Bech·Bruun

Oktober 2018

NYT

Lancering af nyt Corporate Compliance nyhedsbrev

Denne gang handler nyhedsbrevet bl.a. om bøder efter databeskyttelsesloven, fravær af fængselsstraf for direktør i en kartelsag og en status vedrørende gældende sanktioner og eksportkontrol.

Nyhedsbrevet er relevant for dig, der har interesse inden for området Corporate Compliance, uanset om det er i privat eller offentligt regi. Emnerne vil være anti-korruption, bekæmpelse af hvidvask, eksportkontrol, sanktioner, erhvervsstrafferet og enterprise risk management. Nyhedsbrevet vil udkomme kvartalsvis.

Denne gang sætter vi bl.a. fokus på de første bødestraffe, der er på vej efter den nye databeskyttelseslov, vi ser nærmere på en dom, der afviser at fængsle en direktør i en kartelsag efter konkurrencelovgivningen, og på eksportkontrol og gældende sanktioner virksomheder og banker bør være opmærksomme på.

Databeskyttelse: Større bøder på vej

Databeskyttelsesloven er trådt i kraft, og Datatilsynet har taget hul på de første tilsynsbesøg hos danske virksomheder og myndigheder. Dermed vil de første bødesager formentlig dukke op i løbet af efteråret.

Loven åbner mulighed for, at idømme virksomheder bøder på op til 20 mio. euro (eller 4 procent af den globale omsætning i virksomheden, hvis det er højere). Offentlige myndigheder risikerer bøder på op til 2 procent af driftsbevillingen. Ledende medarbejdere kan risikere bøder (dog i en mindre størrelsesorden) og – i særlige tilfælde – frihedsstraf.

Rigsadvokaten har nu udsendt en meddelelse til landets anklagere om behandlingen af disse sager. Der er lagt op til et tæt samarbejde mellem Datatilsynet og politiet. I den første periode efter lovens ikrafttræden skal alle sager forelægges for de regionale statsadvokater – for at sikre ensartede strafpåstande i sagerne i hele landet.

Det fremgår ikke af meddelelsen, hvor store bøder anklagemyndigheden vil gå efter. Det må imidlertid forventes, at niveauet vil blive hævet betragteligt i forhold til de "normalbøder" på 25.000 kr., der var udgangspunktet efter de gamle regler.

Datatilsynet får stor indflydelse i forbindelse med beslutninger om tiltalerejsning, strafpåstand og eventuel anke af byretsdomme. Alt dette for at sikre, at dansk retshåndhævelse sker på rette vis og på EU-niveau.

Straffesager om overtrædelse af loven kan afgøres med et bødeforelæg udstedt af Datatilsynet. Denne mulighed vil imidlertid først blive udnyttet, når der er dannet en praksis på området. I den første tid vil alle sager om overtrædelse af loven derfor blive afgjort i byretten.

Arbejdsret: Ny bødepraksis for ulovligt arbejde

Der er sket en udvikling i praksis om bøder for ulovligt arbejde, og en lovændring er på vej.

Virksomheder, der er certificerede efter den såkaldte "fast track"-ordning, har mulighed for en mere smidig procedure ved ansættelse af medarbejdere, der ikke er EU-borgere. En bøde for overtrædelse af udlændingeloven på 20.000 kr. eller derover betyder imidlertid, at virksomheden som udgangspunkt mister sin certificering. Det kan i det praktiske liv have store konsekvenser for de arbejdsgivere, der beskæftiger udlændinge, fx i kortere projektforløb, og hvor en fejl i papirarbejdet kan koste dyrt.

Domstolene har ved flere lejligheder taget stilling til strafniveauet ved beskæftigelse af udlændinge uden arbejds- og opholdstilladelse. "Normalbøden" til arbejdsgivere i sager om ulovligt arbejde er 10.000 kr. pr. påbegyndt

måned af den ulovlige beskæftigelse. I kvalificerede tilfælde 20.000 kr., jf. udlændingelovens § 59, stk. 5 og 6. I to nyere afgørelser har domstolene imidlertid efter en konkret vurdering fastsat lavere bøder, end udgangspunktet angiver, til certificerede arbejdsgivere, der ikke har haft økonomisk vinding af at beskæftige de pågældende udlændinge (UfR 2017.2775 Ø og Københavns Byret, dom af 11. september 2017, bøder på hhv. 10.000 kr. og 15.000 kr.).

Dette har ført til, at anklagemyndigheden med virkning fra januar 2018 har ændret praksis, sådan at anklagerne fremover i højere grad skal vurdere bødepåstanden fra sag til sag, når der er tale om "administrative fejl". Desuden er der en lovændring på vej, der skal hjælpe arbejdsgivere, der uforvarende overtræder reglerne – samt en forhøjelse af bøderne for de arbejdsgivere, der bevidst spekulerer i at beskæftige udenlandsk arbejdskraft ulovligt, se Regeringens lovkatalog for 2019 s. 57, jf. www.stm.dk/publikationer/skriftlig-del18/Lovgivning%20-%20Folketingsåret%202018-2019.pdf.

Konkurrenceret: Direktør slap for fængsel

Ingen frihedsstraf til direktør i en virksomhed, der havde deltaget i et kartel.

Retten i Holbæk afsagde den 19. september 2018 dom i en sag, hvor anklagemyndigheden havde krævet fængselsstraf til direktøren i et selskab, der var involveret i (alvorlig) overtrædelse af konkurrenceloven. Resultatet af sagen blev en bøde på 100.000 kr.

Der var tale om en nu 76-årig tidligere ejer af en nedrivningsvirksomhed, som i forbindelse med en nedrivningsentreprise, der var sat i udbud, havde modtaget en konkurrents tilbud og derpå ladet sin virksomhed afgive tilbud. Anklagemyndigheden havde krævet den 76-årige idømt fængselsstraf, idet det bl.a. var gjort gældende, at der var tale om en kartelaftale af grov beskaffenhed. Retten fandt dog efter en samlet vurdering, at forholdet ikke var af grov beskaffenhed, bl.a. fordi der var tale om førstegangstilfælde uden (stor) økonomisk vinding (Rettens j.nr. 60-1112/2018).

Dermed er der fortsat ikke afsagt nogen domme i Danmark, hvor den øverste ledelse i en virksomhed er blevet idømt frihedsstraf i kartelsager eller andre "grove" konkurrencesager. Efter skærpelsen af straffene i 2012 er det almindeligt, at anklagemyndigheden rejser sag mod både virksomheden og den øverste ledelse, men straffen for det personlige ansvar er altså bøde, der typisk ligger i intervallet mellem 25.000 kr. og 100.000 kr.

Eksportkontrol: Status oktober 2018 vedr. sanktioner og eksportkontrol

Danmark (EU) har fortsat sanktioner, dvs. forbud mod bestemte transaktioner og forbud mod forretninger med nærmere bestemte enkeltpersoner, i forhold til de følgende lande/territorier:

- Iran (begrænsede sanktioner, de fleste blev ophævet i 2016)
- Krim og Sevastopol
- Nordkorea
- Rusland
- Syrien.

USA har desuden sanktioner mod følgende lande:

- Iran (nærmest total embargo)
- Cuba
- Sudan
- Venezuela.

Rusland har iværksat modsanktioner mod USA på udvalgte områder som følge af krisen på Krim/Øst-Ukraine.

Danske virksomheder kan lovligt handle med Iran m.m., når de følger europæiske regler og Europa-Kommissionens statut om spærring. USA har imidlertid i de seneste måneder strammet retorikken overfor selskaber, der handler med Iran, Cuba m.m. (fx præsident Trump på Twitter: "De kan handle med dem, eller de kan handle med os."). USA har med Trump i spidsen valgt at trække sig ud af atomaftalen med Iran og har genindført sanktioner mod Iran. Sanktionerne vil blive strammet yderligere i november måned. Danske og europæiske virksomheder står nu med en udfordring i navigeringen mellem hhv. det amerikanske politiske pres og den europæiske opbakning til et samarbejde med Iran.

Tilsvarende kan Rusland tænkes at følge op overfor firmaer, der handler med amerikanske virksomheder, der er omfattet af Ruslands modsanktioner (primært olie- og gasindustrien). Det anbefales at følge udviklingen i forhold til Iran og Rusland nøje, eventuelt via Dansk Industris hjemmeside www.danskindustri.dk.

En opdateret oversigt over de aktuelle sanktioner kan findes her um.dk/da/udenrigspolitik/folkeretten/sanktioner/gaeldende-sanktioner/.

Desuden gælder der (fortsat) regler om eksportkontrol, dvs. krav om eksportgodkendelse i forhold til visse produkter (bl.a. "dual use"-produkter) og godkendelse af forretningstransaktioner med bestemte lande, regioner, enkeltpersoner og selskaber (bl.a. for at forhindre terrorfinansiering).

Compliance: Trusselsniveauet for cybercrime er fortsat "meget højt"

Forsvarets Efterretningstjeneste har den 29. september 2018 indviet det nye Center for Cybersikkerhed, der kommer til at spille en central rolle i danske myndigheders og virksomheders sikkerhed. Truslen fra kriminelle, der benytter internettet til kriminelle formål og til spionage, er fortsat "meget høj", fastslår tjenesten.

Angrebene på danske myndigheder kommer primært fra fremmede stater og fra grupper, der nyder støtte fra disse staters myndigheder. Der er her navnlig tale om (forsøg på) spionage. Angreb på danske virksomheder kan også komme fra fremmede stater, men her er det navnlig statsstøttede hacker-grupper og "uafhængige" kriminelle, der udgør truslen.

Angrebene kan komme i flere former. Spionage udføres ofte som et såkaldt "Advanced Persistent Threat-angreb", der er en særligt avanceret, målrettet og vedholdende form for hackerangreb. Angreb af denne type kræver stor kapacitet og ekspertise. Der er set eksempler på angreb, der har stået på over flere år med det formål at skaffe oplysninger om forretningshemmeligheder.

"Spear-phishing" er forsøg på at skaffe information om en bruger eller adgang til et netværk ved at stjæle fx brugernavn og kodeord – eller ved at installere malware (ondsindede programmer) på brugerens computer. Angrebet kan ske via en e-mail eller gennem såkaldt social engineering, hvor brugeren på forskellig vis manipuleres eller narres til at give de ønskede oplysninger eller installere den skadelige software på sin computer.

Angrebene kan rettes mod computere – eller mod fx mobiltelefoner, hvor det er muligt fx at aktivere mikrofon og kamera, uden brugeren bliver opmærksom på det.

Angrebene bruges naturligvis også til at stjæle penge eller informationer. Der ses eksempler på pengeafpresning, hvor en virksomhed må betale store beløb for at genvinde kontrollen over deres it-netværk eller for at undgå, at deres data ødelægges.

"Hacktivisme" er udtryk for en aktivitet, hvor en virksomhed angribes af grupper af "utilfredse" aktivister. Disse angreb, der er motiveret af politiske eller ideologiske overbevisninger, kan have til formål at ødelægge eller lamme en virksomheds netværk. Formålet kan også være at overtage netværket for at sprede propaganda. Angrebene kan gennemføres af enkeltpersoner, der ikke behøver være specialister på feltet, da "kogebøger" til disse angreb kan findes på internettet.

Det er nødvendigt, at myndigheder og virksomheder til stadighed har fokus på it-sikkerhed og vedligeholder medarbejdernes opmærksomhed på området. Hjælp og vejledning kan nu bl.a. findes i det nye center for Cybersikkerhed.

Øget indsats mod hvidvask og terrorfinansiering

Regeringen vil fremsætte et lovforslag, der strammer sanktionerne for overtrædelse af hvidvasklovgivningen.

Forslaget er en udmøntning af den politiske aftale, som regeringen og samtlige politiske partier, bortset fra Enhedslisten, i september 2018 indgik på grundlag af den samlede nationale strategi til bekæmpelse af hvidvask og terrorfinansiering 2018-2921 om yderligere initiativer til styrkelse af indsatsen mod hvidvask og finansiering af terrorisme.

EU's 4. hvidvaskdirektiv blev gennemført i dansk ret i maj/juni 2017 med reglerne om det offentlige ejerregister og den nye hvidvasklov, der indebærer betydelige nye pligter for de omfattede virksomheder. Den politiske aftale og det bebudede lovforslag er udtryk for et politisk ønske om at styrke håndhævelsen af reglerne. Det sker gennem både yderligere stramninger af de pligter, som påhviler virksomhederne, og forhøjelse af sanktionsniveauet for overtrædelser.

Således kan det nævnes, at fit & proper-kravene til medlemmer af ledelsen i finansielle virksomheder skærpes, ligesom pengeinstitutter og udbydere af betalingstjenester pålægges at udarbejde en politik for sund virksomhedskultur. Der indføres en særlig fast track-ordning for særligt mistænkelige transaktioner, og såvel Finanstilsynet som Statsadvokaten for Særlig Økonomisk og International Kriminalitet forventes tilført yderligere ressourcer, ligesom Danmark vil deltage aktivt i det kommende internationale arbejde med at styrke samarbejdet om bekæmpelse af hvidvask på tværs af lande.

Hertil kommer, at bødeniveauet foreslås forhøjet med op til 700 pct. for de alvorligste overtrædelser. Dette vil gøre det danske strafniveau til et af de højeste i Europa.

Har du spørgsmål til nyhedsbrevet, er du velkommen til at kontakte en af vores specialister på området.
Du kan også rette henvendelse til din sædvanlige kontaktperson hos Bech-Bruun.

Thomas Munk Rasmussen
Partner
T +45 72 27 33 55
E tmr@bechbruun.com

Lars Lindencrone Petersen
Partner
T +45 72 27 35 35
E llp@bechbruun.com

David Moalem
Partner
T +45 72 27 33 42
E dmm@bechbruun.com

Poul Gade
Senioradvokat
T +45 72 27 34 23
E pga@bechbruun.com

Mikkel Chislett
Senioradvokat
T +45 72 27 34 45
E chis@bechbruun.com