

Deloitte.

20 gode råd
Stå stærkere når det
blæser op til storm

En compliancehåndbog



Compliance – en sag for ledelsen

Det er forretningskritisk for virksomheder at være compliant i forhold til lovgivning, brancheguidelines og omverdenens forventninger. En strategisk tilgang til compliance kan løfte dit brand betydeligt og styrke din forretning, hvorimod manglende compliance på kort tid kan få din virksomhed økonomisk og omdømmemæssigt i knæ.

Compliance er et ledelsesværktøj – og vi vil i denne håndbog give dig gode råd til, hvordan du kan systematisere og integrere dine complianceaktiviteter og samtidig være på forkant med markedets forventninger til din virksomhed.

Compliance trends

Inden for compliance er der især tre trends, virksomheder skal være opmærksomme på. Det øgede fokus på compliance betyder en tiltagende bevægelse fra Soft Law mod Hard Law. Dvs. der indføres flere love, samtidig med at interessenters forventninger til, hvordan man opfører sig i branchen og tager fx miljøhensyn og socialt ansvar, stiger.

Derudover er kompleksiteten i forhold til compliance stigende, fordi flere og flere virksomheder konsoliderer, samtidig med, at der er store forskelle på, hvordan compliance håndhæves globalt. Danske virksomheder med produktion og salg i udlandet har ofte sværere ved at opnå samme fordelagtige vilkår som de lokale virksomheder, de konkurrerer mod.

Sådan bliver du compliant

Det kræver tid, kompetencer og strukturerede processer at blive compliant. Derfor har vi udviklet et koncept - Compliance360 - som sikrer, at I:

1. Følger de Hard Laws og Soft Laws, der gælder for jeres virksomhed.
2. Udnytter compliance som en løftestang til at styrke interessenters forventninger til jeres brand.
3. Skaber en systematisk struktur for, hvordan I håndterer og vurderer risici, processer, kontroller og rapportering på tværs af hele organisationen.
4. Forankrer ansvaret for compliance ét sted og udnævner en complianceansvarlig, som indgår i ledelsen.
5. Får kompetent rådgivning og sparring, adgang til et globalt vidensnetværk og erfaringer fra alle brancher og industrier.



COMPLIANCE OMFATTER

- Hard Laws: Nationale og internationale love, regler og standarder, som udløser bøder og sanktioner ved overtrædelse.
- Soft Laws: Branchespecifikke guidelines, som ikke nødvendigvis udløser bøder eller sanktioner ved overtrædelse.
- Forventninger fra interessenter: Ethiske normer og social ansvarlighed, som virksomheder selv kan regulere og udnytte strategisk til at styrke virksomhedens omdømme.

Fire komplekse områder inden for compliance

Arbejdstagerrettigheder, risikostyring, beskyttelse af persondata og antikorruption er de mest omfattende områder inden for compliance. Herunder får du en indføring i, hvad din virksomhed skal være særligt opmærksom på, og hvordan I navigerer uden om risiciene.

1. Arbejdstagerrettigheder: Et komplekst, dansk arbejdsmarked udfordrer byggebranchen

I Danmark er arbejdstagerrettighederne temmelig komplekse sammenlignet med andre lande. Det er derfor svært for udenlandske virksomheder, som opererer i Danmark enten direkte eller som underleverandør, at skabe overblik over de love, der vedrører deres medarbejders arbejdsforhold og lønvilkår.

Resultatet er, at der sker mange fejl omkring løn, pension, tidsregistrering, arbejdssikkerhed og administration blandt udenlandske virksomheder i Danmark – og ofte falder en sag om overtrådte arbejdstagerrettigheder ned i kategorien social dumping.

Især i byggebranchen, som anvender udenlandsk arbejdskraft, er social dumping en velkendt trussel. Som hovedleverandør til fx et stort anlægsbyggeri i Danmark har man ansvar for, at den samlede produktion sker i overensstemmelse med gældende lovgivning. Derfor rammer det bundlinjen, når underleverandørerne ikke lever op til arbejdstagerrettighederne.

Leverandørstyring er en samlet betegnelse for, hvordan I skaber gennemsigtighed, klare processer og kontroller i forhold til at styre krav og forventninger til underleverandører, så arbejdstagerrettighederne overholdes igennem hele projektløbet og af alle involverede parter.

FEM GODE RÅD OM LEVERANDØRSTYRING

1. Vær på forkant med, hvilke krav dine underleverandører skal leve op til. Gør det klart i udbudsmaterialet, at I vil gennemføre kontroller og hvilke sanktionsmuligheder gælder, hvis man som leverandør ikke lever op til jeres krav. Undlader I at skrive dette, har I reelt ikke nogen sanktionsmulighed.
 2. Fjern kompleksiteten og gør arbejdsmarkedsregler og overenskomster forståelige og konkrete for dine leverandører. Oversæt dem evt. til leverandørernes modersprog for at mindske risikoen for misforståelser.
 3. Involver vigtige interessenter, fx leverandører og fagforeningsrepræsentanter, på et opstartsmøde, hvor de kontraktuelle forventninger adresseres, og I sikrer, at underleverandører forstår indholdet.
 4. Foretag løbende målrettede og effektive kontroller af underleverandørerne, så I er på forkant.
 5. Hav beredskabet på plads i tilfælde af, at en sag begynder at rulle enten i medierne eller internt i organisationen. Gør jer klart, hvordan I vil undersøge sagen, hvad I vil kommunikere og vær konsekvente i forhold til, hvordan I håndterer non-compliance i forbindelse med arbejdstagerrettigheder.
-

2. Persondata: Ny EU-Forordning skærper kravene til beskyttelse af persondata

Den digitale transformation i virksomheder ændrer bl.a. den måde, vi indsamler, arbejder med og arkiverer data. Nye teknologier giver os helt nye forretningsmuligheder, men øger også risikoen for, at data kommer i de forkerte hænder. Hackere anvender stadig mere avancerede metoder, og it-sikkerheden skal derfor løbende skærpes.

Mange virksomheder famler i blinde i forhold til, hvordan de skal håndtere og sikre persondata. EU's eksisterende databeskyttelsesdirektiv fra 1995 er for længst blevet overhalet af nye teknologier, som bl.a. sociale medier og cloud computing, der binder data sammen på kryds og tværs.

Derfor forventes EU at indføre en forordning om beskyttelse af persondata, som træder i kraft i 2017 og vil medføre store stramninger og højere bøder fra dag ét.

I takt med at datamængderne stiger, bliver databeskyttelse – og især kritiske persondata – et stadig vigtigere område i jeres compliancestrategi. Det tager tid at planlægge og idriftsætte compliance inden for dette område, og I kan med fordel allerede nu skabe jer et overblik over, hvordan den ny EU-forordning påvirker jeres – og jeres leverandørers - forretning.

FEM GODE RÅD OM PERSONDATA

1. Find først ud af, hvor jeres persondata befinder sig henne? Hvordan opbevarer I dem, og hvordan flyder de gennem organisationen?
 2. Udarbejd en risikovurdering, hvor I definerer, hvad det er særligt vigtigt for jer at kunne styre, overvåge og kontrollere i forhold til persondata? Hvilke procedurer har I i forvejen for at sikre persondata, og hvilke nye procedurer skal etableres?
 3. Etabler en strategi og et program for, hvilke nye kontroller skal identificeres og implementeres.
 4. 'Privacy by design' er et centralt emne i den nye EU-Forordning. 'Privacy by design' betyder, at du skal tænke risikoen for sikkerhedsbrud ind i dine projekter fra start. Det er ikke noget, man kan implementere efterfølgende.
 5. Hav et beredskab klart, hvis der sker sikkerhedsbrud, og gør jer på forhånd klart, hvordan I anmelder sikkerhedsbrud og håndterer såvel praktik som kommunikation til omverden.
-

HVILKE KRAV SKÆRPES I NY EU-FORORDNING?

EU-Forordningen stiller især krav til dokumentation for, at data beskyttes, og at personer får egenkontrol med data. Forordningen indeholder punkter som:

- Personer får retten til at blive glemt, dvs. personer kan selv vælge at få slettet data
- Personer skal have nem adgang til egne data
- Personer skal nemt kunne flytte egne data fra en service provider til en anden
- Personer skal underrettes om databrud inden for 24 timer
- Der indføres ét sæt regler, som gælder for alle virksomheder i EU – og virksomheder uden for EU, som handler med EU-lande
- Økonomiske sanktioner skærpes betydeligt ved overtrædelse

Kilde: European Commission, Factsheet on data protection reform, 2012, "Why do we need an EU data protection reform?"

3. Antikorrupktion: Hold fokus på dine agenter i højrisikolande

Danske virksomheder, som etablerer sig i udlandet, konkurrerer ofte med lokale virksomheder på produkter og priser. I højrisikolande som Brasilien, Rusland, Indien og Kina (BRIC) har myndighederne en mere lempelig håndhævelse af bestikkelse og korrupktion, end vi kender det fra Danmark, og danske virksomheder oplever derfor, at de lokale konkurrenter hurtigere opnår fx byggetilladelser eller godkendelse af nye produkter.

Nogle virksomheder vælger derfor at gøre brug af en lokal agent, som kender markedet og det offentlige system. Men det kan være vanskeligt at styre agentens arbejdsmetoder, og alt hvad agenten foretager sig, har virksomheden ansvaret for.

Bestikkelse og korrupktion straffes særdeles hårdt, og efter indførelsen af UK Bribery Act i 2011 er den økonomiske straf skærpet kraftigt for alle virksomheder, der driver forretning både i og uden for Storbritannien. Hvis man – bevidst eller ubevidst – begår bestikkelse i et andet land end Storbritannien, kan man altså retsforfølges i Storbritannien. En del danske virksomheder er omfattet af UK Bribery Act.

For at komme korrupktion og bestikkelse i forkøbet er det vigtigt, at virksomhedens ledelse er ekstra tydelig omkring virksomhedens værdier - også kaldet tone at the top. Hele organisationen på tværs af lande og agenter må ikke være i tvivl om, hvilke værdier skaber det forretningsmæssige fundament for jeres virksomhed.

FEM GODE RÅD OM ANTIKORRUPTION

1. Virksomheder skal starte med at gennemføre en risikovurdering. Afhængigt af virksomhedens kompleksitet kan man opsætte et antal forskellige korrupktionsscenerier. I hvilke lande er risikoen størst?
 2. Dernæst skal I undersøge, om I imødekommer principperne i UK Bribery Act – eller anden gældende lovgivning
 3. I skal udarbejde processer for hver enkelt område, hvor bestikkelse kan komme på tale i de lande, I har udvalgt (fx gavebeløb – hvordan sikrer vi, at gavebeløb overholdes og posteres korrekt gennem hele organisationen?)
 4. I skal etablere procedurer for kontrol og rapportering til ledelsen i Danmark
 5. I skal lægge en klar strategi for, hvordan I kommunikerer med medarbejdere og omverden, hvis noget går galt. Der skal etableres et beredskab, så I hurtigst muligt kan rette op på situationen
-

SÅDAN FOREBYGGER DIN VIRKSOMHED OVERTRÆDELSE AF UK BRIBERY ACT:

Til trods for en overtrædelse af UK Bribery Act vil en virksomhed kunne frifindes, hvis der er tilstrækkelige procedurer sat op med det formål at forhindre bestikkelse i at finde sted. Det kræver at følgende principper kan dokumenteres:

1. Den øverste ledelse har ansvar for at etablere en antikorrupktionkultur – "tone at the top"
2. Virksomhedens korrupktionrisici skal regelmæssigt vurderes
3. Politikker og procedurer til at forhindre korrupktion skal være klare, anvendelige og tilgængelige
4. Politikker og procedurer skal implementeres effektivt
5. Der skal udvises rettidig omhu af alle forretningspartnere
6. Virksomheden skal løbende overvåge, gennemse og opdatere antikorrupktionssystemer

Kilde: Dansk Industri

4 Risikostyring: Ingen forretningsstrategi uden risikostyring

Uanset hvor stor eller lille virksomhed, I driver, er risikostyring noget, I skal forholde jer til på linje med forretningsstrategien. Hvordan vil I gerne tjene penge – og hvad kan forhindre jer i det?

Ledelsen bør danne sig et overblik over eksterne og interne faktorer, som vil kunne påvirke virksomhedens fremtidige indtjening. Risiciene er særligt store inden for:

Supply Chain, fordi virksomheder er meget afhængige af leverandørers tidsfrister, kvalitet og pris

Cybersikkerhed, fordi mængden af cybertrusler stiger i takt med at it-infrastrukturen bliver mere kompleks

Øget konkurrence fra virksomheder, der med nye 'disruptive' teknologier og nye digitale forretningsmodeller vinder kunder fra traditionelle leverandører

Udfordringen for mange danske virksomheder er, at de ikke får undersøgt, hvordan potentielle risici kan true forretningen. De gør en stor indsats for at identificere, hvilke risici de er særligt udsatte for, men får ikke operationaliseret deres risikostyring. For store koncerner er det især en udfordring, at risikostyring ikke koordineres på tværs af siloer.

I skal skabe en struktureret proces for, hvordan I undersøger og identificerer risici. Det er vigtigt, at risikostyring bliver operationaliseret i organisationen ved fx at koble KPI'er på de identificerede risici. Risikostyring skal indgå i den daglige drift i både moderselskab og eventuelle datterselskaber.

FEM GODE RÅD OM RISIKOSTYRING

1. Risikostyring skal først og fremmest forankres i virksomheden. Hvem har det overordnede ansvar for, at I styrer jeres risici, så I kan følge jeres forretningsstrategi?
 2. Dernæst skal I skabe rammerne for, hvordan I vil arbejde med risikostyring. Hvem gør hvad? Hvilke risici vil I gå i dybden med? Hvordan vil I måle på risiciene? Hvornår vil I gøre det? Og hvilke processer skal sikre, at I kommer i mål?
 3. I skal nu fastlægge et realistisk ambitionsniveau i forhold til de risici, I vil arbejde med. Hvor lang tid har vi? Hvordan prioriterer vi tiden?
 4. For hvert risikoområde skal I udarbejde konkrete handlingsplaner. I skal gå helt i dybden – det er bedre end at dække bredt. De største risici skal I forsøge at eliminere helt.
 5. Endelig skal I sørge for at få involveret de rette interessenter i processerne og på et tilstrækkeligt højt niveau. Hav et beredskab klart, hvis noget alligevel går galt, så I på forhånd har afklaret, hvem gør hvad.
-

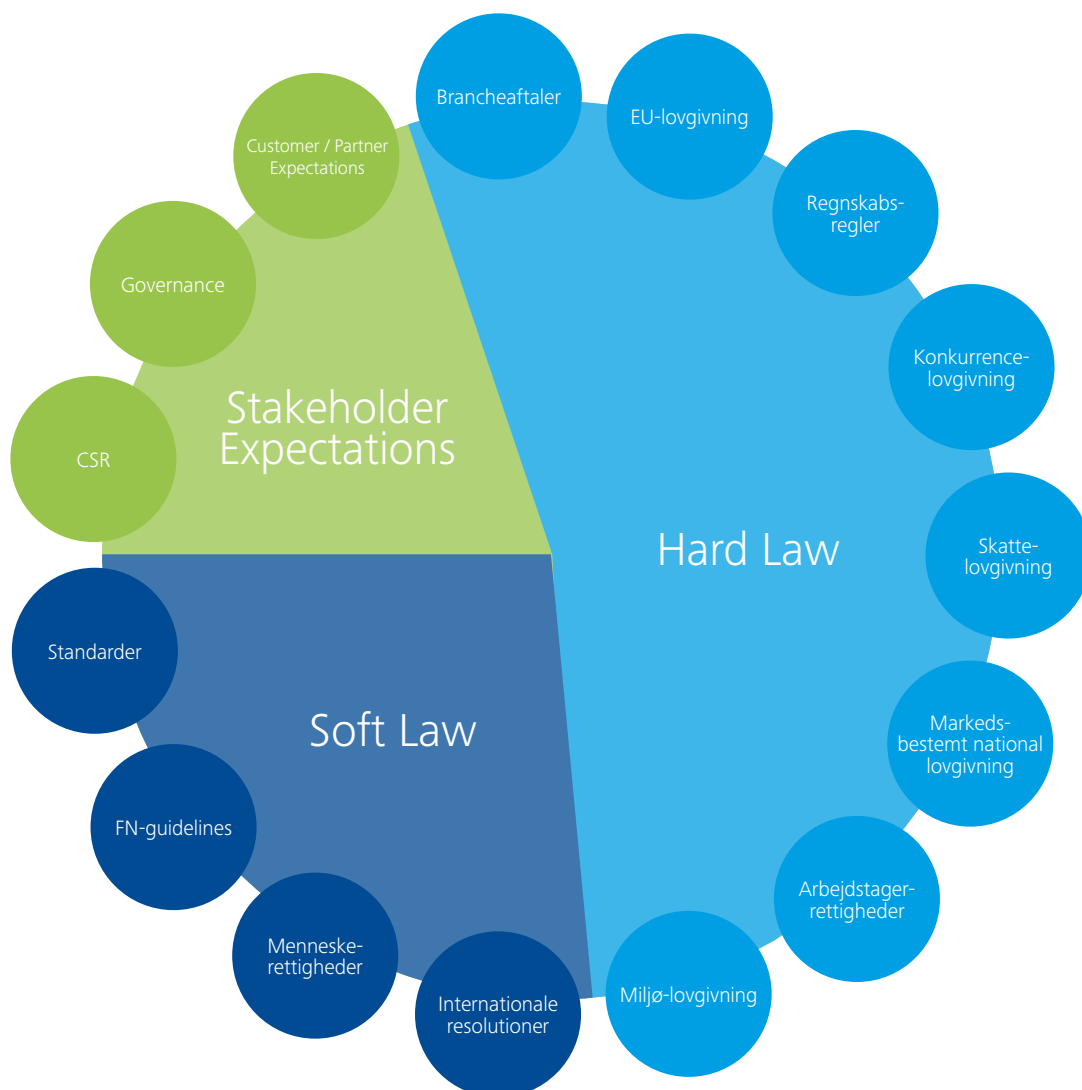
VIDSTE DU, AT ...

- At halvdelen af nordiske virksomheder ikke har en selvstændig Chief Compliance Officer?
- At 74% af nordiske Chief Compliance Officers ikke er en del af direktionen?
- At op mod 50% af nordiske virksomheders complianceansvarlige ikke kender eller har eget budget?

Kilde: Deloitte "The Nordic Compliance Survey – Risk Assessment", juni 2014

Hvad er Compliance360?

Compliance360 er et best-practice-værktøj udviklet af Deloitte, som sikrer din virksomhed en strategisk og struktureret tilgang til compliance.



Den systematiske tilgang i Compliance360 afdækker risici, etablerer processer og procedurer for kontrol og rapportering 360 grader rundt i virksomheden. Ansvaret for compliance forankres, og alle compliance-tiltag integreres, så virksomhedsledelsen får lettere ved at vurdere, hvordan det samlede risikobillede ser ud, hvor de svage led er, og hvad der skal til for at skabe et stærkere fundament.

Compliance360 er et gennemtestet værktøj og hjælper din virksomhed med at imødegå risikoen for negativ

påvirkning af virksomhedens økonomi, drift eller omdømme. Compliance360 sikrer fuldt overblik over hele processen og minimerer risikoen for pludselige overraskelser, hvis procedurer, systemer eller mennesker svigter.

Deloitte Compliance dækker hele paletten af Hard Law, Soft Law og forventninger fra interessenter. Vi har spidskompetencer inden for alle de områder, som er omfattet af compliance, og vi har et stærkt netværk globalt, som kan hjælpe dig, uanset hvor i verden din virksomhed opererer.

Compliance360 i seks trin

Compliance360 følger seks trin, hvor vi kommer hele vejen rundt om alle de faktorer, der bidrager til, at jeres virksomhed bliver compliant og kan anvende compliance som et ledelsesværktøj og dermed opnå konkurrencemæssige fordele.

Maturity Assessment: Hvor moden er jeres virksomhed?

Vi gennemgår virksomhedens interne politikker og procedurer, samt kortlægger de love, regler, standarder og etiske forventninger, som virksomheden forventes at følge. Vi giver ledelsen og dens interessenter et samlet overblik over, hvor compliant virksomheden er, og hvor der er plads til forbedringer.

Prevent: Hvor sikker er jeres virksomhed?

Politikker, procedurer og forventninger gennemgås for relevante forretningsenheder og afdelinger. Er politikkerne klart beskrevne, og er der konsekvent opfølgning på kritiske felter? Bliver relevante interessenter inddraget, og forventninger monitoreret? Vi foretager en grundig risikovurdering og vurderer, om compliancesystemer er operationelle og effektive.

Detect: Hvor god er jeres overvågning?

Tillid er godt, kontrol er bedre. Vi undersøger, om medarbejdere følger de foreskrevne politikker og procedurer. Vi måler og overvåger kvaliteten af virksomhedens kontrolapparat, herunder controllerfunktioner, intern revision m.m. Resultaterne rapporteres løbende tilbage til ledelsen med anbefalinger til forbedring.

Integrated detection: Hvor strategisk er jeres compliance?

Compliance er et komplekst net af interaktion mellem politikker, procedurer, systemer og mennesker. Med integrated detection løfter vi compliance ud af siloerne og sikrer, at viden konsolideres. Vi rådgiver om strategiske elementer og opbygger en virksomhedskultur, der understøtter virksomhedens strategiske forretningsmål.

Investigation: Hvad gør I, hvis noget går galt?

Vi opbygger fremadrettede complianceprogrammer for, hvordan I håndterer situationen, hvis noget går galt. Hurtig reaktion, klar kommunikation og medie håndtering er en integreret del af processen. Det er rapportering til interne og eksterne interessenter også. Vi tilrettelægger et forløb, så læring kontinuerligt samles op og deles.

Integrated Compliance: Hvad kan I opnå?

Integrated compliance sikrer, at den opbyggede compliancefunktion opererer som en naturlig del af virksomheden, og at der skabes effektivitet, transparens og værdi. Ved at flytte den silobaserede tilgang til fuld integration bliver compliancefunktionen en naturlig sparringspartner for virksomhedens daglige ledelse fra A til Z.

KONKRETE CASES OM COMPLIANCE

Har du lyst til at få mere viden om, hvordan Deloitte har hjulpet en række kunder med compliance kan du læse konkrete cases på vores hjemmeside: compliance.deloitte.dk

Vil du vide mere om Deloitte Compliance og Compliance360?

Kontaktpersoner



Thomas Brun
Equity Partner
+45 30 93 65 71
tbrun@deloitte.dk



Helena Barton
Partner
+45 30 93 68 13
hbarton@deloitte.dk



Anders Morand
Director
+45 30 93 61 95
amorand@deloitte.dk



Peter Brock Madsen
Director
+45 40 55 62 61
petermadsen@deloitte.dk