|  |
| --- |
| **Interne retningslinjer for databeskyttelse og personalets håndtering af personoplysninger** |
| Udarbejdet af:   |  | Godkendt af ledergruppen:   |  |
| Revideret:   |  | Godkendt af MED:   |  |

**INDLEDNING**

Følgende retningslinjer skal være med til at sikre, en ensartet håndtering af de personoplysninger vi hver dag behandler om borgere, medarbejdere og andre, samt at personoplysninger tilstrækkeligt beskyttet.

Alle medarbejdere har ansvaret for, at retningslinjer overholdes. Hvis der er udpeget en ansvarlig for enkeltområder, fremgår det pr. punkt. Spørgsmål til retningslinjerne skal rettes til **[Leder/Forstander]**.

Retningslinjer gennemgås mindst en gang årligt, for at sikre, at de er opdateret, og at de passer til den aktuelle situation hos os.

Medarbejdere skal læse PIXI for medarbejdere, med henblik på at opnå en grundviden på området.

Pixi og øvrigt omtalt materiale findes **[anfør hvor henne]**

**Overordnet GDPR-ansvarlig er:**

**HÅNDTERING AF PERSONOPLSYNINGER** Ansvarlig:

**Generelle retningslinjer**

Personoplysninger indsamles kun, hvis de er nødvendige for opgaveløsningen. Det vil sige, at vi beder ikke om oplysninger, som vi ikke har konkret brug for.

Personoplysninger bruges kun til de opgaver, der udføres indenfor vores ansvarsområde. Det vil sige, at vi kun anvender oplysninger i forbindelse med de opgaveområder, vi er forpligtiget til at løse.

Personoplysninger må ikke deles med uvedkommende. Det vil sige, at oplysninger om en given borger må ikke gives videre til uvedkommende eller kunne overhøres af uvedkommende.

Personoplysninger skal være korrekte. Det vil sige, at vi altid skal sørge for, at oplysningerne er opdateret, så de er korrekte.

Personoplysninger skal opbevares, hvis det er nødvendigt, eller hvis det er et krav. Det vil sige, at oplysninger, der ikke skal bruges igen, skal slettes med det samme. Oplysninger, der skal anvendes til en efterfølgende opgaveløsning, eller hvor der er et krav til dokumentation fx et sagsforløb, skal gemmes (opbevares).

Personoplysninger skal opbevares forsvarligt – ift. typen af personoplysninger. Det vil sige, at oplysninger i systemer, i elektroniske filer, fysiske dokumenter, løse papirnoter mv. skal opbevares, så de ikke vil være tilgængelige for personer/medarbejdere som oplysninger ikke vedkommer. Desuden skal særligt adgangen til følsomme oplysninger være beskyttet af adgangskoder, nøgler etc.

**Specifikke retningslinjer**

Hovedparten af personoplysninger, som anvendes i det faglige / daglige arbejde, registreres/opbevares i de tilgængelige fagsystemer.

Papirdokumenter / Word filer og tilsvarende vedr. specifik borger skal så vidt muligt scannes og lægges i e-doc og/eller fagsystem med det samme. Papirdokumenter / Word filer og tilsvarende skal derefter slettes.

Følgende dokumenter med personoplysninger håndteres elektronisk:

* Nyeste billeder af beboere / medarbejder opbevares lokalt på PC – overføres fra kamera / telefoner med det samme.
* Gamle billeder fra tidligere års aktiviteter opbevares på ekstern harddisk som befinder sig her \_\_\_\_\_\_\_\_.
* Daglige driftslister (telefonlister, beboeroversigter, personaleoversigter, medicinlister mv.) opbevares lokalt på PC på kontoret.

Følgende dokumenter med personoplysninger håndteres som fysiske dokumenter:

* Telefonliste, medarbejderoversigt, mødeoversigt [**\_\_\_\_\_, \_\_\_\_\_ og \_\_\_\_\_]** opbevares på opslagstavle på kontor.
* Beboeroversigter, medicinlister, allergilister, kostlister **[\_\_\_\_\_, \_\_\_\_\_]** opbevaresher: **\_\_\_\_\_\_\_\_\_\_.**
* Journaler og dokumenter med fortrolige og følsomme oplysninger opbevares i aflåst skabe på **[Leder/Forstander]** kontor
* Særligedokumenter med fortrolige og følsomme oplysninger opbevares her: **\_\_\_\_\_\_\_\_\_\_.**

**SLETTEREGLER**

**Generelle retningslinjer**

Personoplysninger skal slettes, når de har overskredet grænsen for opbevaring. Det vil sige, at oplysningerne skal slettes, når der ikke er noget formål med eller krav til at opbevare oplysningerne mere.

Slettefrister skal overholdes uanset opbevaringsform. Det vil sige, at sletning skal finde sted, uanset om oplysningerne er placeret i it-systemer, i filer/sager i fagsystemer, i mails, i journaliserede dokumenter, på USB-stik, eksterne disks, mobiltelefoner, fotoapparater og tilsvarende mobile enheder, fysiske dokumenter i aflåste arkivskabe etc.

Fastsatte slettefrister, det vil sige tidspunkt for hvornår slettefrist indtræffer og praktisk sletning mv., fremgår sidst i dette dokument, sammen med oplysninger om hvem der er ansvarlig.

**KOMMUNIKATION MED BORGER** Ansvarlig:

**Generelle retningslinjer**

Kommunikationen skal ske sikkert, særligt når kommunikationen indeholder fortrolige eller følsomme personoplysninger.

Mundtlig kommunikation skal ske under hensyn til indholdet af kommunikationen, og så fortrolige eller følsomme oplysninger ikke kommer til uvedkommendes kendskab. Ansvarlig for sikker mundtlig kommunikation er alle medarbejdere.

Skriftlig kommunikation med fortrolige eller følsomme personoplysninger skal sendes krypteret ved hjælp af ”Send sikkert” funktionen på e-mail, eller sendes som digital post.

Forældre, borgere, pårørende eller andre kan ikke give tilladelse til, at der sendes fortrolige eller følsomme oplysninger fx via usikker mail.

**Specifikke retningslinjer**

[Fagsystemer eller lign] skal anvendes til at sende generelle meddelelser til forældre/borgere, der ikke indeholder fortrolige eller følsomme personoplysninger.

E-mail modtager skal kontrolleres, inden mail afsendes, for at sikre, at modtager er korrekt. Sendes til en forkert modtager, anmeldes dette som persondatabrud til ansvarlige.

SMS må kun anvendes som kommunikation med forældre/borgere mv, hvis det er at modtage og kvittere for sygemelding eller lign. korte beskeder fra forældre/borgere.

Chat-funktioner på Facebook, Twitter, Hjemmesider eller lign., må ikke anvendes til at kommunikere med forældre/borgere/pårørende eller andre.

**OPLYSNINGSPLIGT - som en del af registreredes rettigheder** Ansvarlig:

**Generelle retningslinjer**

Vi har en oplysningspligt overfor borgere, medarbejdere mv. (registrerede). Det vil sige, at de pågældende skal oplyses om, hvilke personoplysninger vi behandler om dem, og på hvilket grundlag vi gøre dette. Derfor skal de pågældende modtage et skriftlig overblik herover samt løbende kunne genfinde informationerne.

**Specifikke retningslinjer**

Beboere og evt. pårørende skal modtage og får udleveret ”privatlivspolitik for borgere og pårørende”, når de ankommer til institutionen første gang. I samme forbindelse skal de oplyses om, at privatlivspolitik kan genfindes på institutionens hjemmeside (**link**).

Medarbejdere – uanset ansættelsestype, skal modtage / have udleveret ”privatlivspolitik for medarbejdere” på ansættelsestidspunktet. I samme forbindelse skal de oplyses om, at privatlivspolitik kan genfindes på hjemmeside (**link**).

**Alle medarbejdere er ansvarlige for henvisning til privatlivspolitik**

Medarbejdere henviser til privatlivspolitikken, hvis en registreret stiller spørgsmål om behandling af personoplysninger.

**HENVENDELSER - fra borgere eller pårørende** Ansvarlig:

**Generelle retningslinjer**

Vi har en pligt til at besvare henvendelser fra borgere, medarbejdere mv.(registrerede). Det vil sige, at registrerede kan bede om forskellige type af informationer, om de personoplysninger vi indsamler og behandler om vedkommende, hvorfor vi gør det osv. (Kaldes registreredes rettigheder)

Alle henvendelse skal besvares uden ugrundet ophold og senest efter 30 dage. Der kan søges hjælp fra DPO.

**Specifikke retningslinjer**

Hvis en registreret, henvender sig til personalet, og beder om at få indsigt i de personoplysninger, som vi behandler om vedkommende, sørger modtager af henvendelsen for at give henvendelsen videre til ansvarlig for besvarelsen.

Hvis en registreret beder om at få rettet eller slettet deres oplysninger, vil gøre indsigelse mod vores behandling af personoplysninger om vedkommende eller vil tilbagekalde et samtykke, sørger modtager af henvendelsen for at give henvendelsen videre til ansvarlig for besvarelsen.

Modtager af henvendelser skal notere sig borgerens kontaktoplysninger, tidspunkt for henvendelsen og informere tidspunktet videre til ansvarlig for besvarelsen.

**SAMTYKKE TIL BEHANDLING AF PERSONOPLYSNINGER** Ansvarlig:

**Generelle retningslinjer**

På visse områder har vi en pligt til at indhente samtykke fra den registrerede, inden vi indsamler og anvender personoplysningerne.

Ansvarlig for retmæssig behandling af personoplysninger på grundlag af samtykke er alle medarbejdere.

Det kan være på områder hvor samtykke:

* *er gældende for en periode* fx ved anvendelse / deling af billeder af beboere/borgere på sociale medier, anvendelse / deling af billeder personale fx på hjemmeside i den tid borgeren er i vores institution.
* *er gældende for en situation* fx ved ansættelse hvor vi vil indhente referencer eller ved indhentelse af attester fx straffeattester
* *er gældende i en akut, konkret situation* - Fx til umiddelbar/akut behandling og videregivelse af sundhedsoplysninger ved en ulykke. Samtykke indhentes mundtligt og dokumenteres efterfølgende i **CSC Social** (hvilket normalt kaldes ”informeret samtykke”).

Vi anvender DPO’s skabeloner for samtykke.

Samtykke skal være frivilligt, skal kunne dokumenteres, og skal til en hver tid kunne trækkes tilbage.

Personoplysninger må kun behandles, når samtykke **er** givet.

**Specifikke retningslinjer**

Samtykke manuelt

Følgende samtykker håndteres manuelt ved udlevering og underskrift af en samtykkeerklæring:

* Ansættelse hvor der indhentes referencer (gældende for en situation)
* **\_\_\_\_\_\_\_\_\_\_.** (gældende for en periode)
* **\_\_\_\_\_\_\_\_\_\_.** (gældende for en situation)

Overblik over hvem der har givet hvilke samtykker findes her: **\_\_\_\_\_\_\_\_\_\_.**

Når borger møder hos os første gang, beder vi dem om at tage stilling til valgfrie behandlinger af personoplysninger, ved at læse og underskrive ovennævnte samtykkeerklæringer.

**Samtykker opbevares i mappe på \_\_\_\_\_\_\_\_\_\_\_\_ i [aflåst skab / scannes og gennem på PC].**

For alle samtykker gælder:

Informationen om, hvem der har givet hvilke samtykker, udmeldes til relevante medarbejdere.

Trækkes et samtykke tilbage registreres dette og informationen udmeldes med det samme og behandlingen af personoplysninger stoppes med det samme. Det gælder også samtykke til at tage og anvende billeder.

Hvis behandling af personoplysninger, der er baseret på samtykke, behandles af tredjeparter (fx leverandører, kommunen mv.) skal de også modtage information om, at samtykke er trukket tilbage og at behandlingen skal stoppes.

**HÅNDTERING AF BILLEDER** Ansvarlig:

**Generelle retningslinjer**

Hvis billeder (inkl. video) tages, opbevares eller formidles, anses dette som en behandling af personoplysninger.

Billeder (inkl. video), som omhandler situationer og personer, som kan henføres til vores arbejde, kan som udgangspunkt behandles jf. det lovgrundlag, som vi i øvrigt har til at behandle personoplysninger. Der må ikke tages flere billeder end nødvendigt.

*Uanset billedets (inkl. video) situation eller person i forhold til myndighedsopgaven må personen / personerne ikke føle sig udstillet / krænket, hvis billedet anvendes. Hvis der er den mindste mulighed for, at nogen vil føle sig krænket, må billedet (inkl. video) ikke anvendes, og skal omgående slettes.*

En borger/medarbejder kan altid afvise, at der må tages billeder af vedkommende, uanset typen af billeder. Dette skal i så fald efterleves.

**Specifikke retningslinjer**

Der skal indhentes samtykke (for en periode eller situation) til anvendelse billeder (inkl. video), hvis formålet er til offentligt brug*.* Det vil sige i tilfælde, hvor billeder deles med andre udenforstående fx via Facebook, hjemmesider, avisartikler, til skriftlige materialer til bred publicering udenfor institutionen og lign.

Mht. praktisk håndtering af samtykke henvises til afsnit herover.

Offentliggjorte billeder på fx Facebook, Instagram, hjemmesider mv. må bibeholdes, så længe samtykke forefindes, og så længe borger / medarbejder er tilknyttet institutionen.

Trækkes et samtykke tilbage, skal offentliggjorte billeder slettes. Alternativt skal de sløres, hvis dette er muligt. Hvis billeder findes i trykte medier, er der ikke krav om sletning.

Billeder i billedarkiver, på telefoner, kamera, tablets mv. skal slette jf. sletteregler herunder, så vi har et minimum af billeder, der skal administreres.

**BRUG AF COMPUTER, TABLETS, TELEFONER, KAMERA**

**Generelle retningslinjer**

Institutionens enheder og brug

Institutionen enheder fremgår af oversigt, der findes på: **\_\_\_\_\_\_\_\_\_\_.**

Oversigten viser hvad enheden anvendes til, hvem der må anvende enheden samt hvilken type indhold den må omfatte. Personalet skal overholde disse anvisninger.

I øvrigt gælder:

* Enheder skal låses, når de ikke anvendes / forlades. Skærmlås med kode og en pinkode skal være aktiveret med kort interval, så enheden ikke kan misbruges, hvis den mistes.
* Mobile enheder skal opbevares sikkert, når disse ikke er i brug. Derfor skal de placeres **[i aflåst skab på kontoret].**
* Computere og tablets må ikke anvendes til opbevaring af filer / dokumenter med personoplysninger, medmindre det fremgår af afsnit om håndtering af personoplysninger.
* Billeder (inkl. video) skal tages med institutionen telefoner/kameraer mv.
* Midlertidig opbevaring af personoplysninger kan ske på computer og tablets, hvis disse er sikret med behørig adgangskode og automatisk nedlukning/skærmlås.
* USB-stik eller harddisk kan med godkendelse fra **[Leder/Forstander]** anvendes til midlertidig opbevaring af filer / dokumenter med personoplysninger, og kun hvis disse er krypteret. Filer / dokumenterne skal slettes, straks efter de er overført efter midlertidig opbevaring.
* Medarbejdere har et medansvar for, at der bliver ryddet op på de forskellige enheder, så der ikke bliver opbevaret personoplysninger steder, hvor det ikke er tiltænkt.
* Hvis man har en mobil enhed med på tur, skal den være under opsyn hele tiden.
* Bliver en mobil enhed tabt eller stjålet, skal **[Leder/Forstander]** straks underrettes.
* Det er ikke tilladt at installere programmer og andet på computere, telefoner og tablets uden godkendelse fra **[Leder/Forstander].**

Private enheder / privat brug

* Der må ikke anvendes private enheder til at tilgå kommunens systemer og dermed personoplysninger om, borgere eller andre.
* Privat telefon, privat kamera eller andre private enheder må ikke anvendes til at tage billeder af beboerne eller andre.
* Der må ikke anvendes private USB-stik eller harddiske.
* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ [Her kan indsættes andre regler for brug af private enheder under arbejde]

**Specifikke retningslinjer**

Oversigt over enheder gennemgås min. 2 gange årligt, for at sikre at den er svarende, til det faktiske antal af enheder, som institutionen råder over.

Oversigt over enheder gennemgås min. 2 gange årligt, for at sikre at der ikke findes dokumenter eller filer, der skal opbevares andre steder eller slettes.

**BRUG AF SYSTEMER OG TJENESTER** Ansvarlig:

**Generelle retningslinjer**

Vi anvender **CSC Social** til at håndtere personoplysninger om **[børn, forældre, borgere]** mv.

Vi anvender **[Andet system]** til at håndtere personoplysninger om medarbejdere.

Medarbejdersagsmapper opbevares elektronisk i **\_\_\_\_\_\_\_\_\_\_.**

Alle medarbejdere får et personligt brugernavn og kodeord til vores systemer, når de bliver ansat. Kodeord er personligt, og må ikke deles med andre.

Kodeord skal skiftes minimum hver ½ år. Ansvarlig alle medarbejdere.

**BRUG AF E-MAIL** Ansvarlig:

**Generelle retningslinjer**

**KK-mail [eller anden arbejdsmail]** må som udgangspunkt kun anvendes til arbejdsrelaterede formål. Hvis det ikke generer den arbejdsrelaterede anvendelse, må den personlige arbejdsmail godt anvendes til private formål.

Medarbejdere skal markere private e-mails med teksten ”privat” i emnefeltet eller gemme private e-mails i en folder, hvor teksten ”privat” indgår i folderens navn.

Det er ikke tilladt at sætte en regel op, der automatisk videresender medarbejderens e-mail til en privat ekstern e-mailadresser.

**FYSISK SIKKERHED, ADGANG TIL LOKALER MV.** Ansvarlig:

**Generelle retningslinjer**

Institutionen har åben adgang til en del lokaler, derfor skal medarbejdere løbende sikre, at dokumenter, lister og andet med personoplysninger håndteres forsvarligt i forhold til typen af oplysninger. Det vil bla. sige:

* Lister og dokumenter skal så vidt muligt skærmes, så de ikke kommer til uvedkommendes kendskab.
* Kontorer/skabe skal låses, når de ikke benyttes.
* Skriveborde skal være ryddet for personoplysninger
* Gæster skal ikke have adgang til kontorer uden opsyn.
* Døre og vinduer lukket når institutionen forlades. Sidste person lukker og slukker.

**Specifikke retningslinjer**

Kun medarbejdere med et arbejdsrelateret formål, må tilgå personalemapper.

Personalemapper opbevares i **[aflåst skab]** og telefonlister over medarbejdere hænger **[på leders kontor]**.

**UDDANNELSE AF MEDARBEJDERE**  Ansvarlig:

**Generelle retningslinjer**

Nye medarbejdere skal inden for den første måned efter ansættelse, have gennemlæst ”PIXI for medarbejdere” og modtage introduktion til interne retningslinjer.

Medarbejdere skal entydigt vide, hvem de skal kontakte, i tilfælde af at de har spørgsmål vedr. behandling af personoplysninger, beskyttelse af personoplysninger eller registreredes rettigheder.

Alle medarbejdere skal løbende gennemgå uddannelse med henblik på at vedligeholde kendskab til reglerne om behandling af personoplysninger. Uddannelse skal gennemføres min hvert 2. år for alle medarbejdere.

**HÅNDTERING AF PERSONDATABRUD** Ansvarlig:

**Generelle retningslinjer**

Persondatabrud skal håndteres med det samme, når det opdages, så bruddet omgående stoppes, og den lovpligtig tidsfrist for anmeldelse til Datatilsynet på 72 timer kan overholdes

**Kontaktperson for persondatabrud er \_\_\_\_\_\_\_\_\_\_.**

**Specifikke retningslinjer**

Hvis en medarbejder bliver bekendt med, eller mistænker at, der er sket et persondatabrud, skal vedkommende med det samme kontakte kontaktpersonen. Ansvarlig alle medarbejdere

DPO for selvejende institutioner informeres med det samme. DPO rådgiver om anmeldelse, stop af bruddet samt evt. orientering af de berørte personer. Ansvarlig er kontaktperson.

Persondatabruddet håndteres i øvrigt som det fremgår af konkret proces for håndtering af persondatabrud – som fremgår i Håndbog eller på vores hjemmeside. Ansvarlig er kontaktperson.

Der udarbejdes et notat om baggrund og handlinger på hvert potentielt eller konstateret persondatabrud, uanset om det er anmeldt til Datatilsynet – DPO’s skabelon herfor kan anvendes. Ansvarlig er kontaktperson

**SLETTEREGLER**

På følgende områder slettes personoplysninger af den selvejende institution jf. angivet frist og frekvens:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Procesområde** | **Slettefrist** | **Sletning skal ske** | **Type af oplysninger** | **Slettemetode** | **Ansvarlig** |
| Alm | For. | Føl. |
| Pladsadministration og daglig drift | \_\_ år efter sagen er afsluttet | Hvert år – måned: **\_\_\_\_** | x | x | x | Makulering af papirer | Forstander |
| Manuelt fra lokal enhed |
| Daglig drift (økonomi) | 5 år efter regnskabsårets afslutning | Hvert år – måned: **\_\_\_\_** | x | x | x | Manuelt fra lokal enhed | Leder |
| Samtykke | \_\_ år efter sagen er afsluttet | Hvert år – måned: **\_\_\_\_** | x | x | x | Makulering af papirer | Forstander |
| Magtanvendelse | \_\_ år efter sagen er afsluttet | Hvert år – måned: **\_\_\_\_** | x | x | x | Manuelt fra lokal enhed | Forstander |
| Utilsigtede hændelse | \_\_ år efter sagen er afsluttet | Hvert år – måned: **\_\_\_\_** | x | x | x | Manuelt fra lokal enhed | Forstander |
| Personale – Ansøgninger | 6 måneder efter ansættelse | Hvert ½ år. | x | x |  | Makulering af papirer | Forstander |
| Manuelt fra lokal enhed |
| Administration -Arbejdsmiljø | 5 år efter at sagen er afsluttet | Hvert år – måned: **\_\_\_\_** | x | x | x | Manuelt fra lokal enhed | Forstander |
| Administration Klagesag | 5 år efter endt sagsbehandling | Hvert år – måned: **\_\_\_\_** | x | x | x | Makulering af papirer | Adm. Medarb. |
| Manuelt fra lokal enhed |
| Administration – Indsigtsanmodning | 5 år efter endt sagsbehandling | Hvert år – måned: **\_\_\_\_** | x | x | x | Makulering af papirer | Adm. Medarb. |
| Manuelt fra lokal enhed |
| Tilsyn – STPS, revision osv. | 5 år efter at sagen er afsluttet | Hvert år – måned: **\_\_\_\_** | x | x | x | Manuelt fra lokal enhed | Adm. Medarb. |
| Billeder / video – sociale medier | Må max være 6 mdl. gamle | Hvert ½ år. | x |  |  | Makulering af papirer | Alle m. adgang |
| Manuelt fra lokal enhed |
| System (Angiv) |
| Mails / møde invitationer + papirkurv | Må max være 6 mdl. gamle | Hvert ½ år | x | x | x | Manuelt fra lokal enhed | Alle m. adgang |
| Driftslister | Løbende når behov er væk | Hver 2. månedJan+mar osv. | x | x |  | Makulering af papirer | Alle m. adgang |
| Manuelt fra lokal enhed |
| *TV-overvågning* | *30 dage*  | *Automatisk* | *x* | *x* |  | *Automatisk* | *System* |

**SLETTEREGLER – automatisk**

På følgende områder slettes personoplysninger af Københavns Kommune jf. den slettefunktionalitet der er indeholdt i det givne system. Institutionen har dog noteret sig følgende frister som bør være overholdt.

| **Procesområde** | **Slettefrist** | **Type af oplysninger** | **Slettemetode** | **Udfører** |
| --- | --- | --- | --- | --- |
| Alm | For. | Føl. |
| Administration og drift | \_\_ år efter borger har forladt SI | x | x | x | Fagsystem (CSC Social) | KK |
| Drift (økonomi) | 5 år efter borger har forladt SI | x | x | x | Fagsystem (Angiv hvilket) |  |
| Personale – Ansøgninger | 6 måneder efter ansættelse | x | x |  | Jobnet |  |
| Personal – Ansættelse, drift, fratrædelse | 5 år efter fratrædelse | x | x | x | System (Angiv hvilket) |  |
| Personale - arbejdsskade | 30 år efter at sagen er afsluttet | x | x | x | System (Angiv hvilket)  |  |
| Arbejdsmiljø og klagesager | 5 år efter at sagen er afsluttet | x | x | x | System (Angiv hvilket) |  |
| Administration – Indsigtsanmodning | 5 år efter endt sagsbehandling | x | x | x | Fagsystem - automatisk |  |
| Værgemål og magtanvendelse | \_\_ år efter endt sagsbehandling | x | x | x | Fagsystem (CSC Social) | KK |
| Utilsigtede hændelser | \_\_ år efter endt sagsbehandling | x | x | x | Fagsystem (CSC Social) | KK |
| Tilsyn – Socialtilsynet og revision | 5 år efter at sagen er afsluttet | x | x | x | Fagsystem (CSC Social) | KK |