

ACCOUNTOR PORTAL SIKKERHED OG DATAERKLÆRING

Som professionel serviceudbyder tager vi ansvar for at overholde gældende love såvel som myndighedernes afgørelser. Vi forpligter os også til at følge bedste praksis i branchen i vores driftsoperationer. Vi håndterer alle personoplysninger ansvarligt og fortroligt. Dette er essentielt for at opfylde vores mission, som er at være den førende partner for virksomheder af alle størrelser og for at forbedre medarbejderoplevelsen. Vi har en stærk og stringent holdning til sikkerhed. Accountor er troværdig, ansvarlig og etisk over for vores kunder, partnere, medarbejdere, ledere og andre interessenter i alle vores operationer.

Governance: Databeskyttelse

Accountor har et governance-rammевærk for at sikre overholdelse af privatlivslove, interne politikker og branchens bedste praksis. Vi har etableret dedikerede roller for databeskyttelse i hele vores organisation. I vores governance-model styrer og overvåger Risiko- og Compliance udvalget, bestående af udvalgte medlemmer af lederteamet, overholdelsen af databeskyttelse og relaterede risici på gruppeniveau med hjælp fra Databeskyttelsesrådgiveren (DPO). DPO rapporterer til Chief Information Officer (CIO), som er medlem af Accountor Ledelsesteam.

Hver forretningsenhed er ansvarlig for implementering af databeskyttelseskrav i deres operationer. Databeskyttelsescheferne yder operationel privatlivsstøtte til enhederne. Databeskyttelsescheferne er en del af gruppen privatlivsteam ledet af DPO. Vi har en databeskyttelsespolitik godkendt af Risiko- og Complianceudvalget. Politikken er grundlaget for mere detaljerede instrukser om specifikke områder af databeskyttelse. Sådanne instruktioner omfatter ofte metoder til implementering i praksis, f.eks. risikovurderings- eller leverandørcompliance tjekskabeloner og processer.

Governance: Informationssikkerhed

Accountor har et informationssikkerhedsrammевærk, der er i overensstemmelse med branchens bedste praksis og gældende love. Vores Informationssikkerhedspolitik er godkendt af Risiko- og Complianceudvalget og bliver gennemgået årligt. Politikken implementeres gennem mere detaljerede instruktioner afledt heraf samt med daglige praksisser. ISO 27001 har været det vejledende rammевærk for politikken, instruktionerne og praksisserne.

Informationssikkerhed administreres af gruppen Informationssikkerheds ('InfoSec') Team. Holdet ledes af Group Information Security Officer ('CISO'), som rapporterer til CIO, der igen rapporterer til Accountors CEO. Informationssikkerhedsoperationer inkluderer udførelse af risikovurderinger og revisioner, oprettelse af arbejdsplaner for at reducere risici og implementering af disse arbejdsplaner. Implementering af sikkerhedsaktiviteter dokumenteres og gennemgås regelmæssigt. Accountor afholder årlige træningssessioner for sine medarbejdere i informationssikkerhed. Træningen afspejler politikken og instruktionerne for at sikre overholdelse af gældende krav.

Portal Informationssikkerhed og Databeskyttelse

Accountors portal er specifikt udviklet til at imødekomme Accountor-kunders behov. Mange forbedringer og nye funktioner vil være en del af den løbende udvikling heraf. Chief Information Security Officer og Databeskyttelsesrådgiveren er aktive interessenter i Accountor-portalen. Dette sikrer, at portalen udvikles og bruges i fuld overensstemmelse med regler og bestemmelser. Leverandører og partnere kræves også at overholde disse høje standarder. Portalen hostes af Accountors ISO 27001-certificerede IT-partner. Informationssikkerhedsafdelingen ledet af CISO udfører realtidssikkerhedsovervågning gennem forskellige værktøjer, herunder sårbarhedsscanninger, et 24/7-opererende Security Operations Center (SOC) og regelmæssige eksterne IT-audits. InfoSec har et vidtrækkende mandat til at handle i tilfælde af (ad-hoc) risici.

Branchens bedste-praksis algoritmer bruges til at beskytte autentificeringsoplysninger og data. Portalen bruger 'mindste privilegiums-princippet' til identitets- og adgangsstyring. Adgang til Accountor-medarbejdere gives på et Need to Know eller Need to Use basis. Samme princip og opsætning tilbydes til kundeadministratorerne, som selv er ansvarlige for at give eller tilbagekalde adgang og brugerrettigheder til deres egne brugere. Audit- og eventlogs indfanges, beskyttes og gennemgås regelmæssigt. Accountor tager og tester backups og har indbygget flere lag af redundans i firmaets platform.

For yderligere information er du velkommen til at tjekke informationerne i nedenstående links eller at kontakte din Accountor Business kontaktperson eller team.

<https://www.accountor.com/en/global/privacy-statement>
<https://www.accountor.com/en/global/privacy-compliance>
<https://www.accountor.com/en/global/contact>