BALLERUP KOMMUNE

POLITIK OG ORGANISATION
Digitalisering og Forretningsudvikling

Dato: 5. maj 2022

E-mail: jan@balk.dk
Kontakt: John A. Nielsen

Sagsid: 85.15.00-P30-1-22

Informationssikkerhedspolitik for Ballerup Kommune

Denne informationssikkerhedspolitik er den overordnede politik for informationssikkerhed i Ballerup Kommune. Behandlingen af data udgør en af Ballerup kommunes væsentligste kilder til værdiskabelse i mødet med borgerne. Borgernes fortsatte tillid til, at Ballerup Kommune håndterer deres data forsvarligt er derfor afgørende for kommunens virksomhed. Det skal denne politik sikre, ligesom den skal forebygge sikkerhedsbrist og tab af data.

Ballerup Kommune anvender på flere områder, og i større omfang, digitale løsninger for at leve op til de krav, som borgere, virksomheder, øvrige samarbejdspartnere og lovgivningen stiller til en effektiv administration, og til en hurtig og korrekt service over for kommunens borgere og virksomheder.

Informationssikkerhedspolitikken udmøntes af linjeledelse og de eksisterende rolleindehavere i kommunens tværgående styringsstruktur for det digitale område.

Egedal, Furesø, Allerød og Ballerup Kommuner samarbejder med it-driftsselskabet IT-Forsyningen I/S som de ejer sammen. IT-Forsyningen varetager en væsentlig del af Ballerup Kommunes daglige IT-drift

og support. Da IT-Forsyningen ikke er en del af Ballerup Kommunes organisation, bliver IT-Forsyningen, i forbindelse med databeskyttelse, betragtet som en ekstern 3. part på lige fod med kommunens øvrige leverandører.

Formål
Både data og digitale løsninger er nødvendige for offentlige virksomheder, og databeskyttelse er derfor af vital betydning for Ballerup Kommunes troværdighed og funktionsdygtighed.

Formålet med informationssikkerhedspolitikken er at definere rammer for beskyttelse af kommunens data og særligt sikre, at kritiske og følsomme data og digitale løsninger bevarer deres fortrolighed, integritet og tilgængelighed. Derfor har ledelsen af Ballerup Kommune besluttet et beskyttelsesniveau, der er afstemt efter risiko og væsentlighed samt overholder lovkrav og indgåede aftaler. Sikkerhedsarbejdet tilrettelægges i overensstemmelse med anbefalingerne i informationssikkerhedsstandarden ISO27001.

Hensigten med informationssikkerhedspolitikken er endvidere at tilkendegive over for alle, som har relation til kommunen, at anvendelse af data og digitale løsninger er underkastet standarder og retningslinjer. På den måde kan sikkerhedsproblemer forebygges, eventuelle skader kan begrænses og reetablering af information kan sikres.

Sikre kommunens borgere og virksomheder adgang til en stabil og korrekt kommunal service
Ballerup Kommune har som målsætning, at servicere kommunens borgere og virksomheder på bedst mulige måde. Informationssikkerhedspolitikken har som mål at sikre en tilgængelighed og pålidelighed i kommunens håndtering af data, og sikre at de digitale løsninger understøtter en korrekt borgerservice. Herigennem kan kommunen opnå og bibeholde troværdighed over for kommunens borgere, virksomheder og det offentlige som helhed.

Fortrolighed i forvaltningen
Det er kommunens målsætning, at de digitale løsninger og forvaltningen
som helhed skal sikre, at behandlingen af data og informationer sker med fortrolighed og i overensstemmelse med god forvaltningsskik. Informationssikkerhedspolitikken skal derfor medvirke til, at informationer om borgerne og virksomheder holdes fortroligt for uvedkommende.

Gyldighed og omfang

Kommunens informationssikkerhedspolitik er gældende for alle data, der behandles i kommunen - herunder også data som ikke tilhører kommunen, men som Ballerup Kommune kan gøres ansvarlig for. Dette omfatter alle kommunens afdelinger, enheder og institutioner, hvor der sker en indsamling, anvendelse og eventuel bearbejdning af data. Det inkluderer f.eks.:

- alle data om personale
- alle data om finansielle forhold
- alle data som bidrager til administration af kommunen
- alle data der omhandler virksomheder og borgerne, også når borgeren er en elev eller forælder.

Politikken omfatter også anlægsdata samt andre former for data som er overladt kommunen af andre. Disse data kan være faktuelle oplysninger, optegnelser, registreringer, rapporter, forudsætninger for planlægning eller enhver anden information, som kun er til intern brug. Politikken omfatter kommunens data ligegyldigt i hvilken form de opbevares og formidles på.

Denne politik gælder for alle ansatte uden undtagelse, både fastansatte, politikere og personer som midlertidigt arbejder for Ballerup Kommune. Alle disse personer bliver her betegnet som medarbejdere.

Informationssikkerhedspolitikken gælder tillige for eksterne parter, herunder medarbejdere ansat i virksomheder, som varetager den udliciterede it-drift, supplerende it-arbejdspladser i hjemmet eller andre lokaliteter uden for kommunen, der ad elektronisk vej etablerer forbindelse til kommunens systemer og data. Politikken gælder tillige når persondata som kommunen er ansvarlig for behandles af en 3. part.

Ballerup Kommune skal sammen med samarbejdspartnere af den udliciteret eller hostet it-drift sikre, at kommunens sikkerhedsniveau fastholdes. Dette gælder ligeledes, når samarbejdspartneren anvender eksterne konsulenter til løsning af it-opgaver.

Sikkerhedsniveau
Ballerup Kommune skal træffe fornødne foranstaltninger til at beskytte oplysninger om personer mod uautoriseret anvendelse og mod fejl i de registrerede eller forarbejdede oplysninger. Sikkerhedsniveauet og it anvendelsen i Ballerup Kommune skal til hver en tid være i overensstemmelse med gældende lovgivning og skal sikre, at kommunen kan opfylde sine kontraktuelle forpligtelser.

Ballerup Kommune fastlægger på baggrund af en konkret risikovurdering et sikkerhedsniveau, som svarer til følsomheden af de pågældende data. Ballerup Kommune sikrer løbende overholdelses af gældende lovgivning og regler samtidigt med at de digitale redskaber designes så de understøtter smidige og effektive arbejdsgange.

I al behandling af data sikrer Ballerup Kommune korrekt sikkerhed og beskyttelse af data, samt at data er valide:

- Alle data har en entydig autoritativ kilde dvs. data fødes og vedligeholdes, hvor viden om data er, og når data benyttes uden for den autoritative kilde, skal disse altid være opdaterede og retvisende i forhold til den autoritative kilde
- Medarbejdere sikres adgang til alle nødvendige data for at træffe oplyste og korrekte beslutninger i en given sag i henhold til gældende lovgivning
- Den korrekte identitet bag en given adgang til systemerne er kendt og autoriseret.

Afbalanceret og styret databeskyttelse
Ballerup Kommunes databeskyttelse skal overholde gældende lovgivning, og kommunen fastlægger på baggrund af konkret risikovurdering et sikkerhedsniveau, som svarer til følsomheden af de pågældende data.

Sikkerhedsniveauet skal fastholdes igennem såvel tekniske som organisatoriske rammer. Dermed spiller såvel tekniske kontroller som organisationens og brugernes adfærd en væsentlig rolle i forhold til den samlede databeskyttelse. Samtidig skal det sikres, at politikken implementeres på en måde, så de forretningsmæssige processer understøttes bedst muligt, inden for de givne juridiske rammer.

Ansvar for/godkendelse af informationssikkerhedspolitikken
Kommunalbestyrelsen har det overordnede ansvar for informationssikkerhedspolitikken, herunder fastlæggelse af de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger for overholdelse af lovgivning, sikkerhedsbestemmelser m.m.

I hver valgperiode godkender Kommunalbestyrelsen informationssikkerhedspolitikken og skal en gang i hver valgperiode have en redegørelse for sikkerhedsarbejdet i kommunen. Herudover skal Digitalisering og Forretningsudvikling gennemgå politikken mindst en gang årligt med henblik på at sikre, at den er fyldestgørende og afspejler de faktiske forhold.

Det operationelle ansvar for styring af databeskyttelsen er placeret hos Digitaliseringschefen. Denne har ansvaret for, at de aktiviteter,

standarder, retningslinjer, kontroller og foranstaltninger, der er beskrevet i sikkerhedsportalen, gennemførers og efterleves.

Digitaliseringschefen skal ligeledes sikre, at kommunens ledere integrerer politikken i alle forretningsgange, driftsopgaver og projekter.

Sikkerhedsdokumentation
Informationssikkerhedspolitikken og de fastsatte retningslinjer er grundlaget for det daglige databeskyttelsesarbejde, inkl. de sikkerhedsadministrative opgaver.

Det er den enkelte leders ansvar, at enhver medarbejder i kommunen med adgang til administrative systemer og data har kendskab til informationssikkerhedspolitikken og de tilhørende retningsliner, som er relevante for deres arbejde i kommunen. Det skal til hver en tid være muligt for medarbejderne at få adgang til retningslinjer og underliggende procedurer, hvis der måtte være brug for dette. Informationssikkerhedspolitikken med tilhørende Retningslinjer for databeskyttelse skal være tilgængelig på Ballerup Kommunens hjemmeside og intranet.

Nye medarbejdere skal ved ansættelsen introduceres til de gældende databeskyttelseskrav og informeres om den forventede adfærd i relation til disse.

Beredskabsplanlægning
I samarbejde med leverandører af kommunens it-drift, etableres der et beredskab, som skal sikre, at Ballerup Kommune i tilfælde af større driftsnedbrud eller egentlige katastrofer er i stand til at genoptage kritiske forretningsmæssige aktiviteter inden for en ledelsesgodkendt tidshorisont. Større driftsnedbrud eller katastrofer betyder tab af tilgængelighed af væsentlige systemer, udstyr og/eller faciliteter, hvorfor retablering af tilgængeligheden af disse er et centralt område i beredskabsplanlægningen. Beredskabsplanlægningen skal indgå som en del af den samlede beredskabsplan for Ballerup Kommune.

Der skal minimum én gang årligt foretages en gennemgang af den aktuelle beredskabsplan.

Databeskyttelsesbevidsthed
Databeskyttelsesbevidsthed vedrører kommunens samlede dataportefølje, og gennemførelse af en politik for databeskyttelse kan ikke foretages af ledelsen alene. Alle medarbejdere har et ansvar for at beskytte kommunens data mod uautoriseret adgang, ændringer og ødelæggelse samt tyveri. Alle medarbejdere skal derfor uddannes i databeskyttelse i relevant omfang.

Som brugere af Ballerup Kommunes data skal alle medarbejdere følge informationssikkerhedspolitikken og de tilhørende retningslinjer. Medarbejderne må kun anvende kommunens data i overensstemmelse med det arbejde, de udfører i kommunen, og skal beskytte data på en måde, som er i overensstemmelse med informationernes følsomhed.

Forebyggende sikkerhed
Det er Ballerup Kommunes målsætning, at databeskyttelsen skal sikres gennem forebyggende tiltag og aktiviteter, så medarbejderne i kommunen kan fokusere på borgerservice i stedet for at rette op på sikkerhedsbrud.

Databeskyttelse via viden
Det er Ballerup Kommunes målsætning, at databeskyttelsen skal etableres og fastholdes gennem krav til brugeradfærd, samt en målrettet formidling af viden om databeskyttelse til de medarbejdere og eksterne parter, der har kontakt med de kommunale data, herunder medarbejdere ansat i virksomheder, som varetager it-drift.

Brud på datasikkerheden
Bevidst eller ubevidst overtrædelse af informationssikkerhedspolitikken og de tilhørende retningslinjer kan medføre, at kommunens brugere, samarbejdspartnere, borgere mv. oplever kompromittering af relevante data, ustabilitet, uregelmæssigheder og uhensigtsmæssigheder i anvendelse og bearbejdning af kommunens informationer. Dette kan dels medføre forringelse af den kommunale service og kommunens image og dels økonomisk tab.

Overtrædelse af informationssikkerhedspolitikken og hertil knyttede retningslinjer er at betragte, som en tjenstlig forseelse, og skal, i samarbejde med afsnit for Digitalisering og Forretningsudvikling behandles af den respektive ansvarlige leder som sådan og i overensstemmelse med gældende personalepolitiske bestemmelser herfor.

Databeskyttelsesorganisationen skal indrettes, så situationer med overtrædelse eller manglende overholdelse, samt forsøg på uautoriseret anvendelse, kan rapporteres til Digitalisering og Forretningsudvikling via den respektive ansvarlige leder inkl. angivelse af hændelsesforløb og konsekvens til videre behandling.

I situationer, hvor ikke alene kommunens databeskyttelsespolitik bliver overtrådt, men også lovgivningsmæssige regler, kan gældende straffelov og andre strafbestemmelser få konsekvenser for de involverede medarbejdere.

Organisation og ansvar

Kommunalbestyrelsen har det overordnede ansvar for informationssikkerhedspolitikken og derunder indretningen af databeskyttelsesopgaverne, så de er tilpasset kommunens behov og samtidig opfylder kravene i lovgivningen og god forvaltningsskik.

Kommunaldirektøren uddelegerer det daglige ansvar for databeskyttelsesarbejdet til Digitaliseringschefen. Centercheferne er systemejere, og hermed ansvarlige for overholdelse af databeskyttelsen i de fagspecifikke systemer i deres ansvarsområde.

Vedligeholdelse af informationssikkerhedspolitikken

De generelle uddybende databeskyttelsesretningslinjer og procedurer struktureres i overensstemmelse med ISO27001 standarden. Retningslinjerne skal gennemgås mindst hvert år.

Årligt revideres et sæt af procedurer og et årshjul, der fastlægger og danner grundlag for efterlevelse af informationssikkerhedspolitikken og de detaljerede retningslinjer om databeskyttelse.

Godkendelse

Informationssikkerhedspolitikken er godkendt af Ballerup Kommunes kommunalbestyrelse den 30. maj 2022, og afløser den tidligere godkendte informationssikkerhedspolitik fra den 27 august 2018.