Aabenraa Kommune

# Overordnet politik for informationssikkerhed og databeskyttelse i Aabenraa Kommune

# Indholdsfortegnelse

## Indledning

Dette dokument beskriver Aabenraa Kommunes overordnede rammer for informationssikkerhed og databeskyttelse.

Aabenraa Kommune behandler oplysninger om borgere og virksomheder, som ofte er af følsom karakter og kræver særlig beskyttelse. God informationssikkerhed og databeskyttelse skal derfor være en integreret del af kommunens service til borgere og virksomheder og dermed også en integreret del af det daglige arbejde for ledere, medarbejdere og andre brugere.

Disse rammer skaber, sammen med en løbende risikovurdering, grundlaget for sikker anvendelse af informationsteknologi i Aabenraa Kommune, hvilket er med til at sikre, at tilliden til Aabenraa Kommune opretholdes.

## Formål

Informationer og informationssystemer er nødvendige for Aabenraa Kommunes virke og livsvigtige for nogle borgere. Informationssikkerhed og databeskyttelse har derfor vital betydning for kommunens troværdighed og funktionsdygtighed, så kommunen altid fremstår som en respekteret og betroet myndighed.
Formålet med politikken for informationssikkerhed og databeskyttelse er:

- At definere en ramme for beskyttelse af kommunens informationer, der både tager højde for lovkravene, borgernes tillid til kommunen og en dagligdag, der skal hænge sammen
- At sikre, at kritiske og følsomme informationer i informationssystemer bevarer deres fortrolighed, integritet og tilgængelighed
- At beskyttelsesniveauet afstemmes efter risiko og væsentlighed
- At overholde lovkrav og indgåede aftaler, herunder licensbetingelser
- At oplyse medarbejderne om deres ansvar i relation til virksomhedens informationer og informationssystemer
- At forebygge sikkerhedsproblemer, begrænse eventuelle skader og sikre reetablering af informationer.
- At tilkendegive over for alle som har relation til kommunen, at anvendelsen af informationer og informationssystemer er underkastet standarder og retningslinjer.

Politikken for informationssikkerhed og databeskyttelse skal ligeledes skabe et udgangspunkt for reglerne for informationssikkerhed og databeskyttelse, hvor politikkens principper bliver udmøntet.

## Omfang

Politikken omfatter Aabenraa Kommunes behandling af informationer.
Dette omfatter enhver information, som tilhører kommunen samt informationer, kommunen kan gøres ansvarlig for. Det inkluderer f.eks.:

- Alle informationer om borgere, personale og økonomi
- Alle data, der bidrager til administration af kommunen
- Data overladt til Aabenraa Kommune af andre
- Alle informationsaktiver, uanset hvordan de opbevares eller formidles og uanset form (elektronisk, fysisk eller menneskelig)
- Alle systemer, der tilhører og/eller anvendes af Aabenraa Kommune og som indeholder eller behandler informationer

Politikken gælder for alle medarbejdere, herunder:

- Alle kommunens ansatte uden undtagelse, både fastansatte og personer, som midlertidigt arbejder for kommunen.
- Politikere i Byrådet og politiske udvalg[1]
- Eksterne konsulenter, som arbejder i eller for Aabenraa Kommune
- Alle medarbejdere, der er ansat under aftaleenheder, herunder selvejende institutioner

Ved outsourcing af dele af IT-driften (service- og supportaftaler) skal det sikres i samarbejde med serviceleverandøren, at Aabenraa Kommunes sikkerhedsniveau fastholdes, så serviceleverandøren, dens faciliteter og de medarbejdere, som har adgang til Aabenraa Kommunes informationer, mindst lever op til kommunens informationssikkerhedsniveau.

## Principper for sikkerhedsniveau

Aabenraa Kommune skal sikre, at sandsynligheden for og konsekvenserne af et sikkerhedsbrud reduceres til et acceptabelt niveau (også kaldet risikovillighed), så:

- Borgerne til stadighed kan føle sig trygge ved at overlade deres data til kommunen.
- Aabenraa Kommune sikrer medarbejdernes tryghed og arbejdsvilkår.
- Aabenraa Kommune sikrer genoptagelse af normal drift inden for de aftalte tidsfrister.

Sikkerhedsniveauet skal fastlægges på baggrund af risikovurderinger. I risikovurderingen skal der både kigges på ISO 27001 og GDPR, hvilket vil sige, at der både skal risikovurderes i forhold til til Kommunen (kaldet forretningen i ISO-standarden) og til den registrerede (borgeren).

Risiko- og konsekvensvurderinger gennemføres mindst en gang årligt, under hensyntagen til balancen mellem investering i tid til risikovurdering og det formodede sikkerhedsniveau, så ledelsen kan holde sig informeret om det aktuelle risikobillede. Der foretages ligeledes en konkret risikovurdering ved større forandringer i organisationen eller systemerne, samt ved nye projekter eller tiltag, der involverer behandling af personoplysninger.

Politikken for informationssikkerhed og databeskyttelse tager udgangspunkt i god IT-skik og best-practice, samt standarder og lovgivning på området.

Aabenraa Kommune vil tage udgangspunkt i ISO 27001 standardens principper for styring af informationssikkerhed, herunder planlægning, implementering, revurdering og forbedring af styringsindsatsen, samt tage udgangspunkt i ISO 27001 Anneks A[2] som overordnet ramme for valg af organisatoriske, adfærdsmæssige, tekniske, fysiske tiltag, i det omfang der er sammenhæng mellem sikkerhed, funktionalitet og økonomisk investering.

Aabenraa Kommunes informationssikkerhed og databeskyttelse skal leve op til:

1) Sikkerhedsmæssige krav, der udspringer af lovgivning. Som følge af Aabenraa Kommunes omfattende opgaver og dermed behandling af personoplysninger, gælder specielt databeskyttelsesforordningen og lovgivning omkring persondata.
2) Sikkerhedsmæssige krav, der er aftalt med myndigheder eller samarbejdspartnere.

Det er vigtigt at informationssikkerhed og databeskyttelse har et forretningsorienteret afsæt og en pragmatisk tilgang, så borgernes og virksomhedernes data på en omkostningseffektiv og professionel vis

[1] Byrådet er fritaget for at efterleve GDPR jf. kommunalstyrelsesloven § 8b, men Byrådet er stadig underlagt kommunens informationssikkerhedsregler jf. ISO 27001 for at sikre Aabenraa Kommune mod brud på IT-sikkerheden. Det kan f.eks. være diverse e-læringskurser, regler for skift af password og andre tiltag, der tager udgangspunkt i ISO 27001.
[2] Anneks A indeholder 114 anbefalede kontrolmål og kontroller, man skal forholde sig til for at efterleve ISO-standarden

sikres bedst muligt, og derved styrker borgernes og virksomhedernes tillid til kommunens behandling af deres data.

Informationssikkerhed og databeskyttelse i Aabenraa Kommune skal fastlægges på baggrund af en *risikobaseret tilgang* og som en afvejning af de ofte modstridende hensyn til for eksempel:

- Ønsket om *tilstrækkelig sikkerhed* så kommunens troværdighed ikke kan drages i tvivl.
- Krav om *efterlevelse af lovgivning* på området, særligt omkring databeskyttelse.
- *Omkostningerne* ved investeringer i sikkerhed og hensynet til økonomisk ansvarlighed.
- Den *sociale gevinst* ved en given digitalisering eller behandling af informationer.
- Ønsket om *brugervenlighed* i det daglige arbejde, så foranstaltninger ikke opleves som en barriere, men også muliggør den faglige professionalisme og udfoldelsesfrihed.

Et meget højt sikkerhedsniveau kan for eksempel medføre høje omkostninger eller indvirke på de daglige processer eller kvaliteten af den ydede service. Derfor skal den konkrete tilgang både afveje de ovennævnte hensyn og efterleve lovgivning og indgåede aftaler.

## Organisering

Direktionen beslutter organiseringen af informationssikkerhed og databeskyttelse. Direktionen har besluttet, at informationssikkerhedsudvalget består af Den Digitale Styregruppe. Den nærmere organisering af informationssikkerhed og databeskyttelse er tilgængelig på medarbejderportalen.

Det operationelle ansvar for den daglige styring af informationssikkerhedsindsatsen, er placeret hos IT- og digitaliseringschefen, der fungerer som sikkerhedsleder. Denne sikrer, at de aktiviteter, standarder, retningslinjer, kontroller og foranstaltninger, der er beskrevet i informationssikkerhedsreglerne[3], gennemføres og efterleves. Ligeledes er det væsentligt, at informationssikkerhed integreres i alle forretningsgange, driftsopgaver og projekter.

Til at rådgive og vejlede Direktionen og til at føre tilsyn med at Aabenraa Kommune overholder databeskyttelsesforordningen, har Aabenraa Kommune udpeget en databeskyttelsesrådgiver. Direktionen har besluttet at placere Databeskyttelsesrådgiveren hos ekstern rådgiver. Databeskyttelsesrådgiveren fremlægger årligt en rapport, der skal belyse den gældende situation ift. databeskyttelse.

## Sikkerhedsbevidsthed

Gennemførelse af en politik for informationssikkerhed og databeskyttelse kan ikke foretages af ledelsen alene. Alle medarbejdere har et ansvar for at bidrage til at beskytte kommunens informationer mod uautoriseret adgang, ændring og ødelæggelse samt tyveri. Alle medarbejdere skal derfor løbende uddannes i informationssikkerhed og databeskyttelse i relevant omfang, dette er et ledelsesansvar.

Som bruger af Aabenraa Kommunes informationer skal alle medarbejdere følge politikken for informationssikkerhed og databeskyttelse, de underliggende regler og de retningslinjer, der er afledt heraf.

Kommunens informationer må udelukkende anvendes til udførelse af de relevante arbejdsopgaver. Informationerne skal beskyttes i overensstemmelse med deres følsomhed, særlige og/eller kritiske indhold.

## Overtrædelse

Den enkelte medarbejder har ansvaret for efterlevelse af gældende sikkerhedspolitikker og regler. Medarbejdere, som ikke overholder politikken for informationssikkerhed og databeskyttelse eller deraf

[3] https://medarbejderportalen.aabenraa.dk/media/0ppp4smj/regler-for-informationssikkerhed-2020.pdf?format=noformat

afledte retningslinjer, vil blive behandlet i overensstemmelse med Aabenraa Kommunes gældende regler og personalepolitik[4].
Såfremt en medarbejder opdager trusler mod informationssikkerheden eller brud på denne, skal dette straks meddeles til sikkerhedslederen, databeskyttelsesrådgiveren eller nærmeste leder.

## Revision

Informationspolitikken revurderes, hvert andet år inden udgange af andet kvartal. Ændringer af politikken fremlægges i Informationssikkerhedsudvalget efter indstilling fra sikkerhedslederen.
Herefter behandles ændringer af direktionen og besluttes i Økonomiudvalget.

## Godkendt

Politikken er behandlet den 17. juni 2024 i Informationssikkerhedsudvalget
Politikken er behandlet den 26. juni 2024 i Direktionen
Politikken er godkendt den 13. august 2024 i Økonomiudvalget.

[4] https://medarbejderportalen.aabenraa.dk/til-ledere/mit-personale/retningslinjer-vejledninger-personalepolitikker-og-hr-regnskaber