# POLITIK FOR DATAETIK

# SDC A/S

# FEBRUAR 2024

# INDHOLD

# 1 Indledning

Data har stor værdi og har stort potentiale til at påvirke strategiske og kommercielle beslutninger for virksomheder i den finansielle sektor. Et væsentligt element i SDC's strategi er at gøre vores kunder i stand til at skabe øget vækst og forretningsværdi på baggrund af deres data.

SDC har en vigtig rolle som it-leverandør til finansielle virksomheder i de nordiske lande og behandler store mængder data på vegne af vores kunder. Det er derfor af afgørende betydning for SDC, at vi i alle henseender behandler data korrekt, sikkert og på en etisk forsvarlig måde.

SDC tager sit ansvar som databehandler alvorligt. Vi ønsker at blive opfattet som en respekteret, kompetent og ordentlig samarbejdspartner, der overholder den til enhver tid gældende lovgivning og følger udviklingen inden for god dataadfærd og -etik. Denne politik har til formål at bidrage til dette.

SDC's behandling af data strækker videre end GDPR, da SDC som full-service it-leverandør indsamler og opbevarer mange værdifulde data på vegne af vores kunder. Dataetik er derfor relevant for SDC's behandling og anvendelsen af alle former for data og går videre end overholdelse af lovgivningen vedrørende beskyttelse af persondata.

SDC's politik for dataetik gælder for hele SDC, herunder SDC's filial i Polen.

Denne politik skal anvendes i overensstemmelse med og som en del af SDC's IT-sikkerhedspolitik, SDC's Persondatapolitik, SDC's Outsourcingpolitik samt SDC's IT-risikostyringspolitik.

# 2 SDC's anvendelse af data

SDC behandler store mængder data på vegne af vores kunder. Det drejer sig både om persondata og andre typer data, som tilhører vores kunder. Vi behandler vores kunders data sikkert og fortroligt og i overensstemmelse med de aftalte krav og standarder, herunder krav til behandling af persondata og finansielle data.

Derfor har SDC implementeret en lang række tekniske og organisatoriske foranstaltninger for at demonstrere et passende højt og tilstrækkeligt niveau af databeskyttelse. Beskyttelse af privatliv og data er nøgleelementer i at bevare tilliden hos SDC's kunder, medarbejdere og partnere. SDC sikrer, at vores kunder efter behov kan supplere deres data i SDC's systemer med data fra andre samarbejdspartnere og fra egne systemer. Data herfra er med til at kvalificere vores kunders forretningsstyring og kunderettede aktiviteter.

Enhver behandling af data skal ske under iagttagelse af kravene i SDC's IT-sikkerhedspolitik. Formålet med denne er at sikre, at der er en effektiv styring af adgangen for

medarbejdere og eksterne brugere til SDC's lokaler, faciliteter og data samt forebygge og/eller mindske ulemperne ved funktionsfejl og sikre data- og informationsfortrolighed ud fra begreberne om Fortrolighed, Integritet og Tilgængelighed (FIT).

SDC sikrer gennem overholdelse af IT-sikkerhedspolitikken, at både kundedata og SDC's egne data er korrekte, konsistente og fuldstændige.

SDC har implementeret processer og systemer for adgangsstyring, som sikrer, at adgang til data i SDC er baseret på et arbejdsbetinget behov.

SDC's medarbejdere er både under og efter ansættelsen i SDC forpligtet til at iagttage en ubetinget tavshedspligt med hensyn til oplysninger om SDC's interne forhold, systemer og kunder. Dette er præciseret i den enkeltes ansættelseskontrakt samt i SDC's persondata-politik for medarbejdere.

SDC indsamler ikke data egne selvstændige behov eller formål, fx profilering af individer. Dette er således ikke en del af den aktuelle forretningsstrategi eller de nuværende forretningsaktiviteter.

SDC behandler udelukkende vores kunders data med henblik på at levere de aftalte ydelser til vores kunder.

# 3 Forankring i organisationen

SDC's ledelse er ansvarlig for at sikre, at hvert forretningsområde i SDC inkluderer overvejelser om pålidelig og korrekt anvendelse af data i udvikling og vedligeholdelse af systemer og processer. Systemejerskab er entydigt placeret i organisationen. SDC's organisationsstruktur er decentral, svarende til ansvarsfordeling, og sikrer effektiv intern kontrol, rapportering og opfølgning.

Aktiviteter for at sikre forsvarlig brug af data indgår i de daglige arbejdsrutiner, så det ønskede niveau kan opnås med færrest muligt administrative og organisatoriske ressourcer, samt med fokus på at undgå udfordringer i forhold til nøglepersoner mv.

Det daglige arbejde med dataetik foregår i SDC's enkelte forretningsområder. Relevante interne processer og retningslinjer for dokumentation og håndtering af data, herunder persondata, bliver løbende implementeret og gennemgået. Endvidere har SDC et større antal underliggende politikker, processer og retningslinjer om brug af persondata mv., som løbende bliver gennemgået eller opdateret efter behov. De indgår alle i de organisatoriske trin for at sikre, at der træffes passende foranstaltninger og for at dokumentere kravet om ansvarlighed i henhold til GDPR og IT-sikkerhed.

Alle interne politikker, processer og retningslinjer er tilgængelige for alle medarbejdere på SDC's intranet. Der sker løbende uddannelse og sikkerhedstræning af alle medarbejdere, blandt andet ved onboarding af nye medarbejdere og konsulenter.

# 4 Samarbejde med leverandører

SDC stiller en række krav sine leverandører. Flere af disse krav udspringer af den lovgivning, som den finansielle sektor er underlagt, herunder krav til finansielle virksomheders outsourcing, og andre krav udspringer fra SDC's kunder.

Det følger blandt andet af SDC's outsourcingpolitik, at der skal ske en forudgående undersøgelse (due diligence) af alle outsourcing-leverandører. Herudover stiller SDC en lang række kontraktuelle krav af henholdsvis databeskyttelses- og outsourcing-relateret karakter.

SDC fører tilsyn med sine leverandører. Dette er forankret bredt i SDC's organisation med tilhørende processer og ejerskab. Der er et særligt fokus på tilsyn i forhold til GDPR og outsourcing.

# 5 Anvendelse af nye teknologier

SDC har etableret både interne og eksterne boards, som inddrages i beslutninger om anvendelse af ny teknologi og som rådgiver til øvrige afdelinger i SDC for så vidt angår tværgående spørgsmål om IT-arkitektur.

IT-Sikkerhedschefen er ansvarlig for det sikkerhedsmæssige aspekt af databeskyttelse i SDC. Opgaven består i at sikre et passende teknisk og organisatorisk niveau af sikkerhedsforanstaltninger i SDC samt bistå forretningen med løbende sparring om passende tekniske og organisatoriske sikkerhedsforanstaltninger.

SDC's DPO skal inddrages, hvis en anvendelse af nye teknologier medfører behandling af persondata.

SDC justerer løbende sine politikker og tilføjer guidelines, når ny teknologi tilsiger det. I 2023 har SDC tilføjet en guideline for brug af Public AI-engines.

SDC's kunder skal som dataansvarlige foretage en analyse af de påtænkte behandlingsaktiviteters konsekvenser for beskyttelse af personoplysninger, dvs. en konsekvensanalyse, før der igangsættes en ny behandling af data, som kan indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder SDC vil som databehandler bistå vores kunder med at sikre overholdelse af forpligtelserne i forhold til gennemførelse af konsekvensanalyser og levere aftalte bidrag under hensyntagen til behandlingens karakter og de oplysninger, der er tilgængelige for SDC.

# 6 Vedligeholdelse

Disse retningslinjer for dataetik er opdateret den 1. februar 2024 og er godkendt af SDC's direktion.

Legal & Compliance gennemgår mindst en gang årligt retningslinjerne og foretager de nødvendige tilpasninger med inddragelse af relevante områder i SDC's organisation. Opdateringer forelægges til godkendelse for direktionen.