Lersø Parkallé 112, 2.
2100 København Ø
Tlf 33 85 45 00
info@ok-fonden.dk

OK-FONDENS DATABESKYTTELSESPOLITIK
8. MAJ 2018

OKF-003

Indhold

1. Mål for databeskyttelse og behandling

OK-Fondens vision er, at mennesker kan forfølge deres drømme og leve livet – hele livet, og ønsket om den enkeltes selvbestemmelse og tryghed er omdrejningspunktet i OK-Fondens arbejde, uanset det enkelte menneskes livssituation, alder og helbred.

Da OK-Fonden som grundlag for sin virksomhed registrerer en række følsomme oplysninger om beboere, brugere og medarbejdere er det vigtigt for efterlevelse af visionen, at OK-Fonden gennem en effektiv databeskyttelse medvirker til, at der er tillid til OK-Fondens ydelser og administration.

OK-Fonden ser derfor et højt databeskyttelsesniveau både som et krav om at kunne overholde lov- og myndighedskrav og som et kvalitetselement for at kunne tilbyde en sikker service for beboere, brugere, medarbejdere, kommuner og andre samarbejdspartnere.

Databeskyttelse er derfor en nøgleværdi i OK-Fondens automatiske og manuelle databehandling af oplysninger, herunder sikker behandling af personoplysninger.

1.1 Omfang

Databeskyttelsespolitikken beskriver de af ***ledelsen fastsatte*** målsætninger for databeskyttelse i OK-Fondens afdelinger, aktieselskaber, institutioner samt de tilknyttede selvejende institutioner og boligselskaber. Den danner grundlag for udformning af OK-Fondens ***databeskyttelseshåndbog*** med de underliggende retningslinjer og forretningsgange.

Databeskyttelsespolitikken er gældende for alle ***medarbejdere*** i OK-Fondens afdelinger, aktieselskaber og institutioner og i de tilknyttede selvejende institutioner.

Alle ***leverandører og samarbejdspartnere***, der er databehandlere for OK-Fonden og som har fysisk eller logisk adgang til systemer, data og personoplysninger, skal gøres bekendt med OK-Fondens databeskyttelsespolitik og efterkomme den.

Databeskyttelsespolitikken dækker alle ***tekniske og administrative forhold***, der har direkte eller indirekte indflydelse på drift og brug af de anvendte automatiske databehandlingssystemer samt manuelle arkiver og registre.

I det omfang Ok-Fonden eller en institution er databehandler for en dataansvarlig kommune eller anden virksomhed, har instrukser fastsat af den dataansvarlige forrang i forhold til OK-Fondens databeskyttelsespolitik.

Databeskyttelsespolitikken er især formuleret med henblik på beskyttelse af personoplysninger, men den finder tilsvarende anvendelse på økonomiske- og andre data.

1.2 Hovedmålsætninger for sikkerheden

Under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene gennemfører OK-Fonden passende tekniske og organisatoriske foranstaltninger, der sikrer et sikkerhedsniveau, som passer til disse risici.

Et passende og tilstrækkeligt databeskyttelsesniveau[1] opnås igennem tekniske og organisatoriske foranstaltninger, der sikrer:

- ***vedvarende fortrolighed, integritet, tilgængelighed og robusthed*** af OK-Fondens behandlingssystemer og behandlingstjenester i forhold til den risikovurdering, der er gennemført for de enkelte systemer og typer af personoplysninger.
- anvendelse af ***pseudonymisering og kryptering,*** hvor det er relevant, herunder ved dataudveksling med databehandlere og eksterne parter og offentlige myndigheder
- evnen til rettidigt at ***genoprette tilgængelighed*** af og adgangen til data i tilfælde af en fysisk eller teknisk hændelse
- en procedure for regelmæssig ***afprøvning, vurdering og evaluering*** af databeskyttelsessikkerheden
- beskyttelse af OK-Fondens it-aktiver, oplysninger og data i OK-Fondens varetægt.

Et tilstrækkelige sikkerhedsniveau ***fastholdes*** ved

- at der ***vedvarende*** forefindes ***retningslinjer og forretningsgange***, som sikrer, at databeskyttelse er en integreret del af OK-Fondens drift og daglige arbejde
- at have en ***kontinuerlig forbedringsproces***, der løbende vedligeholder og optimerer databeskyttelsespolitikken, retningslinjer og forretningsgange
- *at det* igennem ***kontrakt- og leverandørstyring*** sikres, at brugen af eksterne leverandører, konsulenter og samarbejdspartnere lever op til den gældende databeskyttelseslovgivning og OK-Fondens databeskyttelsesniveau
- at der i forbindelse med indførelse af ***nye IT-systemer*** gennemføres:
    - passede tekniske og organisatoriske foranstaltninger med henblik på gennem standardindstillinger at sikre, at kun personoplysninger, der er ***nødvendige*** behandles
    - en evt. analyse af de påtænkte behandlingsaktiviteters konsekvenser for beskyttelse af personoplysninger, hvis det skønnes nødvendigt (***Konsekvensanalyse***)

[1] Som beskrevet i Databeskyttelsesforordningen artikel 32

1.3 Hovedmålsætning for behandling af personoplysninger

OK-Fonden har som mål at tilrettelægge sin administration og at anvende egnede databehandlings-systemer, så det sikres, at OK-Fonden kan leve op til ***lovgivningens principper og regler for behandling af personoplysninger***.

Ledelsen fastsætter derfor principper og forretningsgange for OK-Fondens behandling af personoplysninger, der sikrer overholdelse af Databeskyttelsesforordningen og Databeskyttelsesloven. Forretningsgangene, der ***dokumenteres***, omfatter

- ***principper for behandling af personoplysninger***
- anvendelse af ***samtykke*** som grundlag for behandling af personoplysninger
- procedurer for udøvelse af den ***registreredes rettigheder,*** herunder underretning ved registrering og udøvelse af retten til berigtigelse, sletning eller begrænsning af behandling og ret til dataportabillitet
- ***fortegnelser udarbejdet over behandlingsaktiviteter*** med personoplysninger
- underretning om ***brud på datasikkerheden*** til Datatilsynet og den registrerede
- ***konsekvensanalyse***, når dette er relevant ved indførelse af nye behandlingssystemer
- databeskyttelse gennem ***design og standardindstillinger***

OK-Fonden benytter leverandører som ***databehandlere***, der i aftaler stiller de fornødne garantier for, at de leverer passende tekniske og organisatoriske foranstaltninger, således at behandlingerne opfylder regler og principper i lovgivningen herunder, at det er beskrevet, hvordan databehandleren sikrer fortrolighed, integritet, tilgængelighed og robusthed.

OK-Fonden vil endvidere lægge vægt på, at de anvendte databehandlingssystemer er indrettet således, at OK-Fonden nemt og hurtigt kan administrere udøvelsen af de registreredes rettigheder.

2. De samlede regler for databeskyttelse og databehandling

OK-Fondens samlede regler for databeskyttelse og behandling består af:

- OK-Fondens databeskyttelsespolitik
- Databeskyttelseshåndbog med sikkerheds- og behandlingsregler
- Medarbejdervejledning og -erklæring om databeskyttelse

Med hensyn til datasikkerhed følger OK-Fonden retningslinjerne i den internationale standard ISO 27001, men da OK-Fondens kerneopgave er social service og ikke databehandling, og da fonden i meget vidt omfang hoster sine IT-programmer og data, herunder personoplysninger hos eksterne databehandlere, ønsker OK-Fonden ikke at gennemføre en egentlig certificering.

OK-Fonden vil under hensyntagen til implementerings- og driftsomkostninger, behandlingernes karakter, risici og alvor for beboernesnes rettigheder sikre passende organisatoriske og tekniske foranstaltninger om sikkerhed i OK-Fonden og ***gennem databehandleraftaler med leverandørerne***.

OK-Fonden vil ved aftaler med leverandører lægge vægt på, at de tilbudte løsninger understøtter muligheden for nemt og hurtigt at kunne opfylde forpligtelserne i lovgivningen med hensyn til de registreredes rettigheder herunder underretning ved registrering og udøvelse af retten til berigtigelse, sletning eller begrænsning af behandling og ret til dataportabillitet

OK-Fonden vil tillægge det positiv vægt, såfremt en leverandør overholder en godkendt ***adfærdskodeks*** som omhandlet i Databeskyttelsesforordningens artikel 40 eller er ***certificeret*** efter forordningens artikel 42.

3. Centraliseret dataansvar og bindende regler

De samlede regler for databeskyttelse- og databehandling gælder for OK-Fondens administration og institutioner, der hører direkte under OK-Fonden samt for aktieselskaber, der er ejet af OK-Fonden og selvejende institutioner, hvor OK-Fonden er repræsenteret i bestyrelsen, og hvor der er indgået en bindende aftale om, at OK-Fonden varetager dataansvaret for institutionens/aktieselskabets behandling af personoplysninger som dataansvarlig og/eller databehandler for en kommune.

I ***bilag 1*** findes en oversigt, der viser, hvilke institutioner, der hører direkte under OK-Fonden samt aktieselskaber, selvejende institutioner og boligselskaber, hvor der er indgået aftale om, at OK-Fonden varetager dataansvaret.

I ***bilag 2*** findes teksten til de ***aftaler***, der indgås om, at OK-Fonden varetager dataansvaret for institutionen, aktieselskabet eller boligselskabet. Det fremgår heraf at de er er forpligtet til at følge de samlede regler for databeskyttelse og databehandling fastsat af OK-Fonden.

I de tilfælde, hvor ***OK-Fonden fungerer som databehandler for private institutioner eller foreninger,*** der ikke er omfattet af OK-Fondens bindende virksomhedsregler (fx administration for boligforeninger, eller HR-administration for selvejende institutioner), udarbejder OK-Fonden en databehandleraftale, der tiltrædes af de pågældende i forbindelse med indgåelse af aftale om, at OK-Fonden fungerer som databehandler for foreningen/institutionen.

4. Overordnet organisering og hosting af personoplysninger

OK-Fonden ønsker som hovedregel at anvende databehandlersystemer og opbevaring af personoplysninger ***hos eksterne leverandører***, der sikkert hoster og stiller IT-systemer til rådighed, således at OK-Fonden ikke selv har behov for at råde over kompetence til at drifte sådanne systemer.

OK-Fonden ønsker endvidere i videst muligt omfang at organisere opbevaringen af personoplysninger således, at personoplysninger om de enkelte personer ikke findes fordelt på flere systemer og både i elektronisk og manuel form.

Viser en analyse af en ønsket behandling af personoplysninger, det tekniske niveau i løsningen, behandlingens karakter, risici for databrud samt implementerings- og

driftsomkostninger, at det vil være mest hensigtsmæssigt, kan der etableres systemer og opbevaring af data i institutionen elektronisk og/eller i manuelle systemer.

5. Databeskyttelsesrådgiver

OK-Fonden, der er en privat virksomhed, skal som udgangspunkt efter Databeskyttelsesforordningens artikel 37 ikke udpege en databeskyttelsesrådgiver, idet OK-Fondens kerneaktivitet er social service og ikke overvågning eller behandling af følsomme oplysninger.

Nogle af OK-Fondens selvejende institutioner har imidlertid driftsoverenskomst med en enkelt kommune, hvor forholdene er så regulerede, at institutionen er en del af den offentlige forvaltning. Disse institutioner skal ifølge Databeskyttelsesforordningens artikel 37 stk. 1, a) udpege en databeskyttelsesrådgiver.

OK-Fondens ledelse udpeger en databeskyttelsesrådgiver for de institutioner, der er en del af den offentlige forvaltning. Databeskyttelsesrådgiveren varetager de i Databeskyttelsesforordningen artikel 39 nævnte opgaver vedrørende OK-Fondens funktioner som dataansvarlig for egne systemer og personoplysninger og funktionen som databehandler, hvor en kommune er dataansvarlig. Databeskyttelsesrådgiveren kan endvidere efter OK-Fondens ledelses beslutning udføre andre opgaver og have andre pligter ud over dem, der er omfattet af funktionen som databeskyttelsesrådgiver.

I ***bilag 3*** er angivet de af OK-Fondens tilknyttede selvejende institutioner, der er en del af den offentlige forvaltning, og som derfor skal udpege en databeskyttelsesrådgiver.

6. Ansvar og organisering

OK-Fondens målsætning er, at alle medarbejdere har ansvar for datasikkerheden, og at de er bekendte med og efterlever OK-Fondens databeskyttelsespolitik, retningslinjer og forretningsgange, der er beskrevet i databeskyttelseshåndbogen.

På hver institution, boligselskab og aktieselskab omfattet af de bindende virksomhedsregler og på OK-Fondens hovedkontor udpeges en datasikkerhedsansvarlig, der sammen med lederen af enheden er ansvarlig for behandlingen af personoplysninger og for behandling af klager og henvendelser fra de registrerede.

Et antal af de ansvarlige i de selvejende institutioner og et antal af de ansvarlige i OK-Fondens egne afdelinger og institutioner udgør en ***Databeskyttelsesgruppe***, der nedsættes af OK-Fondens ledelse og som med støtte fra OK-Fondens direktion skal sikre reglernes efterlevelse og løbende opdatering.

Planlægning, implementering og kontrol af datasikkerheden er defineret af **OK-Fondens** ledelse, der også er ansvarlig for implementering og vedligeholdelse af databeskyttelsessystemet og er ansvarlig for opfølgning på sikkerhedshændelser.

OK-Fondens lokale ledere fastsætter således som angivet i
databeskyttelseshåndbogen, hvem der har ansvaret for

- hver af institutionernes, ***automatiske og manuelle databehandlingssystemer***,
- styring af ***systemadgang og netværksadgang***,
- tildeling af rettigheder, indgåelse af ***IT-kontrakter og andre kontrakter***,
- ***indkøb af hardware og installation af software,***
- behandling af ***henvendelser fra de registrerede,***
- ***registrering*** og dokumentation af ***brud på datasikkerheden*** – uanset alvorlighed
- evt. ***anmeldelse af brud på persondatasikkerheden*** til Datatilsynet og
- evt. ***underretning af de registrerede***, der er berørt af bruddet

Databeskyttelsespolitikken revurderes og godkendes én gang årligt, eller i forbindelse med eventuelle situationer, der nødvendiggør det.

Ledere og medarbejdere er ansvarlige for at efterleve retningslinjer og procedurer for datasikkerhed i det daglige arbejde. Medarbejdere, der konstaterer eller oplever brud på datasikkerheden, skal anmelde det hurtigst muligt til lederen.

Den nødvendige viden og kompetence om datasikkerhed kommunikeres til alle medarbejdere, og der arbejdes løbende med holdninger og viden om datasikkerhed.

Ledelsen i den enkelte afdeling og institution er ansvarlig for, at databeskyttelsespolitikken overholdes.

7. Databeskyttelseshåndbog

Databeskyttelsespolitikken danner grundlag for udformning af OK-Fondens ***databeskyttelseshåndbog*** med de underliggende retningslinjer og forretningsgange. Håndbogen inddeles i følgende hovedområder.

7.1 Organisering og ansvar

Beskrivelse af, hvem der har ansvaret for de forskellige databehandlersystemer centralt og lokalt, indgåelse af IT-kontrakter og køb af IT-udstyr, manuelle systemer med persondata og ansvaret for instruktion og undervisning af medarbejderne om databeskyttelse. Endvidere beskrives, hvem der har ansvaret for behandling af henvendelser fra og meddelelser til de registrerede samt ansvaret for behandling og anmeldelse af brud på persondatasikkerheden.

7.2 Retningslinjer for sikkerhed, der især berører medarbejderne

I dette afsnit samles de retningslinjer og regler, der har særlig betydning for medarbejderne, det er for eksempel instruktion og undervisning om databehandlingssikkerhed, adgangsstyring og brugeradministration, login og password form og brug, anvendelse og opbevaring af mails, anvendelse af mobilt udstyr, beskyttelse mod tyveri, anvendelse af privat udstyr, brug af internettet og netværkstjenester, brug af personoplysninger på opslagstavler herunder triagetavler og brug af individuelle håndarkiver og oversigter

7.3 Generelle sikkerhedsbestemmelser
Der fastsættes her regler for anskaffelse og bortskaffelse af IT og kommunikationsudstyr, logning og overvågning, backup, netværkssikkerhed, beskyttelse mod skadevoldende programmer og kode, styring af sikkerhedshændelser, styring af leverandører, databehandlere og underdatabehandlere, krav til databehandleraftaler samt krav til databehandleraftaler, hvor kommuner er dataansvarlige for systemer, der stilles til rådighed samt OK-Fondens forretningsbetingelser som databehandler for private.

7.4 Principper, regler og forretningsgange for behandling af personoplysninger
Der beskrives de regler og retningslinjer, der sikrer, at OK-Fonden er i overensstemmelse med reglerne i Databeskyttelsesforordningen og Databeskyttelsesloven herunder: Principper for behandling af personoplysninger – privatlivspolitik, anvendelse af samtykke, procedurer for den registreredes rettigheder og udarbejdelse af fortegnelser.

8. Risikovurdering og klassifikation af data

8.1 Risikovurdering
OK-Fonden ønsker at være bevidst om enhver risiko, og ud fra en risikovurdering opnå, at et passende *og tilstrækkeligt sikkerhedsniveau etableres både elektronisk og fysisk.*

Ledelsen deltager aktivt i risikovurderingen og er ansvarlige for at vurdere trusler, konsekvenser og risici ved automatisk og manuel databehandling. Det tages op i ledelsen en gang om året, om risikovurderingen skal revurderes, samt ved eventuelle større ændringer i opgaver, leverandører, databehandlingssystemer.

I risikovurderingen og klassificeringsarbejdet kan databehandlersystemer, der er ens eller fælles for en type institutionen behandles sammen, for eksempel systemer, der anvendes af plejehjem eller psykiatriske institutionen med henblik på at gennemført ensartede sikkerhedsretningslinjer og sikkerhedsforanstaltninger.

I de tilfælde, hvor OK-Fonden er ansvarlig databehandler for en kommune lægger OK-Fonden de risikovurderinger, som kommunen har udarbejdet til grund for behandlingen af personoplysninger, der er omfattet af kommunens dataansvar.

8.2 Klassifikation
For at sikre, at systemer og data har det rigtige sikkerhedsniveau, skal disse klassificeres. Data og systemer skal klassificeres efter både tilgængelighed, integritet (pålidelighed), fortrolighed og robusthed.

I de tilfælde, hvor OK-Fonden er databehandler for en kommune, lægger OK-Fonden kommunens klassificeringer til grund for behandlingen af personoplysninger, der er omfattet af kommunens dataansvar.

8.2.1 Tilgængelighed
Målet er, at databehandlingssystemerne har en høj tilgængelighed, således at systemer og data i disse er tilgængelige for autoriserede brugere i et omfang der afspejler behovet for adgang til de oplysninger, der er nødvendige for rettidig administration. Det er endvidere

målet at minimere risikoen for systemnedbrud og at sikre, at der kan ske en rettidig genopretning af tilgængeligheden i tilfælde af en fysisk eller teknisk hændelse.

Tilgængelighed af data og systemer prioriteres indbyrdes i følgende kategorier:

- Høj – tilgængelighed er vigtig for driften og indberetninger til det offentlige (fx SKAT og medicindosering) og kan kun vanskeligt erstattes af manuelle systemer.
- Medium – tilgængelighed er vigtigt, men funktionerne kan udføres manuelt i en begrænset tidsperiode (f.eks. ved adgang til en nødjournal).
- Lav – tilgængelighed er ikke kritisk og funktionerne kan afbrydes i en længere tidsperiode (fx informationer om institutionen på hjemmesiden).

8.2.2 Integritet/Pålidelighed

Målet er at opnå en korrekt og pålidelig funktion i OK-Fondens databehandlingssystemer, hvor oplysningerne er korrekte, pålidelige, nøjagtige og fuldstændige, og hvor der er en minimal risiko for datatab som følge af menneskelige eller systemmæssige fejl, forsøg på uautoriserede ændringer, udefrakommende hændelser og lignende.

Integritet eller pålidelighed/rigtighed af data klassificeres efter følgende kategorier:

- Høj – data danner grundlag for beslutninger vedrørende beboernes behandling og udarbejdelse af handleplaner mv.
- Medium – data danner grundlag for beslutninger, men som ikke er kritiske - f.eks. data med økonomisk overblik
- Lav – data danner aldrig eller kun sjældent grundlag for beslutninger - f.eks. data på intranet omkring kantineforhold m.v.

8.2.3 Fortrolighed

Målet er at sikre en fortrolig behandling, herunder transmission og opbevaring af personoplysninger og andre fortrolige oplysninger, hvor kun autoriserede og korrekt identificerede brugere har adgang, og hvor brugernes adgang er begrænset til det nødvendige. Hensynet til beboernes personlige integritet vejer altid tungt over for hensynet til effektivitet og fleksibilitet i administrationen og sagsbehandlingen.

Fortrolighed af data inddeles i følgende kategorier:

- Fortroligt – Data der kun må være tilgængeligt for en begrænset gruppe af personer, f.eks. personaleoplysninger og oplysninger om beboere og brugere
- Internt brug – Materiale, der er tilgængeligt for alle medarbejdere, fx på medarbejder intranettet i OK-Fonden.
- Uklassificeret – Der er ingen fortrolighed og ingen begrænsninger for hvem, der må få adgang til data. Fx oplysninger på hjemmesider.

Persondata behandles altid fortroligt og videregives eller offentliggøres kun med samtykke fra den registrerede, med mindre videregivelse er obligatorisk ifølge lovgivningen.

8.2.4 Robusthed

Målet er at sikre, at databehandlingssystemernes tekniske og organisatoriske modstandsdygtighed ved at sikre dem mod skadelige hændelser. Der kan f.eks. sikres

imod udfald ved dublerede diske, køling, nødstrømsanlæg, automatisk brandslukning, mv. alt afhængig af, om det er relevant.

Høj robusthed kræves af IT-systemer, hvor det er vigtigt, at data kan bruges i den løbende administration og hvor data skal bevares af hensyn til dokumentation og/eller gennemførelse af behandling af beboere og brugere. Der kræves høj robusthed af OK-Fondens centrale systemer til:

- Løn og personaleadministration
- Økonomiadministration

Der kræves høj robusthed af OK-Fondens lokale systemer i institutioner til:

- Omsorgs- og journalsystemer med beboer og klientoplysninger

Middel robusthed kræves af IT-systemer, hvor data anvendes løbende, men hvor der ikke er krav om at data skal bevares i længere tid til dokumentationsformål, kravene er her især, at systemet er sikret mod udfald. Det drejer sig om:

- Overvågnings- og alarmsystemer til beboere
- Videoovervågning
- Elektroniske nøglesystemer

Lav robusthed gælder IT-systemer, der ikke umiddelbart er knyttet til driften og hvor data kan genskabes relativt nemt. Det drejer sig om:

- Hjemmesider
- Systemer, der indeholder kopi af data, der også ligger i systemer, der har høj robusthed.

9. Efterlevelse af databeskyttelsespolitikken

Alle medarbejdere i OK-Fonden er forpligtet til at efterleve den til enhver tid gældende databeskyttelsespolitik med tilhørende retningslinjer, forretningsgange og relaterede bilag.

Alle medarbejdere modtager ved deres tiltræden af stillingen en kopi af de vigtigste bestemmelser om data- og persondatasikkerhed rettet til medarbejderne og underskriver en erklæring om, at de vil overholde reglerne.

En overtrædelse af databeskyttelsesbestemmelser eller regler for behandling af personoplysninger kan efter omstændighederne – lige som i andre tjenstlige forhold - medføre ansættelsesretlige konsekvenser som påtale, advarsel og i gentagelsestilfælde eller i grove tilfælde afsked.

10. Afvigelser

Hvis der opstår situationer, hvor kravene i Databeskyttelsespolitikken ikke kan efterleves, skal det godkendes af ledelsen og dokumenteres, og der indføres alternative sikringsforanstaltninger.

11. Opfølgning på databeskyttelses- og behandlingsreglerne

OK-Fonden ønsker til stadighed at følge op på databeskyttelses- og behandlingsreglerne, og at opfølgningen skal ske ved anvendelse af fælles metoder i alle OK-Fondens egne og tilknyttede institutioner og enheder.

OK-Fonden vil blandt andet løbende vurdere følgende områder:

- Registrering og opfølgning på hændelser inden for IT-sikkerhed og behandlingsregler
- Behandling af IT-sikkerheds- og behandlingshændelser med henblik på løbende forbedringer og vidensdeling
- Løbende at gennemføre revisioner og evalueringer af IT-sikkerhed og behandlingsregler
- En gang om året at revurdere databeskyttelses- og behandlingsreglerne

Opfølgningen på databeskyttelsesarbejdet sker i en nedsat ***databeskyttelsesgruppe*** hvis opgaver og sammensætning er fastsat af OK-Fondens ledelse. (***Bilag 4)***

Det er OK-Fondens mål, at de løbende risikovurderinger viser en faldende tendens med hensyn til områder med tidligere påvist høj risiko for datasikkerhed og/eller behandling af personoplysninger.

Vedtaget af OK-Fondens direktion den xx.xx.2018.

Underskrifter:

Bilag 1 Oversigt – institutioner, som OK-Fonden har dataansvar for

A) OK-Fonden og fondens afdelinger og egne institutioner

OK-Fonden er som følge af ejerskab og instruktionsbeføjelse dataansvarlig eller ansvarlig databehandler for alle sine afdelinger herunder institutioner, der er P-numre under OK-Fonden. Dette var pr. 25-05-2018 følgende:

OK-Fond P-nr. i CVR	Navn
1000711293	OK-Fonden
1013879016	OK-Hjemmet Arendse
1023185217	OK-Fonden Helenes Minde
1023185195	OK-Fonden Thea
1011375428	Plejecenter Baeshøjgård
1020739556	Dr. Anne-Marie Centret
1020739548	Kong Frederik IX´s Hjem
1023187627	OK-Centret Enghaven
1023122959	Hansted Kloster
1023122940	Ravnebjerg
1023122932	Sct. Jørgens Gård
1023187643	Bostedet Jelling Have
1023122975	Jellinggård
1023122967	Kollegiet
1022792985	Afd. Harresø (Harresø Kro)
1021164913	OK-Huset Horsens (Forening)
1016980214	OK-Huset Horsens
1020682392	Cafe Himmelblå
1015823182	Hospice Søndergård

B) Selvejende institutioner omfattet af bindende virksomhedsregler

Der er indgået aftale med følgende selvejende institutioner om, at de er omfattet af OK-Fondens bindende virksomhedsregler:

CVR nr.	Navn
35921451	Den selvejende institution OK-Centret Betty Sørensen Parken
37433306	Den selvejende institution i Hornbæk (Bøgehøjgård)
28980302	OK-Centret Benedikte
37695432	Den selvejende institution OK-Plejecentret Dreyershus
34520348	OK-Centret Egå
27331882	Plejehjemmet Himmelev Gamle Præstegård
35263071	Den selvejende institution OK-Huset Lotte
58635057	Plejecenter Lystoftebakken
36867027	Den selvejende institution Margretecentret Maribo S/I
43524828	OK-Huset Odense, med 2 selvejende institutioner som P- numre:

- P-nr. 1003075569 Den selvejende institution Gurli-Vibeke
- P-nr. 1019111799 OK-Centret Dyruphus

C) Boligforeninger, omfattet af bindende virksomhedsregler

Der er indgået aftale med følgende boligforeninger om, at de er omfattet af OK-Fondens bindende virksomhedsregler:

CVR nr.	Navn
CVR: 18646730	OK-Fonden Ældreboliger Frederiksberg Alle 16
CVR: 19104435	OK-Fondens Ældreboliger Enghaverne 2 – 12 Kerteminde

D)Aktieselskaber omfattet af bindende virksomhedsregler

Der er indgået aftale med følgende aktieselskaber, der ejer 100 % af OK-Fonden om, at de er
omfattet af OK-Fondens bindende virksomhedsregler:

CVR nr.	Navn
13019614	Plejehjemsgruppen af 1960 A/S
25651111	OK-Kompetenceudvikling A/S
20023570	OK-Servicetjeneste A/S, med følgende P-numre (pr. 27-03-2018):
	P.nr. 1004102120 OK-Servicetjeneste A/S
	P.nr. 1013878540 Køkkenet, OK-Centret Baeshøjgård
	P.nr. 1013878850 Køkkenet, OK-Plejecentret Betty Sørensen
	P-nr. 1016984465 OK-Køkkenet på Gammel Kloster
	P-nr. 1017792101 OK-Service Egå
	P-nr. 1021314540 OK-servicetjeneste FRB
	P-nr. 1019182262 OK-servicetjeneste Lotte

Bilag 2 Aftale om bindende regler

AFTALE
OM
DATAANSVAR OG BINDENDE VIRKSOMHEDSREGLER
MELLEM

OK-Fonden
Lersø Parkalle 112, 2.
2100 København Ø
CVR nr.: 14268235

OG

Den selvejende institution/boligforening/Aktieselskabet
<navn>
<adresse)
CVR nr.: XXXX

A) Bindende regler

Det er mellem OK-Fonden og <NAVN> aftalt, at OK-Fonden varetager ***dataansvaret i henhold til Databeskyttelsesforordningen***[2] for institutionen, således at det er OK-Fonden der afgør, til hvilket formål og med hvilke hjælpemidler der må foretages behandling af personoplysninger i institutionen.

I det omfang ***institutionen er databehandler*** for registreringer om beboerne og brugerne i et kommunalt databehandlingssystem varetager OK-Fonden ansvaret som databehandler over for kommunen og indgår en databehandleraftale med kommunen på institutionens vegne, såfremt dette ikke allerede fuldt ud er sket i driftsoverenskomsten med kommunen.

Institutionen er forpligtet til at følge og overholde de af OK-Fonden fastsatte regler i OK-Fondens databeskyttelsespolitik, databeskyttelseshåndbog samt erklæringer, der underskrives af medarbejderne.

Ved anskaffelse af nye databehandlingssystemer eller indførelse af nye forretningsgange til behandling af personoplysninger skal institutionen have OK-Fondens godkendelse inden kontrakter indgås eller forretningsgange iværksættes.

[2] Forordning EU 2016/679 af 27. april 2016 - Databeskyttelsesforordningen

Reglerne gøres ***bindende for de ansatte*** i institutionen ved at der underskrives et tillæg til ansættelseskontrakten som forpligter medarbejderen til at overholde de af OK-Fonden fastsatte databeskyttelsesregler.

De bindende regler herunder OK-Fondens databeskyttelses- og behandlingsregler underkastes revision af et revisionsfirma en gang årligt. Datatilsynet har adgang til resultaterne af revisionerne.

B) Persondata omfattet af de bindende regler og data-flows

OK-Fondens dataansvar omfatter behandlingen[3] af alle personoplysninger i institutionen, herunder oplysninger om institutionens medarbejdere, beboere, der modtager ydelser i eller fra institutionen, pårørende samt leverandører og kontaktpersoner.

En række databehandlingssystemer er et led i OK-Fondens personale- og økonomiadministration for institutionen samt den interne kommunikation i OK-Fonden, og der udveksles i forbindelse med varetagelse af disse funktioner personoplysninger mellem institutionen og OK-Fonden.

En række databehandlingssystemer anvendes af institutionen til behandling af personoplysninger om beboere, der modtager ydelser i institutionen, brugere, pårørende samt leverandører og kontaktpersoner. Disse oplysninger udveksles ikke med og behandles ikke af OK-Fonden men behandles kun af institutionen selv i databehandlersystemer som institutionen selv har anskaffet og driftet eller som OK-Fonden har anskaffet og stiller til rådighed for institutionen. OK-Fonden har imidlertid adgang til at tilse og kontrollere, at behandlingen af personoplysninger i disse databehandlingssystemer sker i overensstemmelse med reglerne.

C) Tredieparters rettigheder

OK-Fonden hæfter for brud på de bindende regler over for tilsynsmyndigheden og med hensyn til erstatningsansvar over for de registrerede. OK-Fonden har bevisbyrden for, at institutionen og/eller OK-Fonden ikke er ansvarlig for et brud på reglerne.

De bindende regler for OK-Fonden offentliggøres på fondens hjemmeside hvad angår beboere, brugere, pårørende og kontakter, og på institutionens hjemmeside henvises til reglerne. Tilsvarende henvises til reglerne på fondens og institutionens intranet hvad angår medarbejdere.

På samme måde angives på OK-Fondens og institutionens hjemmeside og intranet ***information om de registreredes rettigheder*** og hvordan de kan påberåbe sig dem, herunder oplysninger om hvordan de registrerede kan kontakte den dataansvarliges repræsentant i OK-Fonden og i institutionen.

[3] Jfr. definitionen i forordningens artikel 4 stk.1 nr. 2)

D) Efterlevelse og opdatering

Det fremgår af OK-Fondens databeskyttelses- og behandlingsregler, hvordan medarbejderne, der regelmæssigt eller permanent behandler personoplysninger gennemgår et passende uddannelsesprogram i forhold til de bindende regler.

Institutionen udpeger en ansvarlig, der sammen med OK-Fondens ansvarlige har ansvaret for institutionens behandlingen af personoplysninger og for behandling af klager og henvendelser fra de registrerede.

Den ansvarlige i institutionen er tilknyttet en arbejdsgruppe i OK-Fonden, der med støtte fra OK-Fondens direktion skal sikre reglernes efterlevelse.

OK-Fonden forpligter sig til at rapportere ændringer i OK-Fondens databeskyttelses- og databehandlingsregler til institutionen.

Aftalen er tiltrådt på institutionens bestyrelsesmøde den xx.xx.2018

Den _____

For OK-Fonden

_____

For institutionen

_____

Bilag 3 DPO for selvejende institutioner, der er offentlig forvaltning

OK-Fondens ledelse udpeger en databeskyttelsesrådgiver for de selvejende institutioner, der er en del af den offentlige forvaltning og som er omfattet af de bindende virksomhedsregler. Det drejer sig pr. 25-04-2018 om følgende institutioner:

CVR nr.	Navn
35921451	Den selvejende institution OK-Centret Betty Sørensen Parken
37433306	Den selvejende institution i Hornbæk (Bøgehøjgård)
28980302	OK-Centret Benedikte
37695432	Den selvejende institution OK-Plejecentret Dreyershus
34520348	OK-Centret Egå
35263071	Den selvejende institution OK-Huset Lotte
58635057	Plejecenter Lystoftebakken
36867027	Den selvejende institution Margretecentret Maribo S/I
43524828	OK-Huset Odense, med 2 selvejende institutioner som P- numre:

- P-nr. 1003075569 Den selvejende institution Gurli-Vibeke
- P-nr. 1019111799 OK-Centret Dyruphus

Bilag 4 Databeskyttelsesgruppe opgaver og sammensætning

OK-Fondens ledelse nedsætter en databeskyttelsesgruppe, der med støtte fra OK-Fondens direktion skal medvirke til at sikre databeskyttelsesreglernes efterlevelse, implementering, løbende opdatering, behandling af sikkerhedshændelser og fastlæggelse af retningslinjer for anskaffelse og anvendelse af databehandlingsudstyr.

Databeskyttelsesgruppens sammensætning og opgaver er fastsat i:

- OK-Fondens databeskyttelsesgruppe Dokument OKF-027

Bilag 5 Begreber og definitioner

Begreb	Definition
Fortrolighed	Kun autoriserede personer har ret til at behandle oplysningerne, der kun skal være tilgængelige for autoriserede personer.
Integritet	Det er muligt at validere, om data på systemerne er korrekte, pålidelige, nøjagtige, opdaterede og fuldstændige. Herunder sikring af Backup og eller systemdublering
Tilgængelighed	Det skal være muligt at tilgå systemer og data for autoriserede personer, når dette er nødvendigt.
Robusthed	Behandlingssystemers- og tjenesters tekniske og organisatoriske modstandsdygtighed, der beskytter dem mod skadelige hændelser. Dette kan fx være sikring mod udfald ved dublering, køling, nødstrømsanlæg, brandslukning mv.
Pseudonymisering	Behandling af personoplysninger på en sådan måde, at personoplysningerne ikke længere kan henføres til en bestemt registreret uden brug af supplerende oplysninger, der opbevares separat og sikkert.
Kryptering	En proces, der omdanner de oprindelige oplysninger til oplysninger, der er ulæselig for en trediepart.
Vedvarende	Evnen til at sikre fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og -tjenester er en løbende teknisk og organisatorisk forpligtelse
Databeskyttelsespolitik	Databeskyttelsespolitikken indgår i en dokumentstruktur, hvor politikken er det overordnede dokument, som besluttes af ledelsen, og som udstikker de overordnede krav og målsætninger, som opfyldes igennem specifikke retningslinjer, forretningsgange og instrukser, der findes i ***Databeskyttelseshåndbogen***.
Retningslinjer	I retningslinjerne udfyldes de målsætninger, der er fastlagt i politikken i konkrete beskrivelser af, hvordan sikkerhedspolitikken implementeres. Retningslinjerne fungerer på et overordnet niveau og indeholder ikke tekniske og systemrelaterede beskrivelser.

Begreb	Definition
Forretningsgange og instrukser	Forretningsgange og instrukser udgør specifikke vejledninger til, hvordan retningslinjerne på detaljeret niveau overholdes og implementeres i den enkelte afdeling.
Sikkerhedsforhold	Med sikkerhedsforhold menes alle de forhold, som kan påvirke oplysningers sikkerhed i forhold til fortrolighed, pålidelighed og tilgængelighed.
Sikkerhedshændelser	Begrebet forstås bredt som alle de hændelser, der påvirker databeskyttelsessikkerheden, herunder brud på sikkerheden