Deloitte
Statsautoriseret
Revisionspartnerselskab
CVR-nr. 33 96 35 56
Weidekampsgade 6
Postboks 1600
0900 København C

Telefon: 36102030
Fax: 36102040
www.deloitte.dk

Informationssikkerhed og databeskyttelse i Deloitte

Fortrolighed vedrørende kundedata er essentiel for os
I Deloitte anser vi beskyttelse af kundedata, herunder også persondata, som en væsentlig forudsætning for et tillidsfuldt og troværdigt samarbejde med nuværende og kommende kunder.

Vi opfylder dette mål ved løbende at udvikle vores evne til proaktivt at identificere, vurdere og imødegå relevante risici i forbindelse med fortrolighed, integritet og tilgængelighed af kundedata af enhver art.

Deloittes tilgang til informationssikkerhed og databeskyttelse er baseret på den internationalt godkendte standard for informationssikkerhed, benævnt ISO/IEC 27001.

Deloitte er certificeret efter ISO/IEC 27001, hvilket bl.a. betyder, at Deloittes efterlevelse af kravene i standarden årligt bliver kontrolleret af 'British Standards Institution'.

Principper for håndtering af informationssikkerhed
Deloittes håndtering af informationssikkerhed sker ud fra den tilgang, at indsatsen altid er fokuseret på de relevante mål for beskyttelse af vores kunders fortrolige oplysninger. Udfra et princip om løbende tilpasning og forbedring, sikrer vi, at vi imødekommer det stadig stigende krav til informationssikkerhed bedst muligt.

Deloitte Danmark skal desuden som en del af det globale Deloitte-netværk overholde en lang række sikkerhedskontroller, som løbende justeres, så de modsvarer risikobilledet og vores kunders krav og forventninger til os.

Vi har bl.a. implementeret multi-faktor-autentificering i forhold til vores e-mails, hvormed vi indlægger et yderligere sikkerhedslag i forhold til den almindelige beskyttelse af fortrolige oplysninger.

Træning af medarbejdere er grundstenen
Deloittes medarbejdere udgør en grundsten i den fortrolige behandling af vores kunders data. Alle medarbejdere informeres og undervises derfor løbende i deres ansvar, forpligtelser og handlemuligheder. Alle medarbejdere skal overholde et sæt af grundlæggende kontroller, de såkaldte 'Basic Controls'.

Disse kontroller omfatter bl.a. guidelines for, hvordan medarbejderen kan og skal begrænse adgangen til fortrolige informationer og persondata til kun at inkludere de medarbejdere, der har behov for informationen for at kunne udføre deres arbejde.

Derudover omfatter kontrollerne en række faste procedurer, som eksempelvis:

- Opbevaring af data, herunder brug af passwords og applikationer
- Videregivelse af data, herunder brug af email-kommunikation og sikre kommunikationsplatforme
- Udskrift
- Destruktion af data der ikke længere er relevante for opgaven

Deloitte Quality Risk & Security, 31.10.2017