

Den selvejende institution

# SOPHIAGÅRD ELMEHØJEN

et hjem for udviklingshæmmede børn, unge og voksne med værksteder og STU

En del af Landsbyfællesskabet Ølsted

.....

## Databeskyttelsespolitik for Sophiagård Elmeøj

### Overordnet organisering af personoplysninger

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

Sophiagård Elmeøj ønsker endvidere i videst muligt omfang at organisere opbevaringen af personoplysninger i bestemte centrale systemer, så personoplysninger om de enkelte personer ikke findes fordelt på flere systemer og både i elektronisk og manuel form.

#### - Formål

Databeskyttelsespolitikken beskriver det **ledelsesgodkendte niveau** for sikkerhed på Sophiagård Elmeøj og indeholder de overordnede sikkerhedsmålsætninger og danner grundlag for udformning af Sophiagård Elmeøjs **datasikkerhedshåndbog** med de underliggende retningslinjer og forretningsgange.

De retningslinjer, der udformes for at understøtte databeskyttelsespolitikens hovedmålsætninger, skal sikre, at alle medarbejdere arbejder med og forholder sig til sikkerhed i behandlingen af personoplysninger i det daglige arbejde.

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

Datasikkerhed er derfor en **nøgleværdi**, og den er en naturlig del af Sophiagård Elmeøjs automatiske og manuelle databehandling af oplysninger, herunder især personoplysninger.

#### - Omfang

Databeskyttelsespolitikken er gældende for alle **medarbejdere**.

Alle **leverandører og samarbejdspartnere**, som har fysisk eller logisk adgang til Sophiagård Elmeøjs systemer, data og oplysninger skal gøres bekendt med politikken og forpligte sig til at følge den.

Databeskyttelsespolitikken dækker alle tekniske og administrative forhold, der har direkte eller indirekte indflydelse på drift og brug af Sophiagård Elmeøjs automatiske databehandlingsystemer samt manuelle arkiver og registre.

#### - Hovedmålsætninger og sikkerhedsniveau

Sophiagård Elmeøj har følgende sikkerhedsmålsætning:

**"Sophiagård Elmeøj har et passende og tilstrækkeligt teknisk og organisatorisk sikkerhedsniveau, der gælder for alle ansatte, leverandører og samarbejdspartnere ved behandling af personoplysninger og andre data ved hel eller delvis anvendelsen af automatisk databehandling, samt for behandling af manuelle dokumenter."**

Et passende og tilstrækkeligt databeskyttelsesniveau<sup>1</sup> opnås igennem tekniske og organisatoriske foranstaltninger, der sikrer:

<sup>1</sup> Som beskrevet i Databeskyttelsesforordningen artikel 32

.....

Den selvejende institution

# SOPHIAGÅRD ELMEHØJEN

et hjem for udviklingshæmmede børn, unge og voksne med værksteder og STU

En del af Landsbyfællesskabet Ølsted

.....

- **vedvarende fortrolighed, integritet, tilgængelighed og robusthed** af Sophiagård Elmeøjens behandlingssystemer og behandlingstjenester i forhold til den risikovurdering, der er gennemført for de enkelte systemer og data.
- anvendelse af **pseudonymisering og kryptering**, hvor det er relevant, herunder ved dataudveksling med databehandlere, 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 Sophiagård Elmeøjens it-aktiver, oplysninger og data i Sophiagård Elmeøjens varetægt.

Et tilstrækkeligt sikkerhedsniveau **fastholdes** ved

- at der **vedvarende** forefindes **retningslinjer og forretningsgange**, som sikrer, at datasikkerheden er en integreret del af Sophiagård Elmeøjens drift og daglige arbejde.  
Målet er at sikre 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 Sophiagård Elmeøjens 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**).
- **Sophiagård Elmeøjen** følger op på datasikkerheden igennem løbende vedligeholdelse og optimering af databeskyttelsespolitikken og de dertilhørende retningslinjer og forretningsgange.

## - Organisation og ansvar

Sikkerhedsmålsætning:

**"Alle medarbejdere har ansvar for datasikkerheden. De er bekendte med og efterlever Sophiagård Elmeøjens databeskyttelsespolitik, retningslinjer og forretningsgange, der er beskrevet i sikkerhedshåndbogen."**

Planlægning, implementering og kontrol af datasikkerheden er defineret af **Sophiagård Elmeøjens** ledelse, der også er ansvarlig for implementering og vedligeholdelse af databeskyttelsessikkerhedssystemet og er ansvarlig for opfølgning på sikkerhedshændelser.

Sophiagård Elmeøjens ledelse fastsætter i databeskyttelseshåndbogen I-4 **hvem der har ansvaret** for hver af institutionens, **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**, opsamling og styring af **anmeldelse af brud på persondatasikkerheden** til Datatilsynet og 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 ledelsen.

.....

Ølstedgårdsvej 7+9 Ølsted, 5672 Broby, Telefon 6269 2200 Mail: [kontor@sophiagaard.dk](mailto:kontor@sophiagaard.dk),

[www.lf-ølsted.dk](http://www.lf-ølsted.dk). Facebook: Sophiagård Elmeøjen CVR.nr. 2078 3397.

Den selvejende institution

# SOPHIAGÅRD ELMEHØJEN

et hjem for udviklingshæmmede børn, unge og voksne med værksteder og STU

En del af Landsbyfællesskabet Ølsted

.....

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

Ledelsen er ansvarlig for, at databeskyttelsespolitikken overholdes.

## - Databeskyttelseshåndbogen

Databeskyttelsespolitikken uddybes af ledelsen i retningslinjer og forretningsgange. Tilsammen udgør politikken, retningslinjer, beredskabspolitik og forretningsgange Databeskyttelseshåndbogen, der inddeles i følgende hovedområder:

- Retningslinjer for **medarbejdernes håndtering af sikkerhed**.
  - Fokus på, at personoplysninger altid behandles fortroligt
  - Regler for login og password
  - Regler for anvendelse af mobilt udstyr, PC'er, USB-nøgler, mobiltelefoner mv.
  - Regler for anvendelse af private PC'er til behandling af personoplysninger vedrørende beboere og medarbejdere
  - Regler for anvendelse af internettet
  - Regler for anvendelse af mails, herunder sikker mail, og privat anvendelse af institutionens mail
  - Regler for eller forbud mod download af IT-programmer, spil, billeder mv.
- Retningslinjer for **adgangsstyring**
- Retningslinjer for behandling af **data på mobile enheder**
- Retningslinjer for anvendelse af **sikker mail** ved kommunikation med pårørende til beboere og brugere, kommuner og andre offentlige myndigheder
- Retningslinjer for **netværksstyring**, herunder trådløse netværk
- Retningslinjer for **styring af sikkerhedshændelser**, herunder
  - 7) Anmeldelse af brud på persondatasikkerheden til Datatilsynet og de registrerede, herunder procedurer, kontakt til databehandler og indhold i anmeldelsen
  - 8) Forretningsgange for behandling, reetablering og rettelser af data
- Principper og forretningsgange for **behandling af personoplysninger** som beskrevet nedenfor i afsnit 6
- Retningslinjer for **styring af leverandører og data-behandlere**
  1. Databehandleraftaler
  2. Databehandlerens sikkerhedsniveau og håndtering af sikkerhed

## - Principper og forretningsgange for behandling af personoplysninger

Ledelsen fastsætter principper og forretningsgange for Sophiagård Elmeøjens 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 dataportabilitet
- **Fortegnelser udarbejdet over behandlingsaktiviteter** med personoplysninger

.....

Ølstedgårdsvej 7+9 Ølsted, 5672 Broby, Telefon 6269 2200 Mail: [kontor@sophiagaard.dk](mailto:kontor@sophiagaard.dk),

[www.lf-ølsted.dk](http://www.lf-ølsted.dk). Facebook: Sophiagård Elmeøjens CVR.nr. 2078 3397.

# SOPHIAGÅRD ELMEHØJEN

et hjem for udviklingshæmmede børn, unge og voksne med værksteder og STU

En del af Landsbyfællesskabet Ølsted

.....

## - Risikovurdering og klassifikation af data

### 7.1 Risikovurdering

Sophiagård Elmeøjen ønsker at være bevidst om enhver risiko, og ud fra en risikovurdering opnå et passende og tilstrækkeligt sikkerhedsniveau etableret 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.

### 7.2 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) og fortrolighed.

#### ▪ Tilgængelighed

I tilgængelighedskriteriet ligger, at det skal være muligt at tilgå systemer og data for autoriserede personer, når dette er nødvendigt.

Det er for Sophiagård Elmeøjen især vigtigt med høj tilgængelighed til data og IT-systemer, der indeholder oplysninger, der anvendes i forbindelse med:

- behandlingen af institutionens beboere og brugere
- medicinadministration
- personaleadministration, herunder lønudbetaling og indberetninger til myndigheder

Tilgængeligheden sikres først og fremmest igennem bestemmelser i de IT-kontrakter og/eller databehandlertaftaler, der indgås med leverandørerne.

#### ▪ Integritet/pålidelighed

I integritet/pålidelighed ligger, om data på systemerne er korrekte, pålidelige, nøjagtige, opdaterede og fuldstændige.

Det er for Sophiagård Elmeøjen især vigtigt med høj integritet/pålidelighed i data og IT-systemer, der indeholder oplysninger, der anvendes i forbindelse med:

- beslutninger vedrørende beboernes/brugernes behandling og udarbejdelse af handleplaner mv.
- medicinadministration
- personaleadministration

Integritet/pålidelighed sikres først og fremmest gennem den kvalitetskontrol, der finder sted under de fastlagte forretningsgange for behandling af sagerne.

### 7.2.3 Fortrolighed

Med **fortrolighed** menes der, at kun autoriserede personer har ret til at tilgå oplysningerne, og oplysningerne skal kun være tilgængelige for autoriserede personer.

Personoplysninger behandles altid fortroligt og videregives eller offentliggøres kun med samtykke fra den registrerede, med mindre videregivelse har hjemmel i lovgivningen.

I Databeskyttelseshåndbogen angives hvilke personer, der har adgang til henholdsvis beboernes/brugernes og medarbejdernes oplysninger.

.....

Den selvejende institution

# SOPHIAGÅRD ELMEHØJEN

et hjem for udviklingshæmmede børn, unge og voksne med værksteder og STU

En del af Landsbyfællesskabet Ølsted

.....

## - **Overtrædelse af databeskyttelsespolitikken**

Alle medarbejdere på Sophiagård Elmeøjen er forpligtet til at efterleve den til enhver tid gældende datasikkerhedspolitik med tilhørende retningslinjer, forretningsgange og relaterede bilag.

Alle medarbejdere modtager ved deres tiltræden en kopi af de vigtigste bestemmelser om data- og persondatasikkerhed rettet til medarbejderne.

## - **Afvielser**

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

## - **Udarbejdelse og ikrafttrædelse**

Ændringer i sikkerhedsdokumentationen forelægges og godkendes af ledelsen.

Databeskyttelsespolitikken er godkendt den **31.10.2018**.

.....

Ølstedgårdsvej 7+9 Ølsted, 5672 Broby, Telefon 6269 2200 Mail: [kontor@sophiagaard.dk](mailto:kontor@sophiagaard.dk),

[www.lf-ølsted.dk](http://www.lf-ølsted.dk). Facebook: Sophiagård Elmeøjen CVR.nr. 2078 3397.

## Bilag 1: Begreber og definitioner

Begreb	Definition
<b>Fortrolighed</b>	Kun autoriserede personer har ret til at behandle oplysningerne, der kun skal være tilgængelige for autoriserede personer.
<b>Integritet</b>	Det er muligt at validere, om data på systemerne er korrekte, pålidelige, nøjagtige, opdaterede og fuldstændige. Herunder sikring af Backup og eller systemdublering
<b>Tilgængelighed</b>	Det skal være muligt at tilgå systemer og data for autoriserede personer, når dette er nødvendigt.
<b>Robusthed</b>	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.
<b>Pseudonymisering</b>	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.
<b>Kryptering</b>	En proces, der omdanner de oprindelige oplysninger til oplysninger, der er ulæselig for en trediepart.
<b>Vedvarende</b>	Evnen til at sikre fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og -tjenester er en løbende teknisk og organisatorisk forpligtelse.
<b>Databeskyttelsespolitik</b>	Databeskyttelsespolitikken indgår i en dokumentstruktur, hvor politikken er det overordnede dokument, som besluttet af ledelsen, og som udstikker de overordnede krav og målsætninger, som opfyldes igennem specifikke retningslinjer, forretningsgange og instrukser, der findes i Databeskyttelsehåndbogen.
<b>Retningslinjer</b>	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.
<b>Forretningsgange og instrukser</b>	Forretningsgange og instrukser udgør specifikke vejledninger til, hvordan retningslinjerne på detaljeret niveau overholdes og implementeres i den enkelte afdeling.
<b>Sikkerhedsforhold</b>	Med sikkerhedsforhold menes alle de forhold, som kan påvirke oplysningers sikkerhed i forhold til fortrolighed, pålidelighed og tilgængelighed.
<b>Sikkerhedshændelser</b>	Begrebet forstås bredt som alle de hændelser, der påvirker databeskyttelsessikkerheden, herunder brud på sikkerheden.