelige. Nogle dage efter dukkede en ny mail op, nu kunne man mod at overføre penge få ophævet krypteringen. Læsere af "Danske Revisorer" kan selv gætte sig til, hvad der skete, når man overførte penge. Gættede man det ikke, er svaret: Intet.

Og så er vi tilbage ved historien i starten af artiklen om den gratis iPhone 6S. Her var der tale om en mail uden stavefejl eller oversættelsesfejl af maskintypen som "omsæt ideer hurtigt og nemt til professionelle resultater i orden." Desuden var layoutet af mailen så flot, at man et øjeblik kunne fristes til at tro, at det rent faktisk var en mail fra selveste Apple. Et blik på browserlinjen afslørede dog et langt og mærkeligt navn, der umuligt kunne have noget med den hæderkronede computer- og telefonproducent at gøre. Havde man sagt ja til at indløse sin gratis iPhone 6S, var ens computer blevet kompromitteret.

I denne udgave af "Danske Revisorer" har vi fokus på it-sikkerhed. Hvad kan du gøre for at sikre, at du selv og dine klienter ikke lider computernedbrud, tab af data, krav om løsepenge samt en ydmygende og dyr oplevelse?

Læs svarene på de følgende sider.

Løst og fast om it-sikkerhed

10 pluk fra medierne i efteråret 2015:

I en spørgeundersøgelse fra forsikringsselskabet Codan har næsten en tredjedel af virksomhederne i hovedstadsområdet været udsat for it-kriminalitet i 2014. Kilde: DR.

Hos forsikringsselskabet Topdanmark har knap 20.000 virksomheder i øjeblikket en forsikring mod hacking. To tredjedele af dem er kommet til i løbet af det seneste år. Kilde: DR.

Hackerforsikringer kan for eksempel dække det beløb, som hackere kræver, når de laver elektronisk pengeafpresning, skriver Computerworld.
Kilde: DR.

"Der går 12 sekunder fra en computer kommer online, til den er under angreb fra hackere og deres værktøjer." Sådan lyder det fra Kim Aarenstrup, nuværende chef for Nationalt Center for Cyber Crime (NC3) og tidligere it-sikkerhedschef i Mærsk og andre virksomheder. Han vurderer, at 90 % af alle danske virksomheder har haft uautoriseret besøg i deres it-systemer i en eller anden form – og at mange af dem slet ikke er klar over det, fordi deres sikkerhedssystemer er utidssvarende.
Kilde: DI.

Når det gælder mindre virksomheder, er direktør og partner Peter Kruse fra it-sikkerhedsvirksomheden CSIS ret sikker på, at der er store sikkerhedshuller og hackerangreb, som slet ikke bliver opdaget. Han opfordrer til, at man får styr på de mest basale opdateringer og virusprogrammer. Og at man sikrer, at der jævnligt laves en backup. Han hævder videre, at der er sket et boom i antallet af angreb, hvor hackere lukker de ansattes computere og kræver løsepenge for at lukke dem op.
Kilde: DI.

Statsrevisorerne har undersøgt sikkerheden i seks statslige institutioner: Energinet.dk, Banedanmark, National Sundheds-it, Statens It, Direktoratet for Kriminalforsorgen og Rigspolitiets Koncern IT.
Nu kritiseres sikkerheden i staten på ikke mindre end 70 punkter i en sønderlemmende rapport. Ingen af institutionerne har skiftet ikke-personlige passwords årligt, og størstedelen af de pågældende passwords er op til syv år gamle. Enkelte passwords er ikke blevet skiftet siden slutningen af 1990'erne.
Kilde: DR.

Efter en rundspørge konstaterer Dagbladet Børsen, at trusler mod it-sikkerheden ofte forbindes med hackere, virus eller andre udefra kommende faktorer. Men ifølge bladet kommer den største trussel mod virksomhedernes it-sikkerhed indefra.
Kilde: Dagbladet Børsen.

"Det er vanskeligt at overvurdere betydningen af IT-sikkerhed. Jo mere vi bruger teknologi, jo mere eksponerede er vi," skriver Berlingske i en artikel om megatrends i 2016. Avisen mener, at den største sårbarhed ikke er teknologien, men medarbejderne, og at uddannelse af medarbejderne i sikker IT-adfærd derfor er yderst vigtig.
Kilde: Berlingske

Jyllands-Posten noterer, at 83 % af danskerne mener, at online sikkerhed bør komme på skoleskemaet.
Kilde: Jyllands-Posten.

Tidsskriftet "Danske Revisorer" spørger i den anledning: Måske skulle vi sætte os selv på skolebænken, inden vi sender vores børn?
Kilde: "Danske Revisorer".

Anmeld Hacking og DDoS

Rigspolitiets Nationale Cyber Crime Center (NC3) modtager og behandler anmeldelser om hacking og DDoS (Distributed Denial of Service – distribueret servicenægtelse). Et DDoS-angreb lagde for eksempel Folketingets hjemmeside ned fredag den 11. december, hvor adgang til siden var umulig.

Har man været udsat for hacking eller et DDoS angreb, bør man anmelde det til politiet.
Hacking er omfattet af Straffelovens § 263 og er, når nogen uberettiget skaffer sig adgang til andres it-systemer, sociale profiler herunder mailkonti og programmer. Personen, der skaffer sig uberettiget adgang, kan enten slette, ændre eller kopiere data eller blot gøre sig bekendt med oplysningerne.

DDoS er omfattet af straffelovens § 293, stk. 2 og er en hændelse, hvor et it-system bliver udsat for et systematisk og massivt antal forespørgsler eller forsøg på indlogning på f.eks. en hjemmeside. Det vil typisk medføre, at adgang til siden ikke længere er mulig, eller it-systemet bagved er ophørt med at besvare forespørgsler på grund af overbelastning.

SkatteGuiden

Udfør skatterådgivning med sikkerhed for 0 fejl

Download gratis pakke med slutdokumenter på www.karnovguides.dk

(...) *Med SkatteGuiden kan vi nu - uden brug af andre værktøjer og ekstern bistand - give vores kunder en kvalitetssikret løsning på f.eks. skattefri virksomheds-omdannelse eller Aktieombytning.*

Torben Madsen, statsautoriseret revisor, TT Revision

(...) *Jeg har med SkatteGuiden gennemført en anpartsombytning og fusion på 25 % af den normale tid. Systemet er meget nemt at arbejde i, og anvisningerne undervejs af relevant lovstof er meget nyttige.*

Palle Thaisen, statsautoriseret revisor og partner, RIR Revision

Læs mere på www.karnovguides.dk

Få guides til

- Virksomhedsomdannelse
- Aktieombytning
- Fusion
- Spaltning
- Tilførsel af aktiver

Glæd dig også til primo 2016, hvor guiden for Virksomhedsskatteordningen (VSO) også kommer.

KARNOV GROUP

Alt, der kan gå galt, vil gå galt

I dag er hacking og spam-mails en del af den organiserede kriminalitet. Hvordan garderer man sig? Her får du eksperternes gode råd.

Af kommunikationsrådgiver Michael Eisenberg, Intercom

Antallet af sager om databedrageri er vokset fra 694 i 2009 til 4.583 i 2014. Altså mellem seks og syv gange så mange sager på kun fem år. Og det er kun toppen af isbjerget. Politiets statistikker er endnu ikke præcise for disse nye former for kriminalitet, og så er der de mange gange flere sager, hvor anmeldelse ikke finder sted.

Som revisor har man en særlig forpligtelse til at hjælpe sine klienter med at gardere sig mod it-kriminalitet. Tidsskriftet Danske Revisorer har derfor bedt om gode råd hos tre eksperter i it-sikkerhed. Vi har talt med en direktør i landets største teleselskab, med en it-rådgiver med eget enmandsfirma og med koncernchefen og den it-driftsansvarlige fra Foreningen Danske Revisorers største samarbejdspartner og rådgiver. Vi blev meget klogere.

TDC - landets største

Carsten Hvid Challet er administrerende direktør i TDC Sikkerhed, som er en del af landets største teleselskab, TDC. Han siger:

"Ligegyldig hvor meget eller hvor mange forsvarsværker du stiller op, eller du forsvarer dig, så er der så megen tid og penge bag organiseret kriminalitet, at det kan gå galt. Så det gælder om at nedbringe tiden, til man opdager, de er kommet ind i virksomheden. I CSC-skandalen gik der for eksempel mere end 200 dage, før den blev opdaget, hvad der vanskeliggør efterforskningen af, hvilket data der er blevet stjålet eller ændret.

Carsten Challet peger på antivirus, firewalls og sandboxing, som de store hjælpere, der fjerner 98 % af truslerne.

"De sidste to procent skal der mere til at klare. I TDC har vi til det formål Danmarks største Security Operations Center, også kaldet SOC," siger han.

"Er man revisor og behandler personoplysninger, skal man altid beskytte sig bedst muligt. Man er nødt til at entrere med en professionel it-mand eller et it-firma og få rådgivning," mener Carsten Challet.

Han kan også fortælle, at en ny EU-personforordning nu er på vej. Den handler om beskyttelse af personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger. Målet er under hensyntagen til udfordringerne fra nye teknologier at skabe en sammenhængende, stærk og moderne databeskyttelseslovgivning i hele EU.

Udvikling i it-sager hos politiet

	2009	2010	2011	2012	2013	2014
Hacking	39	146	42	40	95	167
Alvorlig hacking	4	0	1	2	0	11
Databedrageri	694	1340	559	1366	2421	4583

Kilde: Rigspolitiet

Note: En række økonomiske sager er reelt it-kriminalitet, men figurerer ikke i ovenstående skema.
Gengivet fra www.computerworld.dk

Forordningen vil stille krav til en virksomhed om, at brud på persondatasikkerheden i visse tilfælde skal anmeldes til myndighederne samt meddeles den ulovligt registrerede.

Og det vil koste penge, hvis man ikke lever op til forordningen:

"Der kan blive tale om bøder på op til 2 % af virksomhedens årsomsætning. Derfor er der en god business case i at sikre sig på it-sikkerhedsområdet" konstaterer Carsten Challet.

Et startsted for arbejdet med sikkerhed kan være dette: "I TDC sælger vi sikkerhed "in-a-box", hvor man får avanceret antivirus og firewall, plus at man for eksempel kan tilkøbe antivirus til mobiltelefoner samt andre ydelser," siger Carsten Challet.

Den uafhængige it-rådgiver

Sune Bielefeldt driver sit eget it-firma Bielefeldt fra Vester-Bisholt mellem Horsens og Juelsminde. Han betjener små og mellemstore virksomheder og har arbejdet med it i næsten hele sit liv.

"Det værst tænkelige, der kan ske for en virksomhed eller person, er, at alle data forsvinder uigenkaldeligt, siger Sune Bielefeldt, og tilføjer: "Backup er en svær disciplin, som kræver rettidig omhu, og konstant bevågenhed, og den slappes over tid i forhold til etablerede løsninger. Lige pludselig sker katastrofen, og så er det nogle gange for sent eller unødig besværligt."

Bielefeldt mener, at man grundlæggende skal sørge for, at de data, som er fundamentet for ens virksomhed, er forsvarligt beskyttet i flere generationer og led. Derudover er det en god idé at have en fuldstændig backup af ens computer, et image, som beskytter mod totalt systemnedbrud eller kryptering foretaget af fremmede gennem inficering.

"Ellers venter et par hårde dage eller uger med at få genskabt systemer og opsætninger, selv om data måske er intakte," siger Sune Bielefeldt.

Han fortæller, at hans revisor i forbindelse med regnskabsaflæggelse spørger, om der er styr på backupsystemer. Hvis der ikke kan fremvises dokumentation for backup og sikring af data, betyder det en påtegning i regnskabet. Det giver øget opmærksomhed og respekt om virksomhedens datadisciplin.

Det store konsulenthus

TimeGruppen er en uvildig rådgivningsvirksomhed inden for revision, investering, pension og forsikring. Udover lov om revisorlovgivning er man også underlagt regler fra Finanstilsynet. TimeGruppens grundydelse til Foreningen Danske Revisorer er skatte- og momsrådgivning samt kurser i alt inden for samme.

Koncernchef Jens Sørensen ser den menneskelige faktor som den største risiko:

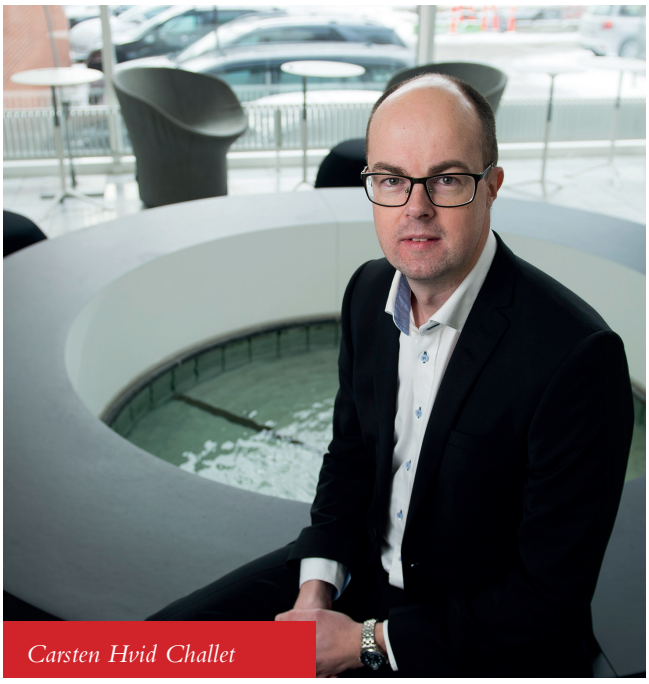
"Vi har fat i de bløde værdier, og det er vigtigt at have en virksomhedskultur, hvor det er okay at sige: 'Jeg tror, der er noget galt her.' Opfører tingene sig mærkeligt, skal man kunne hejse flaget og indrømme, at man er kommet galt af sted. Det gælder om at finde nålen i høstakken hurtigst muligt," siger Jens Sørensen.

Han mener, det er lidt af en skrøne, at mobiltelefoner skulle udgøre en stor risiko, når det gælder hardware:

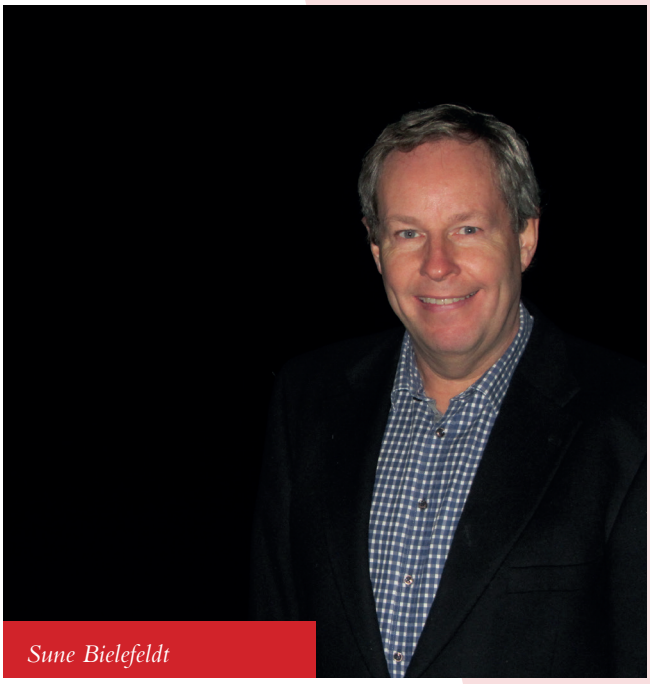
"De bærbare pc'er er en stor risiko, når de er ude af huset. Og kommer en person ind i vores virksomhed og ser en ledig computer, han kan arbejde med, bærbar eller stationær, så er der en risiko der. Alle er meget obs på at have kode på bærbare computere, men det er lige så vigtigt på de stationære," vurderer Jens Sørensen.

Årsagen er indlysende: «Risikoen for malware er til stede overalt. Otte ud af ti virksomheder har malware. Det er alt fra ting, der venter på at blive aktiveret, til opsnapning af e-mails, programmer der lurer på personoplysninger og så videre," begrunder Jens Sørensen.

"Al åben kommunikation er farlig, så man må anlægge en fornuftig vurdering," sammenfatter Jens Sørensen."



Carsten Hvid Challet



Sune Bielefeldt

Sådan garderer du dig

**Eksperterne giver gode råd om it-sikkerhed.
Her får du svar på typiske spørgsmål af:**

Administrerende direktør i TDC Sikkerhed
Carsten Hvid Challet **(CC)**

Sune Bielefeldt fra it-firmaet Bielefeldt **(SB)**

Koncernchef ***Jens Sørensen***, TimeGruppen **(JS)**

It-driftsansvarlig ***Kåre Olsen***, TimeGruppen **(KO)**

Har TDC en standardbrochure, der beskriver de sikkerhedsmæssige problemstillinger, som privatpersoner og erhvervsvirksomheder skal tage sig i agt for, når de benytter computer eller mobiltelefon?	**CC:** Nej det har vi ikke, vi har et blad, der hedder TDC Perspektiv med artikler om mange af disse emner. Ingen kunder er ens. Taler vi forskningsdata, persondata, eller hvad? Der er mange muligheder. Vi tager en samtale og udarbejder noget ud fra kundens krav.
Hvad kræves der af et godt password til en personlig computer? Og til en mobiltelefon.	**CC:** Jo mere kompliceret det er, jo bedre. Det skal også være til at huske. En kombination af store og små bogstaver og tal er godt. **SB:** En kombination af tal, store og små bogstaver og gerne specialtegn. Hvis muligt også på mobil (du kan se Bielefeldts næsten ubrydelige password i boksen "Bielefeldts password"). **KO:** Det skal have en vis kompleksitet. Vi kræver mere end otte tegn. Der skal også være koder på smartphones og iPads. Over halvdelen af virksomhedens dna ligger tilgængeligt i en mail og iPhone.
Hvilke typer password skal man undgå?	**CC:** Det mest brugte er password. Undgå ægtefælles eller kærestes og børns navne. SB: Brug ingen personnavne eller kun tal. KO: Brug ikke navn på børnene.

Bør man også benytte password, når man skal vække computer eller mobiltelefon fra standby tilstand?	**CC:** Ja, det synes jeg. Man skal låse den, hvis man går fra den. Har man mails på sin telefon, så bør man have password der også, eller i det mindste en pinkode. **SB:** Ja. Men hvad er situationen? Er man hjemme, er det en anden situation end et åbent kontorlandskab. Vi tilpasser ikke sikkerheden til de konstant ændrede forhold, vi er under. **KO:** Ja, det skal du, når du genoptager arbejdet.
Man modtager mange mails fra usikre afsendere på sin computer. Er det altid sikkert at klikke på dem og læse blot selve teksten?	**CC:** De fleste postprogrammer læser ikke billeder ind automatisk, men sker det, kan man komme galt af sted. **SB:** Det har tidligere været usikkert, men dagens antivirus sørger for, at det er mere acceptabelt. **KO:** Man skal anlægge en fornuftig vurdering. Man kan jo blive nødt til at modtage mails fra nogen, man ikke kender.
Skal man altid undgå at klikke på links i mail fra usikre afsendere.	**CC:** Man skal passe på ikke at klikke på links i mail fra nogen, hvor man ikke venter noget. Afsenders e-mailadresse kan røbe noget. Man kan også holde musen hen over linket UDEN at klikke og derved se, hvad der kommer op. **SB:** Ja, absolut. **KO:** Det er forbudt at klikke på vedhæftede filer i den slags mails.
Når man som privatperson foretager søgninger på sin egen computer fra sin hjemadresse og derefter går på internettet dagen efter på sin arbejdscomputer på arbejdspladsens fysisk adresse, så kan man opleve, at der popper annoncer op for de produkter, man har søgt på i sit hjem på en anden computer aftenen før. Hvordan kan dette lade sig gøre, og kan man undgå det?	**CC:** Det kan lade sig gøre ved, at man bruger Facebook eller Google begge steder, så kan de kæde de her informationer sammen. **KO:** Det kan være noget med login i browseren, hvor du bruger det samme login.
Facebook og LinkedIn er rigtig gode til helt automatisk at spore bekendtskaber – hvordan sker dette, og kan man undgå det?	**CC:** Facebook kan se, at det er samme konto begge steder.
Er Facebook og Google nogen, man skal passe meget på?	**CC:** Nej, de stiller en gratis service til rådighed, og de tjener penge på at sælge informationer videre. Så det er prisen, man betaler, for at det er gratis. Ellers må man lade være at bruge de gratis tjenester. **SB:** Facebook hører ikke til på en arbejdscomputer. Det tager tid og forstyrrer arbejdsprocesser, og der er potentiel risiko for, at data og kontakter bliver kompromitteret. Man må ikke gemme log-in data til Facebook på sin arbejdscomputer. Man risikerer, at ens arbejdskontakter kompromitteres. **KO:** Vi sikrer vores servere, og så lever vi med, hvis der er en arbejdsstation, der får et problem. Folk installerer ofte mere end de må. Så hegnet er omkring serverne via antivirus. Vi bruger En-able. Windows Defender er bedre end ingenting, men ikke at anbefale. Alle test viser, at det er den tunge dreng i klassen. Køb et AV-program og kom et trin højere op ad stigen.

Hvilke foranstaltninger skal man træffe for sit firmas hjemmeside?	**CC:** Det er vigtigt at sørge for, at de informationer, der ligger, ikke er nogle, man ikke vil have ud. Hvis hackere vil, kommer de ind på din hjemmeside. Man kan placere nogle firewalls foran. Det koster ikke en formue. Mange får bare oprettet en hjemmeside, hvor det er gratis, men beskyttelsen er så også derefter. Jeg er dog mere bekymret over hjemmesider med mange reklamer. Risikoen for at blive kompromitteret er større der. Her tænker jeg på hjemmesider med mange reklamer, som tusindvis besøger hver dag. På siden hentes der måske reklamer fra 20-30 annoncører. Er blot én af dem kompromitteret, får du malware med hjem. **SB:** Hvis man har aktiviteter som butik eller relationer med kundedata gemt, skal man have en mur af sikkerhed rundt om de data. Serviceudbyderen skal med ind over og diskutere, hvordan sikkerheden kan gøres god nok.
Er det sikkert at omtale bankkontonumre, medlemsnumre samt numre på kreditkort i en mail til nogen, man i øvrigt har tillid til, eller kan det opsnappes?	**CC:** Joh, jeg taler jo også med min egen revisor og sender ting over mail, men hvad sender jeg? Det er nok ikke der, man skal skrive sine kreditkortoplysninger. Men overordnet er e-mails ikke et sikkert sted at kommunikere. Man skal opveje brugervenlighed over for sikkerhed eller benytte sig af en sikker e-mailløsning. **SB:** Jeg mener ikke, at et kontonummer er noget, man kan kompromittere. Det står jo på en hver virksomheds faktura som offentligt tilgængelige data. Men man skal ikke sende brugernavne og adgangskoder over nettet, det er fy. **JS:** Vi anbefaler ikke at skrive bankkonto, kreditkortnumre eller personnumre i mails. Men den virkelige verden møder teorien, og hvor er grænsen for fornuft? **KO:** I min verden er der stor forskel på, om der er et vedhæftet dokument med data, eller man skriver det direkte i en mail. Den kan man læse, men det er sværere at læse pdf-filen.
Man hører om Echelon, som hævdes at spore terrorister, narkohandlere samt politisk- og diplomatisk information gennem intensiv overvågning af al trafik på internettet. Tror du, det også bliver brugt til kommercielt tyveri og brud på privatlivets fred?	**CC:** Der er tre typer hacking: Tidligere hackede man hjemmesider for at bringe politiske budskaber, nu er det mere kriminelle, der hacker, og så er der statssponsorerede hackere, der laver industrispionage. Jeg tror, alle nationer er lige gode om det. Mange ting kan man spore tilbage til Kina og Rusland, men om USA er dygtigere til at slette spor, ved jeg ikke. **SB:** Jeg tror, det sker, at der stjæles erhvervsdata fra Danmark. Men det modsatte sker jo også. Der spioneres overalt, men som privatpersoner er vi uinteressante.
Hvordan modtager man som revisor på en sikker måde klientoplysninger som foreløbig bogføring og lignende økonomiske oplysninger på en mail? Hvad skal klienten gøre?	**CC:** Der findes rent faktisk mulighed for at certificere e-mail, så man er sikker på, at den kommer fra den rette. **SB:** I en almindelig fornuftig handelsvirksomhed med 10-100 medarbejdere er der intet, der er industrihemmeligt i regnskaberne. Tallene kommer ud i Erhvervs- og Selskabsstyrelsens data. **KO:** Vi bruger ikke at kryptere materiale, men vi råder til, at man har et velfungerende antivirusprogram. Har man ikke det, kan virus komme med i dokumenterne over til modtager.

Hvordan sender man som revisor på en sikker måde regnskaber til klienten? I dag benytter de fleste nok en simpel pdf-fil uden kode. Er det nok? Hvad skal man gøre?	**CC:** Kode og pdf er intet værd. Det tager 30 sekunder at bryde. Er det noget, som bliver offentligt tilgængeligt, er det måske ikke så vigtigt. Vil man have kryptering, skal man tage fat i nogen, der kan hjælpe med det. Der findes utroligt mange små og store virksomheder, der kan give de få timers vejledning. **JS:** I min verden er det okay at sende regnskabsdata. De er jo offentligt tilgængelige alligevel. Kapitalfonde har nok kryptering mellem afsender og modtager.
Hvordan ser det ud med de nærmest daglige indberetninger, som revisor foretager til SKAT? Er de gængse måder at gøre det på sikre nok?	**CC:** Ja, det vil jeg sige, at det er. Men igen, hvis man bruger en computer, der ikke er godt beskyttet eller har malware, kan nogen kigge med på skærmen. **SB:** Udvekslinger af kontooplysninger bør ikke sendes over mail. TastSelv er sikkert nok, brug det. **JS:** Det går vi ud fra. Al åben kommunikation er farlig, men NemID beskytter kommunikationen. YasySelv er sikker, vi har ingen grund til at tro andet,
Hvordan betragter du som helhed og ud fra din viden sikkerheden i SKAT? Kan vi trygt overlade dem vore egne og vore klienters følsomme data og økonomiske oplysninger?	**CC:** Vi kender ingen historik, der er negativ. **KO:** Den er ok.
Og hvordan med Nets, banker og realkreditinstitutter, som revisorer også kommunikerer med?	**CC:** Man skal tænke over, hvad det er for personfølsomme oplysninger, man sender. **KO:** Vi anser generelt sikkerheden for ok.
Nye betalingsformer som MobilePay (Danske Bank) og Swipp (de andre banker) vinder frem. Hvordan er sikkerheden, hvad skal man passe på med?	**CC:** Det er to nye løsninger, hvor sikkerheden ER tænkt ind fra start. Desuden er det småbeløb, og forbrugeren hæfter ikke for svindel.
Mobiltelefoner: Hvordan sikrer man generelt sin mobiltelefon mod skadelige apps, der kan overtage kontrollen over telefonens indhold?	**CC:** Der er mange apps, som kigger i ens sms og e-mail. Det gælder om at have antivirus. Det fås ikke som standard på de to systemer Android og iPhone. Jeg anbefaler, at man bruger penge på at få antivirus. Tal med dit teleselskab. Jeg tror, det koster omkring 20 kr. om måneden.
Hvad er enhedskryptering i Android? Bør man bruge det?	**CC:** Brug det til at sikre din telefon. Hackere kan få adgang til data på telefonen, også uden at kende pinkode. Men er data krypterede, kan de ikke komme ind i dem.
Man hører, at visse apps har adgang til og må bruge alle ens data, herunder fotos på mobilen. Hvordan hindrer man det?	**CC:** Facebook kigger på mails, på fotos, på alt. Det kan være relevant, at MobilePay får adgang til kontaktoplysninger, men ikke relevant for den at få adgang til sms. De fleste telefoner spørger, før man giver apps lov at få adgang til data.
Hvordan er det med sikkerheden omkring NemID? Hvad skal man tage sig i agt for?	**CC:** Man bør kun benytte NemID på hjemmesider, hvor man er tryg. Husk at kigge i browserlinjen foroven, om man nu er det rette sted. Hvis du får en mail fra et stort pengeinstitut med teksten: "Vi har fået ny hjemmeside," ja, hvor sandsynligt er så det?

Bielefeldts password

Du kan skabe dig et sikkert password ved at følge nogle enkle regler.

Hackere råder over enorm computerkraft, der kan knække lette passwords på under et sekund. Derfor råder jeg til et password på mindst 11 tegn, hvor der både forekommer bogstaver, tal og specialtegn.

Det er bedst, hvis bogstaverne ikke danner et ord, for hackersystemer benytter hele ordbøger, som er hurtige at gennemløbe. Så find på et helt tilfældigt kodeord af typen khg2656&ovw (min. 11 tegn). Det er svært at knække både for nogen, der kender dig og hackere i et fjernt land.

Brug ikke ib2510anne uden specialtegn, hvis I har bryllupsdag den 25. oktober. Det kan gættes af nærtstående hackere, og den slags findes også.

Brug ikke din telefon eller computer til at gemme dine passwords, så er du alt for sårbar. Gem dem på en USB-nøgle, som du har et sikkert sted, så kan du let finde den frem og opdatere den. Bærer du USB-nøglen på dig under rejser, så sørg for at den er krypteret. Men opbevar den ikke sammen med din telefon og din computer. Hav evt. en kopi i papirformat. Mister du din USB-nøgle, er der kun en udvej, udskift alle koder straks.

Vil du kryptere en fil på din USB nøgle, er der flere muligheder:

• Benyt Microsoft Word, og sæt en sikker kode på dokumentet

• Benyt Winzip til at pakke filen ind (bedst). Winzip kan beskytte pakkede filer med password. Filen kan beskyttes med 128 eller 256 bit AES kryptering, så er den næsten ubrydelig. Se mere her: http://kb.winzip.com/kb/entry/109/

• Mange USB-nøgler leveres med egen krypteringssoftware.

Følger du disse tips, er du godt beskyttet – for nærværende.

Sune Bielefeldt, it-rådgiver

SKATTESAGSADVOKATERNE

Aalborg & København

Har dine kunder brug for skattesags- eller skattestrafferetlig ekspertise?

Skattesagsadvokaterne kan via vores samarbejde med FDR tilbyde fordelagtige vilkår i forbindelse med:

- Skatte-, moms- og afgiftssager
- Skatte-, moms og afgiftsstraffesager

Vi fører sager for alle instanser og i alle retskredse i Danmark angående danske og internationale forhold.

Vores ydelser for FDR medlemmers kunder:

- Vi fører skatte-, moms- og afgiftssager
- Vi arbejder som forsvarere i straffesager vedr. skat, moms og afgifter, hvidvask m.v.
- Vi udarbejder bindende svar for små og mellemstore virksomheder og selskaber, samt hovedaktionærer

Samarbejde med os:

- Vi tilbyder en gratis og uforpligtende gennemgang af skatte-, moms-, og afgiftsager
- Vi giver altid en ærlig og reel vurdering af sagen
- Vi samarbejder gerne med klientens primære rådgivere om sagen
- Vi fører ikke andre typer sager end skatte- og skattestraffesager hvorfor vi kun er involveret med klienten indtil den pågældende sag er slut

Kontakt skattepartner Tobias Stenkær Albrechtsen advokat (H):

tlf. 70 20 33 13 eller tsa@skattesagsadvokaterne.dk for en uformel drøftelse.

www.skattesagsadvokaterne.dk

Algade 31, 9000 Aalborg

Østergade 55, 1100 København K

Har vi en sikkerhedspolitik?

Ja, det har man hos tre større revisionsfirmaer, der er medlemmer hos Foreningen Danske Revisorer. Og ja, man gør sig mange overvejelser om sikkerhed.

Af kommunikationsrådgiver Michael Eisenberg, Intercom

Tidsskriftet "Danske Revisorer" har taget pulsen på sikkerheden i tre typiske danske revisionsfirmaer. Vi har talt med partner, revisor Martin Skovholm fra Revisorgården Holbæk, med økonomikonsulent, revisor Britta Engholm Nielsen fra landboforeningen Gefion i Sorø og med partner, revisor Bo Bødker fra Revisorgården i Odense. Den stigende it-kriminalitet gør indtryk, og man spørger løbende sig selv, om man gør det godt nok.

Det mest grundlæggende spørgsmål, når det gælder it-sikkerhed er: Har I en overordnet sikkerhedspolitik for jeres arbejde med egne og kunders data?

"Ja, det har vi," kommer det helt enslydende fra alle tre revisorer.

"Målet er, at vi skal bevare 100 procent tavshedspligt om alt, vi beskæftiger os med," siger Martin Skovholm. I Holbæk opbevarer man alle elektroniske data sikkert i en cloudløsning på eksterne servere, der er intet i selve huset. I Odense har man servere i huset, og man tager egen backup her på to hardware, den ene tager man med hjem hver dag.

Passwords til computere og mobiltelefoner kan være et kildent emne. Hvordan foregår det?

I Holbæk genererer man automatisk passwords, der kan huskes, til hver medarbejder.

"Vi har måske en enkelt øm tå, for vi skifter dem måske ikke helt så ofte, som vi burde. Det burde ske en gang om måneden," erkender Martin Skovholm.

"I Gefion har vi helt klare politikker for, hvor tit vi skifter. I vores økonomiprogram er det hvert halve år," fortæller Britta Engholm Nielsen. Man har dog ikke regler for udarbejdelse af passwords, det klarer medarbejderne selv. I Odense har man ingen politik om passwords til mobil.

Er Facebook en skurk?

Alle tre revisorer og deres kolleger benytter Outlook som deres vigtigste kommunikationsmiddel. Og alle ved, at der er farer forbundet med det.

"En stor fare er, at man ikke tjekker, hvor man sender tingene hen. Er der fem, der hedder Hans, så kan det ryge til den forkerte. Og går det til en konkurrerende virksomhed, kan det være en katastrofe," vurderer Martin Skovholm. I Holbæk sker der særlig backup af Outlook hver dag.

"Vi har talt om, hvorvidt vi burde kryptere, men det er ikke nået op på beslutningsniveau endnu," fortæller Britta Engholm Nielsen fra Sorø. →

Martin Skovholm

Bo Bødker

I Odense bruger man en del penge på virusprogrammer: "Vi har Symantec, som kører hele tiden og tjekker alt, også mails. I det øjeblik, vi åbner en fil, skulle en virus gerne blive fanget der. Medarbejderne ved, at de ikke skal lukke mærkelige mails op," siger Bo Bødker.

"Generelt er vor politik, at man ikke er på Facebook," mener Martin Skovholm. Han vil begynde at overveje, om det er et sikkerhedsproblem overhovedet at have Facebook på computeren.

"Man må godt bruge Facebook hos os, der er ingen politik om, at vi ikke må, og jeg bruger det ikke selv, men der er et par kolleger, der gør," siger Britta Engholm Nielsen.

Bo Bødker vurderer: "Umiddelbart vil jeg sige nej til Facebook, for det har ikke noget med arbejdet at gøre."

Uinteressant at stjæle data

Mange hjemmesider bliver hacket, men hjemmesider er ikke det store problem hos revisorerne. Hvis der er webshop forbundet hos kunderne, skal man tage det alvorligt, men ellers kan hjemmesiden hurtigt komme op igen, er vurderingen hos de tre.

En af de tunge drenge i bankverdenen, Barclays i London, skriver i et standardsvar til "Danske Revisorer", at e-mail er en usikker kommunikationsmetode, og at man derfor ikke bør nævne kontonumre, detaljer om medlemskaber samt kreditkortnumre i en e-mail. Det gør indtryk:

"Det er et meget følsomt emne, svært at vurdere. Jeg synes, det er ok at skrive kontonummeret, det er ikke nok til, at der kan ske misbrug," mener Martin Skovholm.

"Jeg kan ikke helt se, hvor farligt det er. Hvor stor skal sikkerheden være? Der skal være måde med indsatsen," vurderer Britta Engholm Nielsen.

Bo Bødker siger: "Vi nævner oplysninger om kontonumre, og jeg kan ikke se, hvordan man skal kunne misbruge det. PIN-koder og den slags skriver man derimod ikke i en mail."

Hvordan modtager de tre revisorer klientoplysninger som foreløbig bogføring og lignende? Hvilke krav har de til klienten?

"I dag sendes det elektronisk. Det er ikke så følsomt. I et § 21-selskab vil det være noget andet," mener Martin Skovholm.

"Vi har ingen særlige krav til, hvad kunder må sende på mail. Et brev kan jo også blive opsnappet, og der sender vi de samme ting," mener Britta Engholm Nielsen.

Bo Bødker tilføjer: "Hvem er det interessant for? Næppe nogen med de små kunder vi har."

TastSelv vurderes som sikkert

Nu skal det færdige regnskab så tilbage fra revisor til klienten. Hvordan foregår det? Både i Holbæk, Sorø og Odense sender man en pdf-fil uden kode.

"Det mener jeg er ok. Det er uinteressant for andre," vurderer Martin Skovholm.

"Hvis noget skal strammes op, så kommer der nok besked fra it-afdelingen. Jeg mener ikke, der er nogen, der har glæde af de oplysninger," tilføjer Britta Engholm Nielsen
Bo Bødker mener: "Det er personlige og følsomme oplysninger, men hvem har interesse i det? Vore kunder har ikke offentlighedens interesse."

Hvordan ser det så ud med de nærmest daglige indberetninger, som revisor foretager til SKAT? Er de gængse måder at gøre det på sikre nok?

"I TastSelv er der en kommunikationsvej, der fungerer. Man bruger det som et lukket system, og det virker rimeligt sikkert," vurderer Martin Skovholm.

En ting, der højner sikkerheden ved TastSelv, er, at det er klienten, der har givet revisor autorisation til at kunne se data.

"Når jeg så logger på, bruger jeg min medarbejdersignatur samt mit eget, personlige password, som jeg selv har dannet ved et bestemt system, jeg bruger. Derudover skal man jo også have nøglekort for at kunne komme ind på TastSelv," forklarer Britta Engholm Nielsen.

Ingen er fuldkommen

Generelt er de tre revisorer trygge, når de på klientens vegne kommunikerer med Nets og banker:

"Min fornemmelse er, at sikkerheden er ok, fordi vi bruger NemID, hver gang vi logger på, og alt, der kører over det, må være sikkert," vurderer Bo Bødker.

Endelig er de tre revisorer opmærksomme på, om klienternes sikkerhed er i orden. Man beder om at få dokumentation for, at der styr på backupsystemer og sikkerhed, og det skrives ind i regnskabserklæringen.

"Vi har svært ved at revidere sikkerheden i et firma, derfor indeholder ledelsens regnskabserklæring mange punkter, som de skriver under på, og sikkerhed er et af de punkter," forklarer Bo Bødker.

Det vil næppe være forkert at konkludere, at der er en høj bevidsthed om it-sikkerhed i såvel Revisorgården Holbæk som landboforeningen Gefion og Revisorgården i Odense. Bevidstheden handler også om, at man ikke kan nå det fuldkomne.

"Måske burde man ikke bruge samme password flere steder, men på den anden side, hvor mange passwords kan man huske?" smiler Britta Engholm Nielsen som afslutning.

Britta Engholm Nielsen

Sikkerhedstillelse ved virksomhedsordningen

Det følger af virksomhedsskattelovens § 10 stk. 6, at når aktiver i virksomhedsordningen stilles til sikkerhed for gæld, der ikke indgår som en del af virksomhedsordningen, vil sikkerhedsstillelsen som hovedregel udløse beskatning.

Af Advokat (H) Tobias Stenkær Albrechtsen og Vidensjurist Ph.d. (jur) Thomas Rønfeldt, begge fra Skattesagsadvokaterne ApS

Dette gælder for sikkerhedsstillelse, der foretages fra og med den 11. juni 2014. Sikkerhedsstillelse udløser dog ikke beskatning, såfremt nye sikkerhedsstillelser efter d. 10. juni 2014 erstatter allerede stillede sikkerheder, dog under forudsætning af at den allerede etablerede sikkerhed ikke forøges.

Der er ligeledes en række meget væsentlige undtagelser til forbuddet mod disse sikkerhedsstillelser.

Bestemmelsen har mødt meget modstand grundet bredden og uklarheden af afgrænsningen. Kritikken synes berettiget, idet det gentagne gange i forarbejderne og høringssvar er afvist at konkretisere afgrænsningen nærmere, end at risikoen for omgåelse medfører, at vurderingen af de enkelte transaktioner må bero på en konkret vurdering.

Sådanne formuleringer skaber en vis grad af usikkerhed, hvilket det meget store antal bindende svar, der er afgivet, og de mange bindende svar, der afventer, vidner om. Skatterådet har senest d. 3. december underkendt, at beskatningen skal ske udenom hæverækkefølgen, hvilket yderligere viser de udfordringer bestemmelsen giver, også for lovgiver.

Derudover er det vores erfaring, at virksomhedernes pengeinstitutter ikke i fuldt omfang er bekendte med bestemmelsens indhold. Dette gælder særligt bestemmelsens rækkevidde, hvilket ganske givet vil give anledning til udfordringer i forhold til de krav, der stilles til sikkerheder i forbindelse med kundernes arrangementer.

Vi vil med denne artikel samle op på de vigtigste faldgruber, den seneste praksis og status pr. november 2015.

Hvad er sikkerhedsstillelse, og hvad er ikke sikkerhedsstillelse?

Kaution

Kautioner kan efter en konkret vurdering være omfattet af de dispositioner, der udløser skattepligt. Der kan eksempelvis være tale om et arrangement i et pengeinstitut, der har en karakter, hvorefter der er en klar sammenhæng mellem muligheden for kredit i privatsfæren og indestående i virksomhedsskatteordningen.

Det afgørende i henhold til lovens forarbejder, og den seneste praksis, er, om kautionen giver mulighed for kredit i privatsfæren.

Dette vurderingsparameter er fastslået i en række afgørelser, hvor udgangspunktet i forhold til kautioner er, at en personlig kaution ikke i sig selv er nok til, at aktiver, der indgår i virksomhedsordningen, anses for at være stillet til sikkerhed for gæld, der ikke indgår i ordningen.

En kaution kan dog efter en konkret vurdering alligevel konkret udløse beskatning, men dette vil typisk kræve, at der er sammenhæng mellem den stillede kaution og muligheden for kredit i privatsfæren.

SKAT udtalte herom i en konkret sag, at:
"henset til det oplyste forudsætter SKAT, at den stillede kaution ikke indgår som led i et arrangement, der helt eller delvist har som formål at skaffe kredit for spørger i privatsfæren"
Det fremgår således også, at var kautionen stillet for at skaffe kredit i privatsfæren, ville det potentielt set – og formentligt også reelt set – have udløst skat i virksomhedsskatteordningen.

Aftaleretlige sikkerhedsstillelser

Aftaleretlige sikkerhedsstillelser kan eksempelvis være boslodskrav i forbindelse med skilsmisse, hvilket en helt ny afgørelse viser. Stilles aktiver i virksomhedsskatteordningen således til sikkerhed for et boslodskrav i forbindelse med skilsmisse, vil dette altså udløse beskatning. I afgørelsen var det den aftalemæssige sikkerhedsstillelse, der gjorde udslaget.

Havde den tidligere ægtefælle derimod foretaget udlæg til sikkerhed for sit krav, ville dette som udgangspunkt i henhold til den afsagte afgørelse ikke udløse beskatning, da der i et sådan tilfælde ikke ville være tale om en aftalt sikkerhed.

Det er ikke svært at forestille sig, hvordan bestemmelsen herefter vil blive udfordret i praksis, hvor parter i en eventuelt skilsmisse, ikke kun den traditionelle, men også andre tilfælde, vil undgå at lave aftaler, men vente på misligholdelse og foretage udlæg.

Heraf følger ligeledes, at tvungen sikkerhedsstillelse, eksempelvis i form af udlæg, ikke er omfattet af de dispositioner, der udløser skattepligt, da der ikke foreligger en aftaleretlig sikkerhedsstillelse.

Hvorvidt dette kan opretholdes betingelsesløst, forekommer dog ikke oplagt, da det er debitor, der har henvisningsretten til de aktiver, der kan foretages udlæg i. Henvises der til udlæg i aktiver i virksomhedsordningen frem for eksempelvis aktier og anparter, der ikke er i ordningen, men giver fuld dækning, er det ikke oplagt, at anvisning af aktiver i virksomhedsskatteordningen skulle falde uden for skattepligten som følge af, at der ikke er tale om aftalt sikkerhedsstillelse.

Modregning, alskylderklæringer og pantsætningsforbud
Modregning, alskylderklæringer og pantsætningsforbud kan efter omstændighederne også være omfattet af forbuddet.

I en konkret sag blev skatterådet bedt om at tage stilling til, om etablering af en privat kassekredit på 200.000 kr., uden nogen former for sikkerhed, ville være en overtrædelse af stk. 6.

Bekymringen gik helt konkret på bankens modregningsret med midler i virksomhedsordningen, hvor der var ikke ubetydelige kontantbeholdninger.

Det fremgår af forarbejderne til loven, at udgangspunktet er, at det forhold, at et pengeinstitut har en generel modregningsret, ikke er nok til, at aktiverne i virksomhedsordningen anses for at være stillet til sikkerhed. Dette udgangspunkt gælder dog ikke, hvis en konkret vurdering viser, at der er en klar sammenhæng mellem muligheden for kredit i privatsfæren og aktiver i virksomhedsskatteordningen. Dette gælder særligt, hvis der ikke stilles sikkerhed for det private engagement med private aktiver.

SKAT udtalte i den konkrete sag, at der efter SKATs opfattelse må henses til, om det kan antages, at låntager ville kunne have opnået samme kreditfacilitet, hvis ikke långiver anvendte aktiverne i virksomhedsordningen, hvilket var tilfældet i den konkrete sag, hvorfor transaktionen ikke udløste skattepligt.

Heraf følger en særdeles vigtigt pointe. Der kan risikeres beskatning, hvis der oprettes en kreditfacilitet, der alene kan opnås grundet modregningsret med aktiver i virksomhedsskatteordningen, hvis der ikke er private aktiver, der ville muliggør kreditfaciliteten. Dette gælder altså uanset, at der ikke stilles formel sikkerhed. Dette er en ofte overset pointe, idet de færreste er opmærksomme på, at modregningsretten kan udgøre et problem i relation til § 10 stk. 6.

Pantsætning af P/S andele
Hvorvidt pantsætning af P/S andele er omfattet af § 10 stk. 6 er et særdeles relevant spørgsmål, der da også i forbindelse med lovens vedtagelse blev stillet. Svaret herpå var ganske kort og præcist, at det ville en sådan pantsætning være.

Undtagelser

Sædvanlige forretningsmæssige dispositioner, stk. 7
Det fremgår af lovens ordlyd og forarbejderne, at der efter stk. 7 kan anvendes aktiver, der indgår i virksomhedsordningen, til sikkerhed for gæld, der ikke indgår i virksomhedsordningen, hvis det sker som led i en sædvanlig forretningsmæssig disposition.

Sædvanlige forretningsmæssige dispositioner er i sagens natur et meget vidt begreb, og uanset det anvendes i flæng i skatteretten, er det ikke særligt præcist defineret.

Bestemmelse i stk. 7 er et af de punkter, der har givet anledning til kritik, idet det stort set er umuligt at vide, om en disposition/transaktion er indenfor eller uden for grænsen uden at skulle anmode om bindende svar.

Det ligger dog fast, at for at en disposition i forhold til stk. 7 kan siges at være en sædvanlig forretningsmæssig disposition, skal den tjene et forretningsmæssigt formål for den skattepligtige virksomhed under virksomhedsordningen.

Dette kan eksempelvis være tilfældet, hvis der er løbende samhandel mellem virksomheden i virksomhedsordningen og låntager, som afstedkommer behovet for sikkerhedsstillelse som et led i den sædvanlig forretningsmæssig samhandel.

Derudover skal sikkerhedsstillelsen tjene et forretningsmæssigt formål for virksomheden i virksomhedsordningen. Dette medfører, at sikkerhedsstillelsen eksempelvis skal være foretaget på armslængdevilkår, og at modydelsen for sikkerhedsstillelsen skal afspejle den risiko, som virksomheden i virksomhedsordningen påtager sig ved at stille sikkerhed for eksempelvis tredjemands gæld.

Der behøver ikke være tale om en særskilt modydelse, idet modydelsen kan være integreret i parternes samlede udvekslinger.

En helt ny afgørelse viser, hvor vanskellig grænsedragningen kan være. I den konkrete sag, der var et bindende svar, ønskede skatteyderen at overføre aktiver fra virksomhedsordningen til et nystiftet selskab. Skatteyderen ville kautionere for en kreditramme til selskabet på 5.000.000 kr.

Udfordringen i forhold til stk. 7 var flere. For det første oversteg kreditrammen i meget betydeligt omfang den private formue, hvorfor kautionen kun havde en reel værdi, når der blev henset til indeståendet i virksomhedsordningen.

SKAT fandt i sin udtalelse, at sikkerhedsstillelsen ikke var sket på armslængdevilkår, idet SKAT fandt, at sikkerhedsstillelsen rakte langt ud over, hvad der ville være sædvanligt, hvis ikke parterne var interesseforbundne. Allerede af disse grunde kunne sikkerhedsstillelsen/kautionen ikke anses for sket som led i en sædvanlig forretningsmæssig disposition.

Udfordringen var derudover, at skatteyderen fik et stiftertilgodehavende i selskabet, som i kraft af kautionen for selskabets driftskredit, kunne fungere som en kreditfacilitet i privatsfæren.

Skatterådet var enige med SKAT, og tilføjede derudover, at:
"Skatterådet har imidlertid tillagt det særligt vægt, at spørger i denne sag via stiftertilgodehavendet i det selskab, hvortil minkdyrene overdrages, får adgang til den kreditfacilitet, der med afsæt i kautionen etableres i selskabet, og at spørger dermed kan finansiere sit privatforbrug m.v. ved træk på dette tilgodehavende."

Det følger endelig af forarbejderne til loven, at familielån i forbindelse med generationsskifte kan være forretningsmæssigt begrundet, men at dette skal vurderes helt konkret. Altså igen en formulering der giver anledning til at søge bindende svar.

Pant i fast ejendom, stk. 8
Der ses i henhold til VSL § 10, stk. 8 bort fra en sikkerhedsstillelse for gæld med pant i den private del af en ejendom, hvoraf en del er holdt uden for virksomhedsordningen efter reglerne i VSL § 1, stk. 3, 2. og 3. pkt. Dette er altså gældende for de såkaldte blandede benyttede ejendomme.

Dette medfører således, at det er muligt at stille værdien af den private del af den blandede benyttede ejendom til sikkerhed. Dette dog under forudsætning af, at den private gæld, der stilles sikkerhed for, ikke overstiger værdien af den private ejendom, der tjener til bolig for skatteyderen.

Udskiftning af sikkerhed med anden sikkerhed, stk. 9
Bestemmelsen om skattepligt gælder ikke for sikkerhedsstillelse, der etableres fra og med den 11. juni 2014 til og med den 31. december 2017, men kun såfremt sikkerhedsstillelsen afløser en sikkerhedsstillelse, der eksisterede den 10. juni 2014, og alene såfremt sikkerheden ikke forøges i forbindelse med udskiftningen af den eksisterende sikkerhed.

Værdien af sikkerhedsstillelsen pr. 10. juni 2014 opgøres pr. 10 juni 2014, som det laveste beløb af enten gældens kursværdi eller sikkerhedsstillelsens størrelse.

Det er oplagt, at denne formulering giver anledning til udfordringer i forhold til eksempelvis flydende sikkerheder i form af virksomhedspant.

Hvad er konsekvensen af overtrædelse af § 10 stk. 6?

Stilles aktiver i virksomhedsordningen til sikkerhed for gæld, der ikke indgår i virksomhedsordningen, uden at transaktionen omfattes af en af undtagelsesbestemmelserne, anses det laveste beløb af enten gældens kursværdi eller sikkerhedsstillelsens størrelse for overført til skatteyderen personligt.

Opgørelsen af beløbet sker på det tidspunkt, hvor der stilles sikkerhed.

Sikkerhedsstillelsens størrelse opgøres som det laveste beløb af enten gældens kursværdi eller sikkerhedsstillelsen, det vil sige aktivernes handelsværdi. Det er oplagt, at denne formulering giver anledning til udfordringer i forhold til eksempelvis flydende sikkerheder i form af virksomhedspant.

Det fremgår af forarbejderne til § 10 stk. 6, at det beløb, der herefter kommer til beskatning, anses for overført uden for den almindelige hæverækkefølge.

Der er ligeledes ingen tvivl om, at dette har været intentionen med bestemmelsen, men udfordringen derved er, at det fremgår af § 10 stk. 6 ordlyd, at beløbet anses for "overført", uden at det i lovteksten er defineret, om dette skal forstås som indenfor eller udenfor hæverækkefølgen i § 5.

Spørgsmålet var temaet i et helt nyt bindende svar offentliggjort d. 3. december, hvor Skatterådet fik mulighed for at udtale sig om spørgsmålet. Svaret var meget klart:
"Det fremgår klart af lovforarbejderne til virksomhedsskattelovens § 10, stk. 6, at lovgivers udtrykkelige intention har været, at konsekvensen af, at virksomhedens aktiver stilles til sikkerhed for privat gæld, skal være, at der sker beskatning af et beløb uden om hæverækkefølgen i virksomhedsskattelovens § 5.

Skatterådet nærer imidlertid betænkelighed ved at lægge afgørende vægt på lovgivers intention. Efter Skatterådets opfattelse er ordlyden af virksomhedsskattelovens § 10, stk. 6 ikke tilstrækkelig klar til at udgøre en selvstændig beskatningshjemmel. Skatterådet finder således, at den mest naturlige forståelse af ordlyden af lovens § 10, stk. 6, er, at de deri nævnte overførsler skal anses for foretaget i overensstemmelse med virksomhedsskattelovens § 5."

Dette er således status d.d., og det er uklart, hvad rækkeviden bliver af denne udtalelse, som dog må forventes at ville medføre en præcisering i loveteksten, så ordlyden bliver i overensstemmelse med lovgivers intentioner. Imidlertid er det glædeligt, at der endelig er nogle, der igen, efter mange års fravær, begynder at stille sig spørgende overfor alle de "hjemler", som SKAT mener at have. Alt for mange gange kommer SKAT frem til en beskatning, der er yderst tvivlsom i forhold til loven og dennes ordlyd.

Uanset hvad udfaldet imidlertid bliver, gælder det om at holde tungen lige i munden og følge meget nøje med i den praksis, der kommer med de talrige bindende svar, der er indbragt for SKAT, da fejltrin kan blive særdeles kostbare.

Der kan således kun opfordres til, at der indhentes bindende svar, hvis der er den mindste tvivl.

Mere vejledning og færre bøder i fremtiden

Foreningen Danske Revisorer har i de sidste par år sat en del fokus på revisorernes kvalitetskontrol og sanktioner for overtrædelser, hvilket Danske Revisorers læsere har kunnet følge tæt. Vi har gjort politikerne opmærksomme på vores holdning til den nuværende gennemførelse af kvalitetskontrollen blandt revisorerne.

FDR går uden tøven ind for, at der skal være en kvalitetskontrol og i særdeleshed også vigtigheden i at højne revisionernes og revisorernes kvalitet, men vi har samtidig arbejdet på at åbne politikernes øjne for en alternativ strategi ved sanktionering, så formelle fejl bedømt af Revisornævnet blot fører til påtale og vejledning frem for urimelige store bøder.

Det er med stor glæde, at vi nu kan se, at vores arbejde har båret frugt. I forslaget til den nye revisorlov, som Erhvervsstyrelsen har sendt i høring den 21. december 2015, bliver der lagt op til, at kvalitetskontrollen fremover vil have fokus på anbefalinger til forbedringer og opfølgning herpå. Mindre sager vil i den forbindelse i højere grad afsluttes med påbud eller påtale fremfor som nu, hvor sagerne indbringes for Revisornævnet og medfører bødesanktioner. I sager, hvor der er tale om grove overtrædelser, foreslås der nye sanktionsmuligheder, så der kan sættes effektivt ind i denne type af sager. Det vil sige, at man vil ændre sanktionssystemet med lempeligere sanktioner for mindre førstegangsforseelser og til gengæld hårdere sanktioner ved særligt grove overtrædelser.

I forslaget lægges der ligeledes op til, at fremtidens kontrol og kvalitetskontrol af revisionsvirksomheder og revisorer vil være mere risikobaseret. Revisionsvirksomheder, der reviderer mindre virksomheder (klasse B og C) af offentlighedens interesse, skal kvalitetskontrolleres hvert 6. år. Revisionsvirksomheder, der udelukkende reviderer klasse B-virksomheder af ikke-offentlighedens interesse, skal kvalitetskontrolleres efter et risikobaseret system, hvor der ikke er angivet et nærmere fastsat tidsmæssigt interval. Nogle virksomheder vil derfor skulle undergå kontrol lidt hyppigere og andre lidt sjældnere.

Kvalitetskontroller, der er i gang ved overgangen til den nye lov, bliver færdiggjort i henhold til de gamle regler.

Det eksisterende Revisortilsyn og Revisorkommission nedlægges, og det foreslås at få etableret et rådgivende Revisorråd i stedet. Dette betyder, at Erhvervsstyrelsen bliver ansvarlig for tilsynet med revisorer og revisionsvirksomheder.

Foreningen Danske Revisorer arbejder i skrivende stund på et høringssvar på lovforslaget.

Af Susanne Holm, Sekretariatsleder, Foreningen Danske Revisorer

Foreningen Danske Revisorer fortsætter det gode samarbejde med Syddansk Universitet i 2016.

SDU Erhverv arbejder for at bringe virksomhederne tættere på de studerende og FDR arbejder for at blive mere synlige over for de studerende. SDU Erhverv tilbyder virksomheder og faglige organisationer muligheden for at profilere sig over for de studerende på Syddansk Universitet ved at blive erhvervspartnere – og det er det, at FDR fortsat har valgt at være for at imødekomme ønsket om øget synlighed.

I SDU Erhverv hjælper de med spørgsmål om job og karriere, der dukker op undervejs i de studerendes studium – uanset om de lige er startet eller er ved at lægge sidste hånd på specialet. Her kan FDR også bidrage med at hjælpe de studerende – f.eks. med indsamling af data til specialet.

Samarbejdet betyder også, at vi løbende bliver indbudt til arrangementer, hvor de studerende og FDR får mulighed for at komme i dialog med hinanden. I det forgange år har vi været aktive på to af SDU's matrikler – to gange i Odense og 1 gang i Kolding. Vi har været synlige på uddannelsesstederne i form af Company Dating, som er et større arrangement i Odense, hvor flere af SDU's erhvervspartnere er indbudt, og i form af to pit-stops, som er vores mulighed for at booke en stand i nogle timer på en forud aftalt dato.

Vi har haft en meget positiv oplevelse og nogle gode dialoger med de studerende. De studerende har været positive, videbegærlige og har meldt sig ind i FDR, hvilket vi selvfølgelig kun kan være stolte af. Studerende har mulighed for at blive medlem helt gratis, og der er ingen binding til et eventuelt senere betalt medlemskab.

Vi samarbejder dog også om andre ting, idet SDU Erhverv formidlede kontakten til en af vores undervisere på det meget roste kursus "Risici og væsentlighed med udgangspunkt i FDR-audit", som blev afholdt i slutningen af november 2015. I tilknytning til dette vil vi gerne henvise til artiklen i dette blad – "Risiko og væsentlighed ved revision af små virksomheder" skrevet af Rikke Holmslykke Kristensen, Studielektor, Institut for Entreprenørskab og Relationsledelse, Syddansk Universitet.

Vi har derfor besluttet os for at fortsætte dette gode samarbejde i 2016, idet det er givtigt for alle parter – SDU, de studerende og FDR. Vi ser derfor frem til, at FDR fortsat vil være en synlig erhvervspartner for de studerende på Syddansk Universitet i 2016.

Af Susanne Holm, Sekretariatsleder, Foreningen Danske Revisorer

Foreningen Danske Revisorer

Christian Vester, Erhvervspartneransvarlig hos SDU Erhverv, udtaler:

"Hos Syddansk Universitet, SDU Erhverv, er vi meget glade for vores erhvervssamarbejde med FDR. Vi ser et stort potentiale i at samarbejde med en professionel og målrettet faglig organisation, som henvender sig til en specifik gruppe af vores studerende. Med en stor interesse for fremtidens medarbejdere, og et særligt fokus på SMV'erne, som præger vores Region Syddanmark, sætter SDU Erhverv stor pris på det arbejde, som FDR udfører i brobygningen mellem vores fælles målgrupper."

Revision af andelsboligforeninger

Af registreret revisor Bjarne Aalbæk, Faglig Afdeling a/s.

På medlemmernes del af hjemmesiden fdr.dk ligger en artikel om forhold, der skal tages i betragtning, når revisor reviderer andelsboligforeninger.

Det er min opfattelse, at revision af andelsboligforeninger udgør en uforholdsmæssig stor risiko i forbindelse med kvalitetskontrollen, og jeg vil derfor gerne gøre opmærksom på de problemstillin-ger, der relaterer sig til revisionen.

Artiklen beskriver blandt andet, om andelsboligforeninger kan fravælge revision, og fremgangsmå-den for hvordan dette gøres rent praktisk. Der er forslag til formuleringer.

Der er også en beskrivelse af de mest gængse revisionsregler for andelsboligforeninger, herunder revisionsaftale, planlægningsnotat, advokatbrev og revisionsprotokol.

Ligeledes er der en beskrivelse af revision af nøgleoplysningerne, revision af andelsværdien og revi-sion af ejendommen. Der er også en beskrivelse af den regnskabsmæssige begrebsramme, som har betydning 5 steder i regnskabet.

Artiklen viser også eksempler på formulering af den supplerende oplysning, som oftest er et krav i andelsboligforeningers regnskaber.

Artiklen gør således opmærksom på de mest gængse problemstillinger, man som revisor skal være opmærksom på netop nu ved revision af andelsboligforeninger.

Virksomhedsformer - få overblikket her

Det er vigtigt at overveje valg af virksomhedsform grundigt, da et forkert eller uhensigtsmæssigt valg kan give uønskede økonomiske og organisatoriske konsekvenser. Det kan være både dyrt og besværligt at ændre virksomhedsform, hvis ulemperne viser sig.

I forbindelse med valg af virksomhedsform bør man blandt andet overveje følgende forhold:

- Kapitalkrav
- Ledelse
- Hæftelse
- Revisionspligt
- Krav til offentliggørelse af årsrapport
- Skattemæssige forhold

For eksempel er det vigtigt at holde sig for øje, at såfremt der er tale om en lovpligtig indskudskapital, kan virksomhedens kreditorer alene rette krav mod denne kapital – det vil sige, at der er begrænset hæftelse. Er der derimod tale om personligt hæftende virksomheder, kan virksomhedens kreditorer i princippet gå efter virksomhedsdeltagernes private formuer.

De skattemæssige forhold bør ligeledes overvejes, idet visse virksomheder beskattes som et selvstændigt skatteobjekt (f.eks. aktieselskab, anpartsselskab og iværksætterselskab), hvorimod andre virksomheder beskattes hos indehaverne (enkeltmandsvirksomheder, interessentselskaber og kommanditselskaber).

Nogle virksomhedsformer er reguleret intensivt af dansk ret (selskaber), hvor andre ikke er, og disse må derfor selv aftale det fornødne imellem parterne samt over for virksomhedens handelspartnere.

Med hensyn til lederforhold er der for nogle virksomhedsformer præcist angivet, hvordan ledelsen skal sammensættes (selskaber), hvor der for eksempel ikke er nogen krav til sammensætningen af ledelsen i andre virksomheder (interessentskaber og enkeltmandsvirksomheder).

Foreningen Danske Revisorer har udarbejdet et skema, der giver et overblik over virksomhedsformerne og deres forskelligheder med hensyn til ejerforhold, etablering, Det Offentlige Ejerregister, kapitalkrav, ledelse, hæftelse, krav til revision, grad af offentliggørelse og skattemæssige forhold, som revisor kan bruge i forbindelse med rådgivning af sine kunder, når disse skal vælge virksomhedsform. Skemaet kan hentes af foreningens medlemmer på FDR's hjemmeside (www.fdr.dk) efter login.

Af Susanne Holm, Sekretariatsleder, Foreningen Danske Revisorer

Etablerings- og iværksætterkonto

Etablerings- og iværksætterkontoordningen har efterhånden en del år på bagen. Ordningen går ud på, at man med skattemæssig virkning kan "spare" op til etablering af selvstændig virksomhed. Det kan populært siges, at man får fremrykket det skattemæssige fradrag til før, man har etableret sig.

Af skatterådgiver John Rasmussen, Time Tax A/S.

Ved indførelsen af ordningen var der fradrag i den skattepligtige indkomst. Da begreberne personlig indkomst og kapitalindkomst kom til, ændredes fradraget for indskud på en etableringskonto til, at fradraget fik samme værdi som andre ligningsmæssige fradrag. Samtidig indførtes en graduering af hvor store beløb, de afskrivningsberettigede anskaffelsessummer skulle nedsættes, således at det blev forsøgt at få udlignet, at de tidligere fradrag kun var givet som ligningsmæssige fradrag, men at afskrivningerne på erhvervsaktiver kan fratrækkes i den personlige indkomst.

Etableringskontoreglerne er skruet sådan sammen, at jo lavere marginalskatten er, jo bedre kan det betale sig at foretage forlods afskrivninger med etableringskontomidler. Det er helt i tråd med Folketingets ønske om at tilgodese iværksætterkulturen i Danmark, således at skattevirkningen bliver størst i de første år, hvor indtjeningen sædvanligvis er lavest.

En ganske overset "finte" med etablerings- og iværksætterordningen er muligheden for at fremrykke fradrag for driftsudgifter og anskaffelse af driftsaktiver i etableringsåret og de følgende 4 indkomstår.

For mange iværksættere og nyetablerede omtales "finten" som en særlig skatteregel for iværksættere, der giver større skattefradrag.

Der er ikke tale om en særregel, men en i rådgiverkredse overset mulighed for at fremrykke skattemæssige fradrag for driftsudgifter og investeringer i driftsmidler i nystartede virksomheder.

For at forstå dette er det nødvendigt at kende det eksakte indhold i etableringskontolovens § 1:

§ 1. Den, der med henblik på etablering af selvstændig erhvervsvirksomhed eller erhvervelse af virksomhed i selskabsform ved anskaffelse af aktier eller anparter i et selskab foretager indskud på etableringskonto eller iværksætterkonto efter reglerne i denne lov, kan fradrage indskuddet ved opgørelsen af den skattepligtige indkomst.
Stk. 2. Fradrag for et givet indkomstår indrømmes for indskud, der er foretaget i tiden fra den 16. maj i indkomståret til og med den nærmest efterfølgende 15. maj (indskudsåret).
Stk. 3. **Efter etablering af selvstændig erhvervsvirksomhed eller erhvervelse af virksomhed i selskabsform ved anskaffelse af aktier eller anparter i et selskab har fundet sted, kan fradrag for indskud kun opnås for det indkomstår, hvor etablering eller erhvervelse finder sted, jf. § 5, og de nærmest efterfølgende 4 indkomstår. Fradrag kan ikke opnås for efterfølgende indkomstår, hvori indskudte beløb endnu ikke er hævet fuldt ud.**

Det betyder, at det er muligt at anvende etablerings- og iværksætterkontoreglerne i opstartsåret og de følgende 4 indkomstår, under forudsætning af at alle gamle indskud er anvendt.

Man skal særlig være opmærksom på, at fremrykningen af fradraget kan omfatte både driftsudgifter omfattet af de normale regler for fradrag for driftsomkostninger og investeringer i nye driftsmidler.

Indskuddet/fradragets størrelse

Det årlige fradrag for henlæggelser til etableringskonto og iværksætterkonto kan maksimalt udgøre 60 % af lønindtægten i hvert år før etablering af virksomhed. I de 4 følgende år kan fradraget maksimalt udgøre 60 % af lønindtægten og overskuddet af den selvstændige virksomhed. Dog kan fradraget altid udgøre 250.000 kr.

Indskuddet/fradraget skal altid være mindst 5.000 kr.

Man kan selv vælge, om indskuddet skal ske på etableringskonto eller iværksætterkonto.

Forskel mellem etableringskonto og iværksætterkonto

Indskud på etableringskonto med eller uden indskud kan fratrækkes som ligningsmæssigt fradrag med en skattemæssig virkning på ca. 30 %.
Indskud på iværksætterkonto med eller uden indskud kan fratrækkes i den personlige indkomst med en skattemæssig virkning på op til ca. 56 %.
Når beløbene hæves af indskud, eller der anvendes henlæggelser uden indskud, er der en forskel på, hvordan indskuddene skal gå fra i de omkostninger og/eller anskaffelser den skattepligtige har afholdt.

Når der anvendes etableringskontomidler skal udgifter og anskaffelser reduceres med 55 %, således at der kan fratrækkes 45 % af udgifter i virksomhedsindkomsten, ligesom anskaffelsessummer for driftsmidler m.v. reduceres med 55 %. Der kan således foretages skattemæssig afskrivning på 45 %.

Ved iværksætterkonto sker der 100 %

→

reduktion i omkostninger og anskaffelsessummer, idet indskuddet/henlæggelsen fratrækkes i den personlige indkomst.

I praksis anvendes reglerne således

Etableringskonto

En virksomhed er startet i 2014 med eller uden brug af etablerings- eller iværksætterkontomidler. I 2015 frem til fristen for at foretage indskud er der afholdt driftsudgifter for eksempelvis 50.000 kr. Disse udgifter ville efter de normale regler først kunne fratrækkes i 2015. Ved at anvende etableringskonto uden indskud kan man i stedet foretage fradrag på selvangivelsen for 2014 med 50.000 kr. uden indskud og derved fremrykke skattefradraget til 2014. Det skaber en bedre likviditet for den nystartede virksomhed. Man kan som nævnt bruge reglen i etableringsåret og de følgende 4 indkomstår.
Når man fremrykker fradraget, skal der i 2015 ske en regulering af de fradragsberettigede udgifter, idet driftsudgifterne/anskaffelsessummen på driftsmidler skal reduceres, idet der allerede er taget fradrag for udgiften i 2014.

Et eksempel: Virksomhed er etableret i 2014.
I perioden 1. januar 2015 til 15. maj 2015 er der afholdt skattemæssigt fradragsberettiget driftsudgifter med ..... 100.000 kr.
I selvangivelsen for 2014 fratrækkes indskud på etableringskontouden indskud med (ligningsmæssigt fradrag) ..... 100.000 kr.
Skattepåvirkning:
I 2014 opnås en skattebesparelse på ca. 30 % eller ..... 30.000 kr.
Selvangivelsen af driftsudgifterne for 2015 ser således ud:
Afholdte driftsudgifter ..... 100.000 kr.
Ej fradragsberettiget 55 %..... - 55.000 kr.
Fradragsberettiget i 2015 ..... 45.000 kr.
Hvis det lægges til grund, at virksomheden giver et overskud på 300.000 kr. i 2015, vil den samlede skattevirkning være:

Med anvendelse af etableringskonto:
Skattebesparelse i 2014 ved en skatteværdi på 30 %.. 30.000 kr.
Skattebesparelse i 2015 fradrag i personlig indkomst ved 40 % ..... 18.000 kr.
Samlet besparelse i skat..... 48.000 kr.

Uden anvendelse af etableringskonto:
40 % skatteværdi af den fulde udgift på 100.000 kr.. 40.000 kr.
Skattebesparelse ved at anvende etableringskontoreglen ..... 8.000 kr.

Det giver umiddelbart kun mening at anvende reglerne, hvis virksomhedens resultat er mindre end topskattegrænsen, hvilket kan ses af nedenstående eksempel. I hvert enkelt tilfælde vil jeg dog anbefale, at revisor foretager en beregning på, om det ene eller andet kan betale sig for kunden. Jeg anvender samme beløb som ovenfor, men virksomhedens resultat er 600.000 kr. i 2015.

Med anvendelse af etableringskonto:
Skattebesparelse i 2014 ved en skatteværdi på 30 %..... 30.000 kr.
Skattebesparelse i 2015 fradrag i personlig indkomst ved 56 % ..... 25.200 kr.
Samlet besparelse i skat..... 55.200 kr.

Uden anvendelse af etableringskonto:
56 % skatteværdi af den fulde udgift på 100.000 kr..... 56.000 kr.
Merskat ved at anvende etableringskontoreglen ..... 800 kr.

Iværksætterkonto

Hvis samme taleksempler anvendes på Iværksætterkonto, er resultatet:
I selvangivelsen for 2014 fratrækkes indskud på Iværksætterkonto uden indskud med (Fradrag i personlig indkomst)..... 100.000 kr.

Skattepåvirkning:
I 2014 opnås en skattebesparelse på ca. 40 % eller..... 40.000 kr.
Selvangivelsen af driftsudgifterne for 2015 ser således ud:
Afholdte driftsudgifter ..... 100.000 kr.
Ej fradragsberettiget 100 %.....-100.000 kr.
Fradragsberettiget i 2015 .....0 kr.
Hvis det lægges til grund, at virksomheden giver et overskud på 300.000 kr. i 2015, vil den samlede skattevirkning være:

Med anvendelse af iværksætterkonto:
Skattebesparelse i 2014 ved en skatteværdi på 40 %..... 40.000 kr.
Skattebesparelse i 2015 fradrag i personlig indkomst ved 40 % ..... 40.000 kr.
Samlet besparelse i skat.....0 kr.

Uden anvendelse af iværksætterkonto:
56 % skatteværdi af den fulde udgift på 100.000 kr..... 56.000 kr.
Merskat ved at anvende iværksætterkontoordningen..... -16.000 kr.

Det kan derfor ikke betale sig at benytte iværksætterordningen, hvis indkomsten i fradragsåret er under topskattegrænsen, idet skatteværdien af udgifterne i afholdelsesåret (2015) derved får en lavere skatteværdi end skatteværdien i fradragsåret (2014).

Det er min opfattelse, at ovenstående mulighed er en noget overset mulighed, og som i visse tilfælde kan give en konkret skattebesparelse for den nye virksomhed.

Risiko og væsentlighed ved revision af små virksomheder

Risiko og væsentlighed er og vil altid være nøglebegreber ved udførelse af revision, men hvad siger standarder og teorien egentlig om brugen af disse begreber ved revision af små virksomheder?

Af Rikke Holmslykke Kristensen, Studielektor, Institut for Entreprenørskab og Relationsledelse, Syddansk Universitet

Risiko og væsentlighed er nøglebegreber i en revision, som bestemmer art, omfang og tidsmæssig placering af revisionshandlinger, herunder hvilken bevistype, der er behov for, og hvilken styrke beviset skal have.

Som udgangspunkt gælder de samme regler omkring risiko og væsentlighed ved revision af alle virksomhedstyper, da de internationale revisionsstandarder (ISA'erne) ikke skelner mellem forskellige størrelser af virksomheden, men tværtimod konstaterer, at en revision altid er en revision – uafhængigt af størrelsen på virksomheden der revideres. Dog er der få steder konkret vejledning til revision af mindre virksomheder. I denne artikel vil jeg fremhæve denne vejledning samt give mit bud på, hvordan reglerne omkring risiko og væsentlighed kan anvendes i en revision af en lille virksomhed.

Sammenhæng mellem risiko og væsentlighed

Som udgangspunkt vurderes risiko og væsentlighed hver for sig. Men for at kunne skrive under på revisionspåtegningen skal revisor jf. ISA 300.3 *"opnå tilstrækkeligt og egnet revisionsbevis vedrørende de vurderede risici for væsentlig fejlinformation ved at udforme og gennemføre reaktioner på disse risici"*.
Revisor er således nødt til først at vurdere, hvornår der er tale om væsentlig fejlinformation, inden det er muligt at vurdere, hvor risiciene for denne fejlinformation er i regnskabet. Man kan således sige, at væsentlighed er det styrende begreb, da transaktioner, poster og oplysninger, der er uvæsentlige, sorteres fra allerede via den indledende regnskabsanalyse og opnåelse af forståelse af klienten. Det er dog vigtigt at være opmærksom på, at få foretaget en vurdering af, om en tilsyneladende uvæsentlig post alligevel er væsentlig. Eksempelvis hvis andre tilgodehavender, anden gæld eller periodeafgrænsningsposter består af modregnede poster, der, hvis de var bogført på de rigtige konti, kunne være væsentlige.

Væsentlighed

Væsentlighed er i ISA 320.4 defineret som: *"Information er væsentlig, hvis udeladelse eller forkert angivelse heraf kan påvirke de økonomiske beslutninger, som regnskabsbrugeren tager baseret på regnskabet"*.

Væsentlighed afhænger således både af postens eller fejlens beløbsmæssige størrelse, men også af de konkrete forhold ved dens udeladelse eller forkerte angivelse. Vurdering af væsentlighed er således ikke sort/hvid, men derimod et spørgsmål om revisors faglige vurdering og professionelle dømmekraft.

Først fastlægges væsentlighedsniveauet for regnskabet som helhed. Dette kan gøres ved at vælge et relevant benchmark og tage en passende procentdel heraf. Følgende kan bruges (dataene i tabellen er hentet fra Eilifsen & Messier 2015 og dækker over de benchmark og procentsatser, som de otte største revisionsfirmaer i USA anvender):

Benchmark	Procentsats
Resultat før skat	5-10 %
Aktivsum	½-2 %
Nettoomsætning	½-2 %
Egenkapital	1-3 %

Benchmark identificeres med baggrund i elementerne i det regnskab, som skal revideres, og på baggrund af en faglig vurdering af, hvilke elementer i regnskabet brugerne af det pågældende regnskab fokuserer på. For eksempel vil aktionærer typisk fokusere på resultat før skat, mens banken typisk vil fokuse-

Væsentlighedsniveauet bruges i forbindelse med:

Planlægning	Her fastlægges beløbet og poster med risiko for væsentlig fejlinformation identificeres.
Udførelse	Har indflydelse på art, omfang og tidsmæssig placering af revisionshandlinger, herunder størrelsen af stikprøver.
Vurdering/ evaluering af resultater	Giver de fundne fejl anledning til ændringer i den øvrige revision? Er de fundne fejl over eller under væsentlighedsniveauet?
Rapportering	Kan der afgives en blank påtegning? Fundne fejl rapporteres til øverste ledelse i revisionsprotokollen.

re på soliditeten og dermed egenkapitalen. Da små virksomheder som regel ikke udarbejder perioderegnskaber, vil væsentligheden skulle beregnes med udgangspunkt i sidste års regnskabstal eller dette års regnskabstal, såfremt disse foreligger. ISA 320 bemærker desuden vedrørende mindre ejerledede virksomheder, at såfremt resultat før skat konsekvent er lavt, fordi ejeren får størstedelen af overskuddet udbetalt som vederlag, kan det være relevant at bruge et benchmark som resultat før vederlag og skat.

Fastsættelsen af den procentsats, der anvendes på det valgte benchmark, afhænger naturligvis også af revisors faglige vurdering. Det kan dog generelt siges, at hvorvidt procentsatsen skal ligge i den lave eller høje ende af intervallet ovenfor, afhænger af ejerstruktur, finansieringsform og antallet af brugere. Små virksomheder har typisk få eller kun en ejer, hvilket taler for en procentsats i den høje ende af intervallet. Såfremt der er tale om en virksomhed, som udelukkende er finansieret ved egenkapital, taler dette for en procentsats i den lave ende af intervallet i modsætning til en virksomhed, der er finansieret ved hjælp af fremmedkapital, som taler for en procentsat i den høje ende. En virksomhed, hvor regnskabet har mange brugere, taler for en procentsats i den lave ende af intervallet, men en mindre virksomhed vil typisk have få brugere af regnskabet, hvilket taler for en procentsats i den høje ende af intervallet. Man kan således se, at det også er brugerne af regnskabet, der påvirker hvilken procentsats, der fastsættes.

Når væsentlighedsniveauet for regnskabet som helhed er fastsat, kan væsentlighed ved udførelsen fastsættes. Væsentlighed ved udførelsen udgør typisk 50-75 % af væsentlighedsniveauet for regnskabet som helhed og fastsættes til et lavere beløb end væsentlighedsniveauet for regnskabet som helhed for at reducere sandsynligheden for, at den samlede mængde ikke-korrigerede og uopdagede fejlinformationer overstiger det samlede væsentlighedsbeløb.

Både væsentlighedsniveauet for regnskabet som helhed og væsentlighed ved udførelsen skal dokumenteres, og det samme skal også de faktorer, som blev overvejet ved fastlæggelsen af disse beløb. Det er således vigtigt, at der ved fastlæggelse af relevant benchmark noteres, hvorfor dette er valgt (typisk med reference til de relevante brugere af regnskabet), og hvorfor der er valgt en procentsats i den lave eller høje ende af intervallet (typisk med reference til ejerstruktur, finansieringsform og antallet af brugere). Der er naturligvis også mulighed for at samveje forskellige benchmarks, man skal blot huske at argumentere for, hvorfor dette bliver gjort.

Risiko

ISA'erne er bygget op omkring et fokus på risiko. Når revisor har fastlagt væsentlighedsniveauet, skal revisor således identificere og vurdere risiciene for væsentlig fejlinformation. Dette gør revisor gennem en forståelse af den virksomhed, som skal revideres, og denne virksomheds omgivelser. Denne forståelse opnås ved at udføre risikovurderingshandlinger, som skaber grund for udformning og udførelse af yderligere revisionshandlinger. Risiciene for væsentlig fejlinformation skal vurderes både på overordnet regnskabsniveau (vedrører hele regnskabet og påvirker mange revisionsmål) og på revisionsmålsniveau på de enkelte regnskabsposter, transaktioner og oplysninger.

Revisors risikovurderingshandlinger består af forespørgsler til ledelsen og andre relevante medarbejdere, analytiske handlinger samt observation og undersøgelse. Da ISA'erne stiller krav om disse handlinger, er det vigtigt, at udførelsen af disse handlinger fremgår af revisionsdokumentationen. Vær dog opmærksom på at risikovurderingshandlinger alene ikke giver tilstrækkeligt og egnet revisionsbevis, men danner baggrund for udformning og udførelse af yderligere revisionshandlinger. Da små virksomheder, som tidligere nævnt, måske ikke udarbejder perioderegnskaber, som der kan udføres analytiske handlinger på, er det tilstrækkeligt at udføre disse, når første udkast til årsrapporten foreligger. Ud over overstående skal også øvrig viden om og erfaring med virksomheden inddrages. Dette kan eksempelvis være fra tidligere revisioner eller andre opgaver hos virksomheden.

Risikoen for væsentlig fejlinformation vurderes på basis af følgende seks dimensioner:

- Branche, lovgivning og andre eksterne faktorer
- Arten af virksomheden
- Valg og anvendelse af regnskabspraksis
- Mål og strategier samt tilknyttede forretningsrisici
- Måling og kontrol af den finansielle præstation
- Intern kontrolstruktur

I små virksomheder er ovenstående ofte ikke nedskrevet struktureret, men ISA'erne stiller fortsat krav om forståelse heraf. Da små virksomheder ofte er bygget op omkring ledelsen/ejeren, er det særligt vigtigt i disse virksomheder, at opnå en forståelse af ledelsens/ejerens holdninger, opmærksomhed og handlinger, da dette påvirker alle ovennævnte dimensioner og i særlig grad kontrolmiljøet. I små virksomheder er der typisk ikke tilstrækkeligt ansatte til, at der kan opnås en effektiv funktionsadskillelse til styrkelse af den interne kontrol. Til gengæld vil en ejerleder som regel føre et mere effektivt tilsyn med virksomheden, som delvist kan kompensere for den manglende funktionsadskillelse. Vær dog opmærksom på at en ejerleder nemt kan tilsidesætte kontroller, hvilket forøger besvigelsesrisikoen.

Hvis revisor i sin risikovurderingsproces identificerer risici på overordnet regnskabsniveau, fx besvigelsesmistanke, going concern usikkerhed eller manglende regnskabsmæssige færdigheder, kræver dette generelle reaktioner fra revisor. Disse generelle reaktioner vil typisk medføre, at revisor vil udføre flere substanshandlinger. Men ved en revision af en lille virksomhed vil revisionen i forvejen bestå af substanshandlinger, og de generelle reaktioner kan her eksempelvis være opmærksomhed på opretholdelse af professionel skepsis, at der sættes mere erfarne medarbejdere eller eksperter på sagen, at der føres mere tilsyn, at revisionen bliver mere uforudsigelig eller, at der indsamles mere sandsynliggørende (stærkere) revisionsbevis.

Hvis de identificerede risici ikke er på overordnet regnskabsniveau, men derimod på revisionsmålsniveau, fx risici vedrørende værdiansættelse af debitorer, tilstedeværelse af varelager eller fuldstændighed af omsætning, skal revisor udforme og udføre yderligere revisionshandlinger, hvis art, tidsmæssige placering og omfang er baseret på og behandler de vurderede risici for væ-

→

sentlig fejlinformation på revisionsmålsniveau. Husk herunder revision af kontroller, hvis risikovurderingen er baseret på, at der er velfungerende kontroller.

Desto højere risikoen er vurderet til at være, desto mere sandsynliggørende revisionsbevis skal der indsamles.

Det er vigtigt at notere, at for transaktioner, poster og oplysninger, der er væsentlige, skal revisor udforme og udføre substanshandlinger, uanset risikovurdering. Dette krav skyldes, at revisors vurdering af risiko er af skønsmæssig karakter, og revisor hermed kan overse risici. Desuden er der en iboende begrænsning i intern kontrol, da ledelsen altid vil have mulighed for tilsidesættelse heraf. Som tidligere nævnt vil en revision af en lille virksomhed i forvejen bestå af substanshandlinger, hvorfor dette krav ikke vil påvirke revisionen.

Efter identifikation af risici på overordnet regnskabsniveau og på revisionsmålsniveau, skal revisor vurdere, om nogle af de identificerede risici er betydelige risici. En betydelig risiko er en identificeret og vurderet risiko for væsentlig fejlinformation, som efter revisors vurdering kræver særlige revisionsmæssige overvejelser. Ved fastlæggelse af betydelige risici ses bort fra eventuelle identificerede kontroller, og revisor skal overveje følgende:

- om risikoen er en risiko for besvigelser
- om risikoen er knyttet til aktuelle betydelige økonomiske, regnskabsmæssige eller andre begivenheder og derfor kræver særlig opmærksomhed
- transaktionernes kompleksitet
- om risikoen vedrører betydelige transaktioner med nærtstående parter
- graden af subjektivitet ved målingen af finansiel information, der er knyttet til risikoen, især ved de målinger, der involverer et bredt interval for målingsusikkerhed, og
- om risikoen vedrører betydelige transaktioner, der ligger uden for virksomhedens normale forretningsområde, eller som på anden måde fremstår som usædvanlige

Såfremt der kan svares ja til et af ovenstående punkter, taler det for, at der er tale om en betydelig risiko. Den endelige beslutning afhænger af revisors professionelle vurdering. Transaktioner, poster og oplysninger, der er væsentlige, og hvor revisor har fastslået, at der er en betydelig risiko, skal revideres med substanshandlinger, der er specifikt rettet mod denne betydelige risiko. Revisor skal opnå forståelse af relevante kontroller, også selvom kontrollerne ikke bruges. Et eksempel på en væsentlig post med betydelige risici er nettoomsætning, som jf. ISA 240.26 som udgangspunkt indeholder en besvigelsesrisiko.

Både revisors risikovurderinger og reaktioner herpå skal dokumenteres. Vedrørende risikovurderinger skal dokumentationen indeholde de overvejelser, revisor har gjort sig om virksomhedens risici, nøgleelementer i forståelsen af de seks dimensioner af virksomheden og dens omgivelser, de identificerede og vurderede risici for væsentlig fejlinformation på overordnet regnskabsniveau og på revisionsmålsniveau samt de identificerede betydelige risici og hertil knyttede kontroller. Vedrørende generelle og konkrete reaktioner på vurderede risici for væsentlig fejlinformation skal revisor dokumentere de generelle reaktioner i relation til de vurderede risici for væsentlig fejlinformation på overordnet regnskabsniveau og arten, omfanget og den tidsmæssige placering af planlagte yderligere revisionshandlinger.

Herudover skal revisor som noget helt essentielt dokumentere sammenkædningen af de vurderede risici og resultaterne af de udførte revisionshandlinger samt sammenhængen mellem virksomhedens regnskab og bogføring. Hermed dokumenteres og sikres en rød tråd igennem hele revisionen. Som minimum bør revisor således sørge for delkonklusioner på hver enkelt regnskabspost, på eventuelle generelle risici på regnskabsniveau og på betydelige risici for væsentlig fejlinformation på specifikke revisionsmål.

Afslutning

Alt i alt kan det konkluderes, at både fastlæggelse af væsentlighedsniveau og identifikation af risici for væsentlig fejlinformation afhænger af revisors faglige vurdering, uanset størrelsen på den virksomhed som revideres.

Væsentlighed afhænger af revisors faglige vurdering og forventningerne til, hvornår en fejl i regnskabet vil påvirke de økonomiske beslutninger, som regnskabsbrugerne tager på baggrund af regnskabet. Væsentlighedsniveauet skal således fastsættes med baggrund i regnskabets konkrete brugere.

Vedrørende risikovurderingen kan det overordnet siges, at revisor skal identificere og vurdere risici for væsentlig fejlinformation på overordnet regnskabsniveau og på revisionsmålsniveau. Der skal udføres flest revisionshandlinger på væsentlige poster med betydelige risici, foretages en medium indsats på poster, som er væsentlige, men med "normale" risici og udføres færrest handlinger på væsentlige poster uden specifikke risici.

Igennem hele revisionen bør revisor have ISA 330.A63 in mente:
"Formen og omfanget af revisionsdokumentation er baseret på en faglig vurdering og påvirket af arten, størrelsen og kompleksiteten af virksomheden og dens interne kontrol, tilgængeligheden af information fra virksomheden samt anvendte fremgangsmåder og teknik ved revisionen."

Anvendt litteratur

- Primært ISA 315, 320 og 330. Sekundært ISA 240 og 300.
- Eilifsen, Aasmund & Messier, William F. (2015). Materiality Guidance of the Major Public Accounting Firms. Auditing: A Journal of Practice & Theory, 34(2), 3-26.

Momsfritaget undervisning eller ej?

Af Momskonsulent Majken Prip og Momsdirektør Søren Engers Pedersen, TimeTax A/S

Siden indførelsen i 1978 har momsfritagelsen for undervisning og særligt omfanget af den, været et af momslovens tilsyneladende mysterier. Der opstår ofte tvivl om, hvorvidt et konkret udbud af undervisning og kurser er fritaget, eller om der er tale om fuld momspligtig virksomhed.

Er det undervisning eller ej?

Selve fritagelsen for undervisning findes i momslovens § 13, stk. 1 nr. 3, og handler i sin helhed om momsfritagelse for skoleundervisning, undervisning på videregående institutioner, faglig uddannelse og anden undervisning, der har karakter af skolemæssig eller faglig undervisning, samt levering af varer og ydelser i nær tilknytning hertil.

Skolemæssig uddannelse og faglig undervisning

Fritagelsen nævner skolemæssig uddannelse, som omfatter undervisning på offentlige og private skoler og højere læreanstalter m.v. Undervisningstilbud og uddannelser, som hører under en relevant lovgivning, anses ligeledes for omfattet af fritagelsen, hvilket eksempelvis inkluderer aftenskoleundervisning, som er omfattet af folkeoplysningsloven. Dermed forudsætter fritagelsen, at undervisningen foregår på en skole m.fl. Dette kan give anledning til konkurrenceforvridning, jf. nedenfor.

Derudover fritages faglig uddannelse, omskoling, og tilsvarende undervisning, som har til hensigt at opkvalificere elevens faglige kompetencer. I den forbindelse tydeliggør dansk praksis på området, at det er afgørende for en fritagelse, at der er tale om opkvalificering af erhvervsmæssige kompetencer til brug for udvikling i elevens eksisterende hverv eller branche.

Sondringen mellem erhvervsmæssig og ikke erhvervsmæssig undervisning illustreres i praksis, hvor undervisning i forbindelse med et erhvervskørekort til lastbil og bus m.fl. kan omfattes af fritagelsen, da undervisningen har et erhvervsmæssigt sigte, hvorimod køreundervisning til kategori B – almindelig

personbil – ikke kan anses for overvejende at blive gennemført af erhvervsmæssig interesse, hvorfor undervisningen ikke kan omfattes af en fritagelse. Tilsvarende vurdering har man anlagt vedrørende førstehjælpskurser, som også er omfattet af momspligt. Her vurderer man ligeledes, at deltagerne gennemfører kurset i egen interesse, uden at det har relevans for deres jobfunktion (som hovedregel).

Udgangspunktet er dermed, at undervisningen skal være decideret kompetencegivende rent erhvervsmæssigt, for at den kan omfattes af en fritagelse. Det vil eksempelvis være tilfældet, når uddannelsen udbydes som en del af uddannelseslovgivningen, eller hvis uddannelsen er offentligt anerkendt eller branchegodkendt.

Holdundervisning

Fritagelsen for undervisning omfatter ligeledes legemsøvelser, når det har karakter af holdundervisning, herunder gymnastik og cirkeltræning.

I en række afgørelser har det daværende Momsnævn fastslået, at undervisning i gymnastik og tilsvarende beslægtede discipliner eksempelvis dans, afspænding, judo og yoga kan omfattes af fritagelsen for undervisning.

Der skal ved vurderingen af, om undervisningen er omfattet af fritagelsen lægges vægt på, om der er en instruktør eller en lærer gennem hele timen, om der er tale om egentlig holdundervisning således, at deltageren bliver ledt gennem hele programmet, og kan spørge om hjælp mv. undervejs.

Hvis undervisningen har karakter af kursusvirksomhed, som drives med gevinst for øje, og som primært er rettet mod virksomheder, vil den være momspligtig.

Kursusvirksomheder

Udover at fastslå omfanget af fritagelsen for undervisning, indeholder bestemmelsen også en undtagelse, som indebærer momspligt, selv om indholdet har karakter af faglig uddannelse.

Det fremgår således af bestemmelsen i momslovens § 13, stk. 1 nr. 3 2. pkt., at fritagelsen ikke omfatter kursusvirksomhed, som drives med gevinst for øje, og som primært er målrettet erhverv; virksomheder og institutioner m.v.

Selve undtagelsen til fritagelsen i Momsloven tilgodeser de kursusvirksomheder, hvis kunder kan fradrage momsen. Kursusvirksomheden kan pålægge moms på deres ydelser, og ligeledes få adgang til at fradrage købsmoms. Derudover vil en momspligtig kursusvirksomhed ikke skulle afregne lønsumsafgift.

Udfordringen

Men det er netop i forbindelse med undtagelsen, at udfordringerne omkring momsfritagelsen dukker op. Er en kursusvirksomhed fritaget for moms, eller er der i stedet tale om momspligtig virksomhed?

For at kunne foretage sondringen mellem de to rent momsmæssigt er det afgørende, at der først og fremmest tages stilling til, om selve undervisningen i sig selv kan anses for at være omfattet af fritagelsen.

Der skal foretages en konkret vurdering af, om den leverede undervisning kan karakteriseres som skolemæssig eller faglig uddannelse. Når det er tilfældet, at den udbudte undervisning og kurserne i sig selv kan anses for omfattet af fritagelsen, skal det dernæst vurderes, om der reelt er tale om kursusvirksomhed.

En kursusvirksomhed vil i denne henseende være en virksomhed, der leverer en samlet pakke, som inkluderer lokaler, forplejning og underviser m.v. Derudover er momspligten betinget af, at kurserne er målrettet erhverv. Praksis på området tydeliggør ligeledes, at det er afgørende, at undervisningen har et erhvervsmæssigt sigte, eksempelvis vil et kursus i akupunkturmetoder rettet mod praktiserende akupunktører, anses for at være rettet mod erhverv.

Kursusvirksomheder, som leverer kurser, der således retter sig mod erhvervsvirksomheder eller offentlige institutioner, og hvis undervisning ellers kan omfattes af en fritagelse, vil være momspligtige efter undtagelsen i Momslovens § 13, stk. 1 nr. 3. 2.pkt.

Rettes kurserne derimod til privatpersoner, vil de kunne leveres uden moms. Ligeledes gælder det, når kursusvirksomheden leverer ydelser til en fagforening, da fagforeninger i momsmæssig henseender hverken anses for erhvervsmæssig virksomhed eller en offentlig institution.

I de tilfælde hvor virksomhedens undervisning ikke kan anses for hverken skolemæssig eller faglig undervisning, vil de leverede kurser være omfattet af en momspligt, desuagtet om de er rettet mod private eller ej. Det kan eksempelvis gælde madlavningskurser og foredrag om fremtiden.

Afrunding

Ovenstående gennemgang tager udgangspunkt i de danske regler på området, hvor mystikken i fritagelsen for undervisning primært ligger i sondringen af den momsfritagne undervisning, og den undervisning der falder uden for kategori. Vurderingen af fritagelsen og dens omfang kan være kompliceret og omfattende, og det er dermed afgørende for kursusvirksomheder først og fremmest at have for øje, om deres undervisning er fritaget, før der tages stilling til, hvem kurset er rettet imod.

Derudover skal kursusvirksomheder, som afholder kurser udenfor Danmarks grænser, være opmærksom på, at der gælder et fælles regelsæt i EU for afholdelse af kurser og arrangementer. Reglerne fastslår, at momsbeskatningsstedet er der, hvor kurset rent faktisk afholdes. For en dansk kursusvirksomhed, som afholder kursus i Malmø, indebærer reglerne således, at virksomheden skal momsregistreres i Sverige og følge de svenske momsregler på området.

Afs: Foreningen Danske Revisorer · Munkehatten 32 · 5220 Odense SØ

POST B
PP DANMARK

Skift til DataLøn og få adgang til VIP hotline og rådgivning om personalejura

Bluegardens Lønpartnerkoncept er til dig, der administrerer løn for andre

Du håndterer dine kunders løn i DataLøn, som er Danmarks mest anvendte lønsystem. Hver måned håndterer 60.000 virksomheder løn til over ½ million lønmodtagere i DataLøn.

Kom godt i gang – og få løbende support

Vi hjælper dig med at oprette dine kunder og deres medarbejdere i DataLøn. Herefter ringer du bare til VIP Hotline, hvis du har brug for hjælp til deres lønadministration. Og har dine kunder spørgsmål om for eksempel barsels-regler, ferie eller fratrædelse – får du straks svar hos vores personalejurister eller i vores online PersonaleGuide.

Få et møde og to biografbilletter

Hør mere om DataLøn og vores Lønpartnerkoncept. Booker du et møde med os senest den 28. februar 2016, tager vi to biografbilletter med til mødet. Tilbuddet gælder virksomheder, der endnu ikke har en Lønpartneraftale.

Book online på Bluegarden.dk/fdr eller ring til os på 72 27 91 11

* Serviceabonnement koster fra 109 kr. om måneden alt efter samlet antal medarbejdere.

BLUEGARDEN