

POLITIK FOR DATAETIK

BDO Statsautoriseret revisionsaktieselskab



INDHOLD

- 3 **Politikkens formål**
- 3 **Anvendelsesområde**
- 3 **Ansvar for dataetik**
- 4 **Dataetiske principper og værdier**
- 5 **Behandling og anvendelse af data**
 - 6 *Produktionsdata*
 - 6 *Kundestamdata*
 - 7 *Markedsføringsdata*
 - 7 *Medarbejderdata*
 - 8 *Øvrige data*
- 8 **Strategi for dataetik**
- 9 **Overvågning og kontrol**
- 9 **Rapportering om dataetik**
- 9 **Opfølgning på politikken**
- 9 **Referencer**



POLITIK FOR DATAETIK

Politikkens formål

Ledelsen i BDO Statsautoriseret revisionsaktieselskab (BDO) fastlægger i denne politik rammerne for den dataetiske adfærd, der skal sikre faglig korrekt, ansvarlig og forsvarlig behandling af data i forretningsenheder og de administrative stabsfunktioner, således at BDO gennem åbenhed og gennemsigtighed kan fremstå med den ordentlighed og troværdighed, som kunder, medarbejdere, myndigheder og øvrige interessenter forventer af BDO.

Politik for dataetik er et supplement til BDO's politikker for informationssikkerhed, der fastsætter de overordnede krav til fortrolighed, integritet og tilgængelighed i behandlingen af data, herunder personoplysninger, baseret på relevante standarder for informationssikkerhed. Politik for dataetik supplerer desuden BDO's privatlivspolitikker, cookie-politikker og politikker for CSR og bæredygtighed.

Anvendelsesområde

Politik for dataetik omfatter BDO's dataetiske principper og værdier samt de etiske valg, der er truffet for BDO's behandling og anvendelse af data, baseret på anvendte teknologier sammenholdt med samfundsmæssige værdier og normer, og med et fokus på at understøtte BDO's mission og vision, værdigrundlag og forretningsmodel.

Politikken dækker alle typer af data, der behandles i forhold til kunder, medarbejdere, leverandører, samarbejdspartnere og øvrige interessenter, og som BDO selv skaber ved brug af teknologiske løsninger eller indsamler, herunder data fra eksterne kilder.

Politikken omfatter enhver form for behandling og anvendelse af data og supplerer databeskyttelsesforordningens principper om lovlighed, rimelighed og gennemsigtighed i behandlingen af personoplysninger, revisorlovens og straffelovens bestemmelser om tavshedspligt, hvidvasklovens bestemmelser om kundekendskabsprocedurer samt anden relevant lovgivning.

Politikken finder anvendelse i alle forretningsenheder og administrative stabsfunktioner og gælder for alle partnere og ledere og deres medarbejdere.

Ansvar for dataetik

Overvejelser, dilemmaer og principper inden for dataetik forankres i informationssikkerhedsudvalget, som har til opgave at behandle og indstille politik for dataetik til ledelsens godkendelse.

Risk & Compliance er ansvarlig for at udarbejde og vedligeholde politik for dataetik og at implementere denne i organisationen ved at inddrage partnere og ledere i forretningsenhederne og de administrative stabsfunktioner, herunder træne relevante medarbejdere i dataetik. Risk & Compliance er desuden ansvarlig for at overvåge og kontrollere det daglige arbejde med dataetik.

Ansvar for efterlevelse af politik for dataetik er placeret hos partnere og ledere i forretningsenhederne og de administrative stabsfunktioner, der tilsikrer, at de dataetiske retningslinjer følges i det daglige arbejde inden for deres ansvarsområder, at medarbejdere har kendskab til og efterlever politikken, og at dataetiske vurderinger indgår i enhver proces og forretningsgang, der omfatter behandling af data.

Risk & Compliance sikrer i samarbejde med partnere og ledere i forretningsenhederne og de administrative stabsfunktioner, at anvendte leverandører af ydelser inden for databehandling lever op til de dataetiske principper og værdier.

Dataetiske principper og værdier

De dataetiske principper og værdier er defineret med udgangspunkt i den etiske dimension af forholdet mellem på den ene side BDO's dataanvendelse og brug af teknologier til databehandling og på den anden side menneskers fundamentelle rettigheder til privatliv og databeskyttelse, retssikkerheden og de grundlæggende samfundsmæssige værdier, som BDO anerkender og respekterer.

BDO har indført nedenstående grundlæggende dataetiske principper og værdier, der indgår i arbejdet med at sikre en forsvarlig dataetisk behandling og anvendelse af data.



Velfærd og værdighed

BDO prioriterer mennesker før kommercielle interesser, og behandlingen og anvendelsen af data må ikke skade det enkelte menneske og skal ske med respekt for og under hensyn til sociale forhold, samfund og demokrati.



Privatliv og frihed

BDO respekterer privatlivet og de grundlæggende frihedsrettigheder i et demokratisk samfund. Behandlingen og anvendelsen af data skal begrænses til nødvendige data fra godkendte kilder, data må ikke opbevares i længere tid en højst nødvendigt, og deling af data skal begrænses mest muligt.



Retssikkerhed

BDO respekterer de grundlæggende retssikkerhedsmæssige forhold i samfundet, og behandlingen og anvendelsen af data skal ske i henhold til den enhver tid gældende lovgivning.



Selvbestemmelse

BDO støtter mennesket i at træffe oplyste og selvstændige valg og giver så vidt muligt det enkelte menneske kontrol over egne data i behandlingen og anvendelsen, herunder kontrol med hvilke data, der indsamles, hvad data anvendes til, og i hvilke sammenhænge.



Lighed

BDO sikrer lighed ved ikke i sin behandling og anvendelse af data at diskriminere på baggrund af etnicitet, religion, køn, seksualitet, politiske holdninger eller andre helt private oplysninger, og ved at sørge for mangfoldighed og diversitet i udvikling og anvendelse af nye teknologier.



Gennemsigtighed

BDO giver indsigt i egne data og informerer klart og forståeligt om behandlingen og anvendelsen af data, herunder dens formål, funktion, sikkerhed og begrænsninger.



Sikkerhed

BDO sikrer, at behandlingen og anvendelsen af data er tilstrækkelig sikker, robust og pålidelig, at overvågning og udøvelse af tilsyn og kontrol er effektiv, og at potentielle fejl og etiske konsekvenser kan identificeres, evalueres, dokumenteres og minimeres.



Ansvarlighed

BDO er ansvarlig for enhver behandling og anvendelse af data og udvikling af nye teknologier herfor, og BDO træffer de nødvendige foranstaltninger for at undgå misbrug af data eller andre utilsigtede handlinger.

Behandling og anvendelse af data

Forsvarlig dataetisk behandling og anvendelse af data fastlægges på grundlag af de dataetiske principper og værdier, hvor BDO tilstræber, inden for lovgivningens rammer, at finde en rimelig balance mellem fordele og konsekvenser på både kort og langt sigt. Dette arbejde omfatter:



Behandling og anvendelse af data er opdelt i følgende datatyper og behandlingskategorier:

- **Produktionsdata:** Data i revisions- og rådgivningsopgaver og Business Services & Outsourcing
- **Kundestamdata:** Data i form af kunders virksomhedsoplysninger og personoplysninger
- **Markedsføringsdata:** Data fra hjemmeside, kommunikationssystemer og sociale medier
- **Medarbejderdata:** Data på medarbejdere og ansøgere
- **Øvrige data:** Data på leverandører og samarbejdspartnere

Produktionsdata

I udførelsen af opgaver inden for revision, udvidet gennemgang og andre erklæringsopgaver indsamler BDO de data, der er nødvendige for at udføre opgaverne, fra kunden selv og fra eksterne kilder, fx offentlige myndigheder og kundens pengeinstitutter, advokater, kunder og leverandører. Data registreres og opbevares i systemer, der understøtter opgaveprocessen, og BDO strukturerer, sammenstiller, samkører og analyserer indsamlede data som dokumentation for udført arbejde.

I udførelsen af regnskabs- og rådgivningsopgaver indsamler BDO de data, der er nødvendige for at udføre opgaverne, fra kunden selv og fra eksterne kilder. Data registreres og opbevares i systemer, der understøtter opgaveprocessen, og behandlingen og anvendelsen af data sker i overensstemmelse med kundeaftalen.

Kunden indsender bogføringsbilag, bankoplysninger og andre dokumenter med relevans for bogføringen til BDO, når Business Services & Outsourcing udfører bogføringsassistance på vegne af kunden. Data registreres i økonomistyringssystemer og andre systemer, der administrerer data til brug for kundens regnskab, og BDO anvender de indsamlede data i forbindelse med afstemninger, kontroller og rapporteringer.

Kunden indsender løngrundlag og personoplysninger for kundens medarbejdere til BDO, når Business Services & Outsourcing udfører lønadministration på vegne af kunden. Data registreres i lønbehandlingssystemer, og BDO anvender de indsamlede data i forbindelse med kontroller, lønafstemninger og rapporteringer.

BDO indsamler data fra kunder via spørgeskemaer og anvender allerede indsamlede data fra kunder med det formål at udarbejde SMV Barometret, der er en statistiks undersøgelse af tilstanden hos de mindre og mellemstore virksomheder. Indsamlede data registreres, sammenstilles, samkøres og analyseres med henblik på at danne og præsentere grafiske illustrationer i en rapport.

BDO anvender produktionsdata til analyser, benchmarking mv., der dels anvendes til dokumentationsformål, dels til rådgivning af brancher. BDO anvender anonyme data, og der udarbejdes ikke brancheanalyser, hvis der er mindre end 15 virksomheder i populationen. BDO sikrer, at brancheanalyser ikke vil kunne skade den enkelte virksomhed.

BDO videregiver kundens data, når det følger af aftalen med kunden, og når der er behov for at udveksle data med medlemsvirksomheder i BDO-netværket. Kundens data videregives desuden, når offentlige myndigheder og det internationale BDO-netværk gennemfører kvalitetskontrol og tilsyn, og når BDO er forpligtet til det i medfør af gældende lovgivning eller domstols- og myndighedsafgørelse, herunder indberetninger til offentlige myndigheder. Videregivelsen begrænses til det omfang, som er nødvendigt for formålet.

BDO opbevarer kundens data i den periode, som revisorloven, anden særlovgivning eller behandlingsprincipperne i databeskyttelsesforordningen foreskriver, hvorefter kundens data slettes.

Kundestamdata

I forbindelse med kundeaccept og kundeopgaveaccept indsamler BDO relevante virksomhedsoplysninger samt personoplysninger om virksomhedens personkreds og de legale og reelle ejere (kundestamdata), herunder personlig dokumentation i form af kørekort, pas eller lignende dokumenter i henhold til hvidvasklovgivningen. BDO registrerer kun de kundestamdata, der er nødvendige for at kunne overholde lovgivningen.

Kundestamdata og dokumentation registreres i et centralt kundestamdatasystem og system for styring af kunder, kundeopgaver og hvidvaskdokumentation.

BDO videregiver kundestamdata, når offentlige myndigheder gennemfører tilsyn, og når BDO er forpligtet til det i medfør af gældende lovgivning eller domstols- og myndighedsafgørelse, herunder indberetninger til Hvidvasksekretariatet i National Enhed for Særlig Kriminalitet i tilfælde af mistanke om involvering i hvidvask eller finansiering af terrorisme. Videregivelsen begrænses til det omfang, som er nødvendigt for formålet.

Kundestamdata slettes ikke i kundestamdatasystemet med henvisning til, at BDO skal kunne dokumentere uafhængighed i medfør af revisorloven og imødekomme krav om internationalt konflikttjek fra BDO-netværket. Dokumentation, der er indhentet i henhold til hvidvaskloven, opbevares, så længe et kundeforhold består, og slettes 5 år efter et kundeforholds ophør.

Markedsføringsdata

BDO indsamler og registrerer data om kunders, medarbejders og besøgendes digitale adfærd på tværs af anvendte platforme, herunder BDO's egne websider og øvrige digitale kommunikationssystemer og sociale medier. Denne indsamling og registrering sker efter forudgående samtykker til blandt andet indsamling af adfærdsdata og data til profilering samt udsendelser af e-mails. Et afgivet samtykke kan til enhver tid tilbagekaldes.

BDO anvender kun de data, som den enkelte kunde, medarbejder eller besøgende aktivt har valgt at give BDO adgang til. BDO sammenstiller de indsamlede data med generiske kundestamdata og medarbejderdata fra henholdsvis kundestamdatasystemet og HR-systemet. BDO videregiver ikke indsamlet data, og BDO køber ikke personspecifikke data fra databrokers eller andre virksomheder til at berige egne data.

Indsamlede og registrerede data anvendes til automatisk segmentering og personalisering af BDO's produkter, ydelser og services gennem videregivet information i form af valgte interesser, virksomhedsnavn, jobtitel og postnummer i sammenhæng med generel adfærd på websider, når der givet samtykke hertil. Formålet er at give kunder relevant og aktuel viden samt at målrette kommunikation om nye og eksisterende produkter, ydelser og services ud fra en overvejelse om, at det er i kundens interesse at få information, der er relevant.

BDO misbruger ikke cookie-data eller andre informationer, der fremkommer ved kunders og andre virksomheders søgninger og visninger. BDO har respekt for den enkelte persons og virksomheders søgninger på hjemmesiden.

Data opbevares i administrative systemer, og periode for opbevaring og tidspunkt for sletning af data er for hver datatype og -kategori fastlagt i overensstemmelse med databeskyttelsesforordningens bestemmelser om dataminimering og opbevaringsbegrænsning.

Medarbejderdata

I rekrutteringsprocessen indsamler BDO data på ansøgere fra ansøgeren selv og fra eksterne kilder. Data registreres og opbevares i rekrutteringssystemet. Data videregives ikke. Periode for opbevaring og tidspunkt for sletning af data på ansøgere er fastlagt til 6 måneder i overensstemmelse med lovgivningen.

I ansættelsesprocessen indsamler BDO data på kandidater fra kandidaten selv og fra eksterne kilder. Data registreres og opbevares i HR-systemet. BDO indhenter kandidatens straffeattest for gennemgang, men opbevarer den ikke. Nødvendige data på kandidater videregives til relevante offentlige myndigheder og virksomheder, fx forsikrings- og pensionsselskaber, i forbindelse med onboarding.

Under ansættelsen indsamler BDO data på medarbejdere fra medarbejderen selv, ledelsen og eksterne kilder, herunder medarbejdererklæring om tavshedspligt og uafhængighed, referater fra medarbejderudviklingssamtaler og samtykkeerklæringer i forskellige forhold. Data registreres og opbevares i HR-systemet og andre administrative systemer. Nødvendige data på medarbejdere videregives til relevante offentlige myndigheder og virksomheder. Data slettes ikke så længe, at medarbejderen er ansat.

Ved ansættelsesforholdets ophør registrerer BDO fratrædelsesdato og øvrige nødvendige data på medarbejderen i forbindelse med offboarding. Data registreres og opbevares i HR-systemet. Nødvendige data videregives til relevante offentlige myndigheder og virksomheder, og data slettes 5 år efter, at medarbejderen er fratrukket.

Øvrige data

BDO indsamler og registrerer virksomhedsdata på leverandører og samarbejdspartnere samt personoplysninger for disses medarbejdere i forbindelse med såvel indgåelse af leveranceaftaler, fortrolighedsaftaler og databehandleraftaler som den daglige drift. Databehandlingen sker for at dokumentere indgåede kontraktlige forpligtelser.

Data videregives ikke, medmindre BDO er forpligtet hertil i henhold til gældende lovgivning eller domstols- eller myndighedsafgørelse. Data opbevares i administrative systemer, og periode for opbevaring og tidspunkt for sletning af data er fastlagt i overensstemmelse med bogføringslovens krav til opbevaring af regnskabsmateriale.

Strategi for dataetik

Udviklingen i samfundet og den stigende digitalisering forventes at betyde øget brug af nye teknologier og automatiseringer i udvikling og forbedring af BDO's produkter, ydelser og services og i den måde, som BDO adresserer sit marked på. Tilsvarende gælder BDO's løbende arbejde med at optimere og effektivisere sine processer og forretningsgange.

Anvendelse af nye teknologier, fx kunstig intelligens, maskinlæring eller træning af algoritmer, stiller krav til beskrivelse af, hvordan og til hvilke formål disse anvendes, og krav om at inddrage de dataetiske principper og værdier og dermed gennemføre dataetiske vurderinger i ethvert fremtidigt projekt om behandling og anvendelse af data.

I den sammenhæng er BDO bevidst om, at anvendelsen af nye teknologier ikke må medføre eksempelvis forskelsbehandling, forudindtagede og skævvredne resultater (bias) eller forudsigelser om mønstre i adfærdsdata, uden at selvbestemmelsesretten respekteres. BDO er desuden bevidst om, at de ny teknologier for behandling og anvendelse af data skal være lettilgængelige og forståelige.

I takt med den digitale udvikling vil der løbende ske udvikling af nye værktøjer og metodikker, hvor nye dataetiske spørgsmål skal afklares. Informationssikkerhedsudvalget skal løbende tage stilling til spørgsmål, der ikke er afklaret i denne politik for dataetik, og om nødvendigt opdatere den i overensstemmelse med retningslinjerne for opfølgning på politikken.

Overvågning og kontrol

Risk & Compliance er ansvarlig for løbende at overvåge og kontrollere, om politik for dataetik overholdes, og om de nødvendige dataetiske vurderinger udarbejdes især ved implementering af nye systemer med kompleks behandling af data eller ved anvendelse af ny, avanceret teknologi i databehandlingen.

Som et led i den løbende overvågning og kontrol tilrettelægges der uddannelse og awarenesskampagner om dataetik med henblik på at højne og vedligeholde nye og eksisterende medarbejderes kompetencer og dermed medvirke til, at politik for dataetik iagttages og udvikles i takt med nye databehandlingsmetoder og teknologier.

Uddannelse og awarenesskampagner medvirker desuden til at skabe en positiv fejkultur, hvor medarbejdere tør være åbne om fejl og problemer i de datadrevne systemer. En sådan åbenhed og gennemsigtighed er med til at forbedre og optimere dataanvendelsen og højne datasikkerheden.

Rapportering om dataetik

BDO er omfattet af pligten til at redegøre for politik for dataetik i årsrapportens ledelsesberetning i overensstemmelse med årsregnskabslovens § 99 d. Politik for dataetik danner grundlag for denne redegørelse.

Risk & Compliance forestår rapportering af arbejdet med dataetik. Rapporteringen sker løbende til informationssikkerhedsudvalget, der behandler væsentlige risici. Bestyrelsen orienteres i overensstemmelse med den fastlagte forretningsorden for rapportering af complianceforhold og i forbindelse med aflæggelsen af årsrapporten.

Opfølgning på politikken

Risk & Compliance gennemgår, evaluerer og vurderer politik for dataetik løbende, herunder om den skal opdateres. Resultatet af dette arbejde indstilles til behandling i informations sikkerhedsudvalget.

Gennemgang, evaluering og vurdering skal ske mindst en gang årligt og i forbindelse med anvendelse af ny teknologi eller ny metode for behandling og anvendelse af data.

Referencer

Politik for dataetik har reference til lovgivning og andre interne politikker:

- Årsregnskabslovens § 99 d om redegørelse for politik for dataetik i ledelsesberetningen
- BDO's politikker for informationssikkerhed
- BDO's privatlivspolitikker
- BDO's cookiepolitikker
- BDO's politikker for CSR og bæredygtighed

Copyright © BDO Statsautoriseret revisionsaktieselskab

Alle rettigheder forbeholdes. Mekanisk, fotografisk, elektronisk eller anden form for gengivelse eller mangfoldiggørelse af denne brochure eller dele heraf er ikke tilladt uden BDO's skriftlige samtykke ifølge gældende dansk lov om ophavsret. Undtaget herfra er korte uddrag til brug for omtale.

BDO Statsautoriseret revisionsaktieselskab, danskejet rådgivnings- og revisionsvirksomhed, er medlem af BDO International Limited - et UK-baseret selskab med begrænset hæftelse - og del af det internationale BDO-netværk bestående af uafhængige medlemsfirmaer.

BDO er varemærke for både BDO netværket og for alle BDO medlemsfirmaerne. BDO i Danmark beskæftiger mere end 1.300 medarbejdere, mens det verdensomspændende BDO netværk har ca. 95.000 medarbejdere i mere end 164 lande.

10.2022 - PSC