BALLERUP KOMMUNE

BALLERUP KOMMUNE

Dato: 31. mai 2018

Ballerup Kommune

# Politik for ~~informationssikker-hed~~databeskyttelse

## Politik for databeskyttelse i Ballerup Kommune

Denne ~~informationssikkerhedspolitik~~databeskyttelsespolitik er den overordnede ramme for ~~informationssikkerheden~~databeskyttelsen i Ballerup Kommune. Politikken skal sikre, at Ballerup Kommune fortsat kan sikre kommunens høje troværdighed, forebygge sikkerhedsbrist og tab af data ~~og informationer.~~. Behandlingen af data ~~og informationer~~ udgør Ballerup kommunes væsentligste kilder til værdiskabelse i mødet med borgerne.

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 overfor kommunens borgere og virksomheder.

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

Egedal, Furesø og Ballerup Kommune har sammen etableret it-driftsselskabet IT-Forsyningen I/S. ~~ITForsyningen~~IT-Forsyningen varetager en væsentlig del af Ballerup Kommunes daglige drift og support. Da IT-Forsyningen ikke er en del af Ballerup Kommunes organisation, bliver IT-~~Forsyningen~~forsyningen, i forbindelse med ~~informationssikkerhed~~databeskyttelse, betragtet som en ekstern 3. part på lige fod med kommunens øvrige leverandører.

### Formål

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

Formålet med ~~informationssikkerhedspolitikken~~Politik for databeskyttelse er at definere rammer for beskyttelse af kommunens ~~informationer~~ data og særligt sikre, at kritiske og følsomme ~~informationer~~data og ~~informationssystemer~~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 informations-sikkerhedsstandarden ISO27001.

~~væsentlighed samt overholder lovkrav og indgåede aftaler. Sikkerhedsarbejdet tilrettelægges i overensstemmelse med anbefalingerne i informations-sikkerhedsstandarden ISO27001.~~

Hensigten med ~~sikkerhedspolitikken~~Politik for databeskyttelse er endvidere at tilkendegive over for alle, som har relation til kommunen, at anvendelse af ~~informationer og informationssystemer~~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~~

Politik for databeskyttelse har som mål at sikre en tilgængelighed og pålidelighed i kommunens ~~informations~~ håndtering~~, så it-anvendelsen~~ af data og sikre at de digitale læsninger 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 ~~it-anvendelsen~~de digitale løsninger og forvaltningen som helhed skal sikre, at behandlingen af data og informationer sker med fortrolighed og i overensstemmelse med god offentlig forvaltningsskik.
~~Informationssikkerhedspolitikken~~ Politik for databeskyttelse skal derfor medvirke til, at informationer om borgerne og virksomheder holdes fortroligt for uvedkommende.

## Gyldighed og omfang

Kommunens ~~informationssikkerhedspolitik~~Politik for databeskyttelse er gældende for ~~enhver information~~alle data, der tilhører kommunen - herunder også ~~informationer~~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.:

~~anvendelse og eventuel bearbejdning af data og informationer. 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 ~~informationer~~andre former for data som er overladt kommunen af andre. Disse data kan være faktuelle oplysninger, optegnelser, registreringer, rapporter, forudsæt-

ninger for planlægning eller enhver anden information, som kun er til intern brug.

Politikken omfatter kommunens ~~informationer~~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~~Politik for databeskyttelse 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.

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 ~~itanvendelsen~~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 konkret risikovurdering et sikkerheds-niveau, som svarer til betydningen af de pågældende ~~informationer.~~ data.

Ballerup Kommune ~~gennemfører en balanceret risiko-~~sikrer løbende overholdelses af gældende lovgivning og ~~konsekvensvurdering~~ 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:

~~valide:~~

- Alle data har en entydig autoritativ kilde dvs. data fødes og vedligeholdes, hvor viden om data er, og når data benyttes udenfor 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 ~~informationssikkerhed~~databeskyttelse**
Ballerup Kommune har som målsætning, at ~~informationssikkerheden er differentieret i forhold til lovgivningen samt de værdier~~databeskyttelsen overholder gældende lovgivning og ~~informationer~~fastlægger på baggrund af konkret risikovurdering et sikkerheds-niveau, som ~~skal beskyttes, sammen-holdt med et realistisk trusselsbillede.~~svarer til betydningen af de pågældende data.

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

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

~~lovgivning, sikkerhedsbestemmelser mm.~~

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

~~fyldestgørende og afspejler de faktiske forhold.~~

Det operationelle ansvar for styring af ~~informationssikkerheden~~databeskyttelsen er placeret hos chefen for Digitaliseringssekretariatet. Denne har ansvaret for, at de aktiviteter, standarder, retningslinjer, kontroller og

foranstaltninger, der er beskrevet i sikkerhedsportalen, gennemførers og efterleves.

Sekretariatschefen skal ligeledes sikre, at kommunens ledere integrerer ~~informations-sikkerheden~~politikken i alle forretningsgange, driftsopgaver og projekter.

**Sikkerhedsdokumentation**

~~Informationssikkerhedspolitikken~~Politik for databeskyttelse og de fastsatte retningslinjer er grundlaget for det daglige ~~sikkerhedsarbejde~~databeskyttelsesarbejde, inkl. de ~~sikkerheds-administrative~~sikkerhedsadministrative opgaver.

Det er den enkelte leders ansvar, at enhver medarbejder i kommunen med adgang til administrative systemer og data har kendskab til ~~informationssikkerhedspolitikken~~Politik for databeskyttelse 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.

Politik for databeskyttelse med tilhørende Retningslinjer for databeskyttelse skal være tilgængelig på Ballerup Kommunens hjemmeside og intranet.

Nye medarbejdere skal ved ansættelsen introduceres til de gældende ~~informations-sikkerhedskrav, samt~~
databeskyttelseskrav og informeres om den forventede adfærd i relation til ~~it-anvendelsen.~~disse.

**Beredskabsplanlægning**

I samarbejde med leverandører af kommunens it-drift, skal der etableres 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 ~~informations-portefølje~~dataportefølje, og gennemførelse af en politik for databeskyttelse kan ikke foretages af ledelsen alene. Alle medarbejdere har et ansvar for at beskytte kommunens ~~informationer~~data mod uautoriseret adgang, ændringer og ødelæggelse samt tyveri. Alle medarbejdere skal derfor uddannes i ~~informationssikkerhed~~databeskyttelse i relevant omfang.

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

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

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

**Brud på ~~informationssikkerheden~~datasikkerheden**
Bevidst eller ubevidst overtrædelse af ~~sikkerhedsbestemmelserne~~Politik for databeskyttelse 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~~Politik for databeskyttelse og hertil knyttede retningslinjer er at betragte, som en tjenstlig forseelse, og skal, i samarbejde med Digitaliseringssekretariatet 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 Digitaliseringssekretariatet via den respektive ansvarlige leder inkl. angivelse af hændelsesforløb og konsekvens til videre behandling.

~~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~~Politik for databeskyttelse og derunder indretningen af ~~sikkerhedsopgaverne~~databeskyttelsesopgaverne, så de er tilpasset kommunens behov og samtidig opfylder kravene i
lovgivningen og god forvaltningsskik.

Kommunaldirektøren uddelegerer det daglige ansvar for ~~sikkerhedsarbejdet~~databeskyttelsesarbejdet til chefen for Digitaliseringssekretariatet.

Center-/sekretariatscheferne er systemejere, og hermed ansvarlige for overholdelse ~~af informationssikkerheden~~databeskyttelsen i de fagspecifikke systemer i deres ansvarsområde.

**Vedligeholdelse af ~~informationssikkerhedspolitikken~~Politik for databeskyttelse**

De generelle uddybende ~~informationssikkerhedsretningslinjer~~databeskyttelsesretningslinjer og procedurer struktureres i overensstemmelse med ISO27001 standarden. Retningslinjerne skal gennemgås mindst hvert år.
Der udarbejdes et sæt af procedurer og et årshjul, der fastlægger og danner grundlag for efterlevelse af Politik for databeskyttelse og de detaljerede retningslinjer om databeskyttelse.
~~informationssikkerhedspolitikken og de detaljerede retningslinjer om informationssikkerhed.~~

**Godkendelse**

~~Denne informationssikkerhedspolitik~~Politik for databeskyttelse er godkendt af Ballerup Kommunes kommunalbestyrelse den ~~29.08.2016~~XX.XX.18, og afløser den tidligere godkendte ~~informationssikkerheds-politikker.~~Informationssikkerhedspolitik fra den 29.08.16.