HÅNDBOG

Håndbog om Databeskyttelse

Version 27.05.2021

ANSVARLIG

Lone Forsberg

Indholdsfortegnelse

1. HÅNDBOGEN OVERORDNET

1.1. INDLEDNING, DATABESKYTTELSESRÅDGIVEREN & LÆSE-VEJELDNING

Indledning

Hensigten med denne håndbog er at give læseren et indblik i regler om beskyttelse af personoplysninger.

Desuden giver håndbogen gennem eksempler, vejledning og værktøjer et bud på, hvordan databeskyttelse løses i praksis.

Det er også hensigten, at håndbogen skal kunne anvendes som et opslagsværk i dagligdagen, i takt med at spørgsmål opstår.

Databeskyttelsesrådgiveren

Københavns Kommunes Databeskyttelsesrådgiver Jesper Andersen (herefter DPO) er den navngivne DPO for de selvejende institutioner, der har accepteret dette.

Det konkrete DPO-arbejde udføres af DPO teamet for de selvejende institutioner.
Kontaktperson er Lone Forsberg

- Mail: DPOSI@kk.dk
- Tlf.: 3022 0363

DPO's ansvar og opgaver er klart defineret i Databeskyttelseslovgivningen (forordningens artikel 37, 38 og 39) og er uddybet i en vejledning om Databeskyttelsesrådgivere fra Datatilsynet.

I skemaet på næste side fremgår DPO's ansvar og eksempler på konkrete opgaver, som DPO vil udføre for de selvejende institutioner (SI) som deres DPO.

De beskrevne opgaver udgør ikke en udtømmende liste, og DPO'en kan i alle henseender kontaktes for rådgivning. Anbefalinger til hvornår DPO bør kontaktes er beskrevet i de efterfølgende afsnit i håndbogen.

Det anbefales at anvende DPO websiden, der indeholder håndbog, vejledninger, skabeloner mm.

Det skal bemærkes, at DPO's udtalelser kan anvendes som anbefalinger og tilkendegivelser. DPO's udtalelser kan ikke anses som godkendelser. Beslutninger om institutionens håndtering af personoplysninger og af databeskyttelse i øvrigt træffes alene af institutionen.

DPO ansvarsområder	DPO Opgaver (ikke udtømmende)
At underrette og rådgive SI og de ansatte om databeskyttelse	Overvåge fortolkning af loven i evt. retssager / domme mv. Udmelde nyheder – f.eks. Datatilsynets udtalelser Rådgivning ifm. forståelsen og fortolkningen og hvis dette skal omsættes til operationel dagligdag. Konkret rådgivning på enkeltområde – f.eks. Sikkerhedsbrud, registreredes rettigheder i en given situation. Skriftlige eller mundtlige udtalelser – f.eks. vurdering af opbevaring af personoplysninger, slettefrister mv. Inddragelse i SI's beslutninger **inden** disse træffes f.eks. ved nye systemer, udstedelse af retningslinjer/processer, etablering af nye behandlingsområder. Rådgive borgere, der henvender sig direkte til DPO.
At overvåge overholdelsen af de databeskyttelsesretlige regler i SI	Tilsyn på emner eller områder i en enhed ud fra en risikobaseret tilgang. Tilsyn som følge af kritiske hændelser / observationer / sikkerhedsbrud.
At rådgive i forbindelse med udarbejdelse af SI's konsekvensanalyser	Rådgivning når institutionen skal overholde forpligtigelse om at foretage konsekvensanalyse af databeskyttelsen. Forpligtigelsen er der, når en behandling sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder eller frihedsrettigheder – herunder i forbindelse med nye IT-systemer, se nærmere beskrivelse i håndbogen.
At samarbejde med tilsynsmyndigheden.	Høring hos Datatilsynet ved særlige risikofyldte behandlinger.
At fungere som tilsynsmyndighedens kontaktpunkt	Modtage og besvare Datatilsynets henvendelser.

Læsevejledning til håndbogen

Håndbogen indledes med to hovedafsnit.

Afsnit 1.2 handler om begreber, og skal bidrage til forståelsen af alle de udtryk der anvendes gennem håndbogen. Afsnittet kan efterfølgende anvendes som opslagsværk.

Afsnittet 1.3 handler om lovgivningen set i et helikopterperspektiv. Afsnittet skal bidrage til at give den overordnende indsigt i lovgivningens hovedområder og dermed omfang.

Afsnit 2 til 5 handler om lovgivningens bestemmelser i detaljer. Afsnittene beskriver følgende regelområder:

- Behandling af personoplysninger
- Informationssikkerhed
- Registreredes rettigheder
- Hvis noget går galt

Hvert emne behandles på samme måde i følgende underafsnit.

- **Kort fortalt** beskriver emnet i en let forståelig tekst, som rammen for de mere detaljerede beskrivelser og juridiske forklaringer.
- **Hovedregel**, er en sammenskrevet kort version af den eller de regler der gælder for emnet.
- **I praksis**, omsætter emnet til praktik, det vil sige binder lovens krav sammen med daglig håndtering. Der gives eksempler der kan anvendes i dagligdagen.
- **Værktøjer & proces**, beskriver hvis der er udarbejdet skabeloner eller andre værktøjer, der kan eller skal anvendes i dagligdagen for at sikre korrekt håndtering af personoplysninger. Desuden beskrives kort proces for anvendelse.
- **Hvornår søges hjælp**? Lovgivningen er på mange områder overordnet og kan derfor være svær at fortolke, når man står med en konkret handling i dagligdagen. Afsnittet her skal hjælpe læser til at vurdere, hvornår det anbefales at søge hjælp / rådgivning fra DPO, inden der arbejdes videre med forholdet.

I beskrivelserne anvendes begrebet "on-boarding" som er et udtryk for den implementeringsproces SI og DPO gennemfører i samarbejde inden SI overgår til daglig GDPR-drift.

1.2. BEGREBER OM DATABESKYTTELSE

Dataansvarlig / Databehandler

Dataansvarlig

En selvejende institution er dataansvarlig, når denne selv fastsætter formålet med og hjælpemidler til behandling af personoplysninger om kommunens borgere, ansatte og leverandører m.fl. At være dataansvarlig betyder, at være ansvarlig for at overholde kravene i databeskyttelseslovgivningen, og at eventuelle databehandlere på samme vis overholder databeskyttelseslovgivningen.

Databehandler

Hvis den selvejende institution overlader behandling af personoplysninger til eksterne parter eller ved anvendelse af systemer giver eksterne adgang til personoplysninger, er de pågældende databehandlere. Databehandleren kan ikke selv fastlægge formål og hjælpemidler med behandling af personoplysninger (herunder overlade oplysninger til en ny databehandler) med mindre den dataansvarlige giver tilladelse til det. En databehandler kan overlade oplysningerne til en underdatabehandler.

Personoplysninger

Personoplysninger er alle typer af oplysninger (navn, adresse, CPR-nummer, økonomi, helbredsoplysninger, statsborgerskab mv.), som kan knyttes til fysiske personer, f.eks. borgere, ansatte eller medarbejdere.

En oplysning, som ikke direkte kan knyttes til en fysisk person, eksempelvis hvis et cpr-nummer er erstattet med et løbenummer, er også en personoplysning.
En personoplysning behøver ikke direkte at kunne identificere en person. Så snart den kan bruges i kombination med andre oplysninger, til at identificere en person, er det en personoplysning.

Behandling af personoplysninger
Begrebet "behandling" omfatter enhver form for håndtering af personoplysninger. Det kan f.eks. være når den selvejende institution indsamler, registrerer, systematiserer eller opbevarer personoplysninger. Det kan også være en mere konkret håndtering i form af søgning, brug eller sletning af oplysningerne eller hvis disse gives videre til andre.
Der er tale om behandling uanset om det foregår elektronisk eller som fysisk behandling.

En lovlig behandling af personoplysninger
En lovlig behandling af personoplysninger kræver at den selvejende institution har et lovgrundlag der giver lov til at foretage behandlingen fx en særlov. I ganske særlige tilfælde kan det være fx forvaltningsloven, databeskyttelseslovgivningen eller via et samtykke fra den registrerede (borgeren).

Registrerede personer
En registreret person er alle fysiske personer, som institutionen behandler personoplysninger om. Det kan være borgerne, medarbejdere, leverandørers medarbejdere mv.

Fysiske personers rettigheder & frihedsrettigheder
Hvis behandlingen af personoplysninger kan føre til fysisk, materiel eller immateriel skade af personen fx forskelsbehandling, identitetstyveri eller personen taber penge eller vedkommendes omdømme skades. Det kan ligeledes være hvis personens fortrolige/følsomme oplysninger bliver tilgængelige for uvedkommende.

1.3. LOVGIVNINGEN OVERORDNET

Lovgivningens hovedpunkter & intentioner

25. maj 2018 trådte Databeskyttelsesforordningen i kraft sammen med den nationale suppleringslov kaldet Databeskyttelsesloven.

Databeskyttelseslovgivningen gælder for selvejende institutioner, da de anses som offentlige myndigheder, når de via en driftsaftale varetager en offentlig opgave og dermed er undergivet en intensiv offentlig regulering, tilsyn og kontrol.

Intentionerne med Databeskyttelseslovgivningen er at sikre, at personoplysninger behandles sikkert. Der skal dog være en fornuftig balance mellem at overholde Databeskyttelseslovgivningen og fortsat at udføre de myndighedsopgaver, som SI har ansvaret for.

Databeskyttelseslovgivningen kræver derfor, at der udvises ansvarlighed ved:

1. at udpege en Databeskyttelsesrådgiver, der kan rådgive
2. at kunne dokumentere hvilke personoplysninger der behandles og hvordan
3. at sikre at personoplysninger kun behandles, hvis der er lov hertil
4. at det løbende vurderes, om oplysninger kan komme i fare og at behandlinger indrettes så risiko er mindst mulige.
5. at det sikres, at borgernes rettigheder kan opfyldes
6. at risikovurderinger og beslutninger om hvordan SI vælger at overholde lovgivningen kan fremlægges skriftligt

GOVERNANCE - Styring, dokumentation og konkret behandling af data

En SI skal etablere et grundlag for, at personoplysninger håndteres forsvarligt og overholder lovgivningen.

Retningslinjer og slettefrister

Det består af et nødvendigt sæt regler/retningslinjer (inkl. roller og ansvar), der sikrer, at medarbejderen kender krav til den praktiske håndtering og databeskyttelse.

Indholdet og omfanget af regler/retningslinjer skal vurderes i forhold til

- hvilken type af oplysninger der arbejdes med,
- hvor mange og hvordan man har adgang til oplysningerne
- hvordan de skal være beskyttet for at oplysninger ikke kommer til uvedkommendes kendskab og behandles efter reglerne.

Til dette formål anvendes:

- *Retningslinjer og slettefrister (BUF, SUF, SOF)*

Ledelseskontrol

På grundlag af de regler mv. der er defineret fastlægges en klar ansvars- og rollefordeling for ledelsens styring og beslutninger.

Det fastlægges, hvilke kontroller der skal gennemføres af behandlinger og databeskyttelse herunder frekvens og metode, og hvem der gennemfører disse.

Til dette formål anvendes:
- *Ledelseskontrol (med vejledning)*

Årsplan
Som supplement til den løbende ledelseskontrol sikres de nødvendige tværgående aktiviteter i en Årsplan. Det kan være sikring af medarbejdernes uddannelse, dokumentationen for databehandlinger, at regler er tilstrækkelige, formkrav til samtykker er overholdt, vedligeholdelse af persondatapolitik.

Til dette formål anvendes
- *Årsplan (med vejledning)*

Uddannelse af medarbejdere
Slutteligt skal medarbejdere være undervist i regler og processer for hvordan personoplysninger behandles og beskyttes jf. ovenfor.

Til dette formål anvendes:
- *Vejledning vedr. uddannelse af medarbejdere*
- *Undervisnings PIXI til medarbejdere*

Alle anbefalinger findes på DPO Websiden Informationssikkerhed

Beskyttelsen af personoplysninger omfatter ikke kun undervisning i selve behandlingen og kompetencen hos de medarbejdere, der arbejder med oplysningerne. Databeskyttelse omfatter også de fysiske og tekniske omgivelser, som personoplysninger befinder sig i; eksempelvis:

- Omfanget af mulig og etableret databeskyttelse i it-systemer / netværk
- Styring og tildeling af adgange og rettigheder til IT / systemer
- Anvendelse og placering af IT / systemer / PC-er / printere mv.
- Anvendelse og placering af mobile enheder mv.
- Mail / Internet
- Fysiske lokaler & adgange, hvor personoplysninger kan befinde sig mv.
- Fysiske papirer / dokumenter håndtering og opbevaring
- Synlighed / tilgængelighed i fælles informationer

Det skal derfor løbende vurderes, om der er forhold der udgør en risiko for, at personoplysninger er i fare.

Registreredes rettigheder

De registrerede (borgerne) har en del rettigheder som SI skal kunne opfylde. De væsentligste områder er følgende:
- Pligten til at få oplyst om hvilke personoplysninger der behandles og hvorfor

- Retten til at få indsigt i de personoplysninger der behandles
- Retten til berigtigelse, dvs. at få bekræftet og evt. ændret oplysninger, hvis de ikke er korrekte
- Retten til indsigelse, dvs. at få dokumenteret at det er lovligt at behandle givne personoplysninger

Hvis noget går galt (brud på sikkerhed og beredskab)

Hvis personoplysninger på nogen måde kan komme eller er kommet til uvedkommendes kendskab, har SI en forpligtigelse til omgående at stoppe sikkerhedsbruddet og indenfor 72 timer anmelde dette til Datatilsynet. SI bør etablere et konkret beredskab for håndtering af sikkerhedsbrud.

2. BEHANDLING AF PERSONOPLYSNINGER

2.1. DOKUMENTATION AF DATABEHANDLING

Kort fortalt / definition
Lovgivningen stiller krav til dokumentation. Afsnittet beskriver kravene, som blandt andet omfatter fortegnelse og dokumentation af behandling af personoplysninger, der foretages hos den dataansvarlige mv.

Hovedregel
Databeskyttelseslovgivningen stiller krav om, at SI, som dataansvarlig, kan levere en fortegnelse over de behandlinger af personoplysninger, der foretages hos SI.
Fortegnelsen skal have et bestemt indhold for at opfylde kravet.
Desuden stilles krav om, at SI i detaljer ved hvilke personoplysninger, der modtages/indsamles, behandles, opbevares og videresendes til. f.eks. andre dataansvarlige eller databehandlere og på hvilket lovgrundlag dette sker.

I praksis
At levere en fortegnelse og kunne dokumentere behandlinger i detaljer kræver, at de gængse daglige behandlinger er kortlagt, er skriftligt dokumenteret og vedligeholdt.
Dokumentationen kan anvendes i SI's daglige arbejde i forhold til at opfylde oplysningspligten.

Værktøjer & processer
Kortlægning af SI's behandlinger sker igennem on-boarding processen. Registreringer indtastes i et registreringssystem hos DPO.

Fra DPO modtager SI

- fortegnelse,
- detaljeret oversigt over behandlinger (dataprocesser og datastrømme)

SI er ansvarlig for, at dokumentation af behandlinger vedligeholdes ved løbende at indsende rettelser, ændringer og/eller nye behandlinger til DPO.
DPO sikrer registreringer i system og leverer opdateret fortegnelse, risikoprofil mv.
SI er ansvarlig for, at dokumentationen svarer til den faktiske håndtering der sker af personoplysninger.

Hvornår søges hjælp
SI anbefales af søge DPO rådgivning i alle forhold f.eks. vedrørende

- Fortegnelsens indhold og hvordan den anvendes
- Hvad registreringer har af betydning

DPO kan særligt tilbyde:

- Styring og registrering af dokumentation
- Fortegnelsen

2.2. LOVLIG BEHANDLING AF PERSONOPLYSNINGER

Kort fortalt / definition
Afsnittet beskriver, hvad der forstås ved lovlig behandling af personoplysninger og anvisninger til, hvordan dette opnås.

Hovedregel
SI anses som offentlig myndighed og er derfor forpligtiget til at løse myndighedsopgaver. Oftest angiver særlovgivningen retten til at behandle personoplysninger.
SI har ansvaret for at kende og overholde formålet med behandlingen (som det fremgår af særloven). Bl.a. må der ikke indsamles flere personoplysninger, end der er behov for. Oplysninger skal opbevares, så de ikke kommer til uvedkommendes kendskab og må ikke gemmes længere end det er nødvendigt for, at formålet med behandling kan opfyldes.
Har SI et arbejdsbetinget behov for behandlinger uden for særlovens rammer, skal der indhentes samtykke fra de pågældende registrerede (borgere).
Personoplysninger må ikke modtages fra eller videregives til andre dataansvarlige med mindre, der er en lovlig grund til at modtage / aflevere personoplysningerne.
Hvis personoplysninger overlades til databehandlere, skal der foreligge en databehandleraftale med tilhørende instruks, accepteret af begge parter (se senere afsnit).
Særligt for tv- og videoovervågning gælder, at dette som udgangspunkt alene må iværksættes i særlige tilfælde af kriminalitetsforebyggende og tryghedsskabende initiativer.

I praksis
SI's medarbejdere skal have det nødvendige kendskab til indholdet af den særlovgivning, der arbejdes efter, så de ved hvilke personoplysninger, der må arbejdes med og hvordan.
Rutiner og systemanvendelse skal tilrettelægges så behandlingen sker indenfor særlovens rammer, samt at kun medarbejdere med arbejdsbetinget behov har adgang til personoplysningerne.
Medarbejdere skal modtage optimal instruktion / uddannelse i de daglige rutiner og processer.
SI skal sikre nødvendige kontroller af, at personoplysninger er håndteret korrekt.
Anvendelse af evt. samtykke skal være indhentet og udformet efter regler for dette, og samtykket skal overholdes i de daglige rutiner.
SI skal sikre korrekt håndtering og beskyttelse af personoplysninger på særlige områder/rutiner, fx ved anvendelse af mail, sociale medier, formidling af billede eller videomateriale, tv-overvågning etc.

Ved tv- og video overvågning hvor der er almindelig adgang, skal der oplyses om overvågningen ved skiltning eller anden tydelig information. Alle ansatte på stedet skal oplyses om formålet og hvornår optagelserne vil blive gennemgået og evt. videregivet til politiet.

Værktøjer & proces

- *Vejledning vedr. uddannelse af medarbejdere*
- *Undervisnings PIXI til medarbejdere*
- *Skabeloner samtykkeerklæring* – hvor der findes flere varianter alt efter typen af samtykke.

Hvornår søges hjælp

SI anbefales at søge DPO rådgivning,

- Hvis der er usikkerhed om fortolkning og/eller forståelse af særlovgivningen
- Hvis særlovgivningens regler skal balanceres i forhold til krav til databeskyttelse
- Ved anvendelse & overholdelse af samtykke
- Ved håndtering af personoplysninger på særlige områder

2.3. SAMTYKKE

Kort fortalt / definition

Afsnittet beskriver hvad samtykke betyder, hvordan og hvornår det anvendes og hvordan et samtykke udformes.

Hovedregel

Samtykke kan anvendes som grundlag for behandlingen af personoplysninger, hvis der ikke er anden lovgivning / særlovgivning, der giver ret til at behandle personoplysningerne.
Hvis samtykke er nødvendigt, skal det overholde de krav til udformning, som fremgår af Databeskyttelseslovgivningen.
Samtykke skal være frivilligt, skal kunne dokumenteres og skal til en hver tid kunne trækkes tilbage.

For børn under 18 år skal samtykke som udgangspunkt gives af indehaveren af forældremyndigheden eller værge. For informationssamfundstjenester, såsom sociale medier eller andre onlinebaserede services, kan børn og unge over 13 år selv give samtykke.

I praksis

<u>Selve samtykket</u>
Før samtykke indhentes skal det altid vurderes, om behandlingen af personoplysningerne kan ske på et andet grundlag f.eks. love, bekendtgørelser eller lignende.
Kun hvis lovgrundlag ikke kan findes, skal der indhentes samtykke.
Det skal være helt tydeligt for borgeren, hvad der gives samtykke til og samtykket skal være frivilligt for borgeren. Dvs. borgeren skal have mulighed for at afslå uden, at det har direkte eller indirekte konsekvenser.

En usaglig negativ og indirekte konsekvens er f.eks. hvis en sagsbehandler anmoder en borger om et samtykke om at dele borgerens rygestop-oplevelser på Facebook – i øvrigt korrekt og reelt frivilligt – hvis det påvirker behandlingen af en ansøgning om borgerens tilknytning til et dagtilbud.

Dokumentation af indhentede samtykker
Et samtykke skal kunne dokumenteres og bør derfor være skriftligt. Ved et mundtligt samtykke vil det være vanskeligt at bevise hvad det omfatter, f.eks. hvis borgeren gør indsigelse med behandlingen.

SI skal sørge for, at det indhentede samtykke opbevares så det kan findes, evt. slettes ved tilbagekaldelse, og gyldighedsperioder kan overskues.

Tidligere indhentede samtykker (før 25. maj 2018) skal også dokumenteres. Kan gyldigheden af samtykket ikke dokumenteres, skal der indhentes et nyt.

Hvis samtykke trækkes tilbage
En borger kan til enhver tid trække sit samtykke tilbage. Det skal være lige så nemt for borgeren at trække det tilbage, som det var at afgive det. Tilbagetrækkes samtykket, skal SI omgående stoppe behandlingen, som samtykket har givet lov til.
De behandlinger der er foretaget på grundlag af samtykket, før det blev trukket tilbage, er fortsat lovlige. Det vil sige, at det kun er fremtidige behandlinger der skal stoppes, når samtykket trækkes tilbage. Det skal altid vurderes, om personoplysningerne skal slettes, efter et samtykke er trukket tilbage. Hvis oplysninger bruges til andre lovlige behandlinger, kan de fortsat opbevares.

Værktøjer

- *Skabeloner samtykkeerklæring* – hvor der findes flere varianter alt efter typen af samtykke.

Hvornår søges hjælp

SI anbefales at søge DPO rådgivning,

- Hvis der er usikkerhed om særlovgivningen kan anvendes som behandlingsgrundlag eller om der skal indhentes samtykke
- Ved udformning af samtykke
- Hvis der er usikkerhed omkring hvad der skal gøres, hvis et samtykke trækkes tilbage

2.4. ANVENDELSE AF SOCIALE MEDIER

Kort fortalt / definition
Afsnittet giver retningslinjer for, og håndtering af anvendelsen af, sociale medier til kommunikation med og information til borgerne (registrerede)

Hovedregel
På siden/profilen bør formål med brug af siden/profilen fremgå, hvis dette ikke er muligt, så skal det fremgå på SI's egen hjemmeside.

I øvrigt er hovedreglerne:

- Enhver aktivitet på sociale medier skal være båret af en kommunal interesse
- Politiske interesser må ikke fremmes
- Individuel støtte til private erhvervsvirksomheder må ikke ydes
- Generelle erhvervsfremmende aktiviteter må godt støttes
- Det er ikke tilladt at tagge politikere, medarbejdere eller borgere
- Væsentlige nyheder må ikke formidles ALENE på sociale medier, men skal formidles på hjemmeside og i pressen også
- Indhold på sociale medier skal være korrekt og opdateret

I praksis
SI's anvendelse af sociale medier vil blive vurderet i on-boardingprocessen. I forlængelse heraf har SI ansvaret for at sikre, at følgende forhold er opfyldt:

<u>Ansvar for data og samtykke</u>
SI er dataansvarlig for de personoplysninger, som offentliggøres på SI's sider/profiler.
Borgerne er dataansvarlige for de oplysninger, de selv offentliggør på SI's sider/profiler.
Ved offentliggørelse af indhold på SI's sider/profiler, som SI ikke selv har udarbejdet, skal SI sikre tilladelse fra indehaveren af ophavsretten.
Situationsbilleder kan offentliggøres, hvis de er harmløse og ikke miskrediterende overfor personerne på billederne på nogen måde.
Billeder af enkeltpersoner, navne, citater/udtalelser og videomateriale med borgere og/eller medarbejdere kan offentliggøres, hvis SI har indhentet samtykke fra de pågældende personer.
Ved børn under 13 år, skal samtykke indhentes hos forældrene.
Samtykket skal være frivilligt, specifikt, informeret, utvetydigt og skriftligt.
En borger/medarbejder kan til enhver tid trække sit samtykke tilbage.

<u>Borgerdialog gennem sociale medier</u>
Modtager SI henvendelser/spørgsmål fra borgere gennem det sociale medie, bør disse **<u>ikke</u>** bevares derigennem. Derimod bør der henvises til institutionens kontaktmail, for spørgsmål og svar, for at sikrebeskyttelse af de personoplysninger

Værktøjer

- *Skabeloner samtykkeerklæring* – hvor der findes flere varianter alt efter typen af samtykke.

Hvornår søges hjælp
SI anbefales at søge DPO rådgivning,

- Hvis der er usikkerhed om tolkningen af regler i givne situationer herunder om der skal indhentes samtykke
- Ved udformning af samtykke
- Hvis der er usikkerhed om hvad der skal gøres, hvis et samtykke trækkes tilbage

2.5. OPBEVARING AF PERSONOPLYSNINGER OG VURDERING AF SLETTEFRISTER

Kort fortalt / definition
Afsnittet beskriver regler for opbevaring og sletning af personoplysninger, samt hvordan slettefrister kan bedømmes, såfremt lovgivning ikke stiller krav til sletning.

Hovedregel
Personoplysninger må kun opbevares, så længe det er nødvendigt, og har et lovligt formål, eller hvis det er nødvendigt for at dokumentere udførelsen af en myndighedsopgave. Retningslinjer for hvor længe personoplysninger må opbevares (slettefrist) kan være angivet i særlovgivningen.
Angiver særlovgivningen ikke en slettefrist, undersøges det om en evt. anden praksis gør sig gældende.
Såfremt anden praksis heller ikke findes, skal SI selv vurdere, hvor længe personoplysningerne må gemmes.

I praksis
Opbevaring / slettefrister for SI's aktiviteter bliver gennemført og dokumenteret under on-boarding processen.

I forbindelse med opbevaring af personoplysninger skal det altid overvejes om disse kan anonymiseres for at øge beskyttelsen, så de ikke længere er omfattet af databeskyttelseslovgivningen.

SI har efter on-boarding ansvaret for at vedligeholde informationerne om slettefrister

Alle ændringer og tilhørende dokumentation for at ændringer er nødvendige, skal fremsendes til DPO med det samme.

Desuden skal SI sikre, at slettefrister opfyldes i praksis. Det vil sige, at SI tilrettelægger rutiner for, at personoplysninger fremfindes og slettes.

Sletning omfatter alle personoplysninger, der har overskredet grænsen for opbevaring f.eks. personoplysninger placeret i it-systemer, i filer/sager i fagsystemer, i journaliserede dokumenter, på USB-stik, eksterne disks, mobiltelefoner (og tilsvarende mobile enheder), fysiske dokumenter i aflåste arkivskabe etc.

Der bør føres løbende ledelseskontrol med at rutiner gennemføres.

Værktøjer
- *Retningslinjer og slettefrister (BUF, SUF, SOF)*

Hvornår søges hjælp
SI anbefales at søge DPO rådgivning,

- Hvis der er overvejelser om nødvendigheden af anonymisering
- Hvis der er usikkerhed om anbefalede slettefrister
- Når sletning skal finde sted i praksis

DPO kan særligt tilbyde:

- At udarbejde vurdering af slettefrister i samarbejde med SI

2.6. MANUEL BEHANDLING AF PERSONOPLYSNINGER OG USTRUKTUREREDE DATA

Kort fortalt / definition
Afsnittet definerer manuel behandling og ustrukturerede data med personoplysninger, som bevidst eller ubevidst opstår i forbindelse med SI's aktiviteter. Desuden beskrives, hvilke regler / anbefalinger der skal følges for at sikre personoplysninger i den forbindelse.

Hovedregel
Manuelle behandlinger og behandling af ustrukturerede data følge de samme principper, som al øvrig behandling af personoplysninger. Det vil sige, at behandlingen skal have et lovligt/legitimt formål, fx som følge af en særlov. Alternativt skal behandlingen knytte sig til daglig drift, og/eller ligger i naturlig forlængelse af at udføre myndighedsopgaven.
Indgår der følsomme personoplysninger i behandlingen, kræver det som udgangspunkt samtykke fra borgeren.
Simple behandlinger (f.eks. informationslister, noter på opslagstavler etc.), hvor der kun indgår almindelige personoplysninger, kræver ikke samtykke.

Fordi behandlingerne ikke er beskyttet af it-systemers sikkerhedsfunktioner, men er fysisk tilgængelige eller er indeholdt i ubeskyttede medier etc. skal SI sikre rutiner for beskyttelse af personoplysningerne.

I praksis
Manuelle behandlinger er behandlinger, der ikke er direkte foretaget i et system. Det kan være:

- Fysiske noter og dokumenter med personoplysninger
- E-mails
- Word, Excel, PDF og Power Point filer med personoplysninger f.eks. gemt på lokale drev
- Personoplysninger opbevaret på USB-stik, eksterne harddiske
- Personoplysninger i sms-beskeder
- Outlook mødeaftaler
- Billeder på mobiltelefoner, og lign.

Ustrukturerede data er typisk et produkt af en manuel behandling. Ustrukturerede data kan eksempelvis opstå, hvis medarbejdere skriver noter ned omkring borgere i et Word-dokument, og gemmer det tilfældigt på computeren. Det kan ligeledes være håndskrevne noter omkring borgere.

Ustrukturerede data der bør undgås, er eksempelvis:

- Noter med oplysninger om pårørende, der ikke er nødvendige for institutionens daglige arbejde, og derfor bør undgås. F.eks. mors tandlægebesøg som årsag til afhentningstidspunkt for barn i institution.

Ustrukturerede data der kan accepteres:

- En liste til en chauffør om særlige hensyn der skal tages til borgerne med fysiske og psykiske handicap, ved transport. Oplysninger skal have karakter af konkrete anvisninger og følsomme oplysninger bør undgås.

SI's manuelle behandlinger og ustruktureret data er omfattet af on-boarding processen ved en gennemgang af de behandlinger der foregår hos SI.

I forlængelse heraf er det SI's ansvar at sikre og vedligeholde regler og rutiner for, hvordan manuelle behandlinger og ustruktureret data håndteres og slettes således at de er lovlige og behandles med størst mulig sikkerhed.

Værktøjer

- *Skabelon til registrering af ustruktureret data*
- *Skabelon til registrering af manuelle behandlinger*

Hvornår søges hjælp

SI anbefales at søge DPO rådgivning,

- Hvis der er usikkerhed om definitionen af manuel behandling
- Når sikkerhed omkring manuelle behandlinger skal vurderes
- Når der er tvivl om håndtering og indholdet af ustruktureret data
- Når der skal findes optimale løsninger på legitim anvendelse af ustruktureret data

2.7. FYSISK SIKKERHED

Kort fortalt / definition

Fysisk sikkerhed omfatter alle forhold af fysisk karakter hos den dataansvarlige, hvor der behandles personoplysninger (fx brug, opbevaring eller arkivering). Afsnittet beskriver regler og opmærksomhedspunkter vedrørende fysisk sikkerhed.

Hovedregel

Hovedreglen er, at alle tænkelige fysiske forhold skal være vurderet og tilrettelagt, så de skaber den bedst tænkelige beskyttelse af personoplysninger.

I praksis

Vurdering af SI's fysiske sikkerhed er omfattet af on-boarding processen ved en detaljeret gennemgang.

I forlængelse heraf er det SI's ansvar at vedligeholde regler og rutiner for, hvordan fysiske forhold skal være tilrettelagt samt sikre at det sker i praksis.

Til dette hører bl.a.

- Fysiske lokaler og kontrol af adgange hertil
- Fysiske dokumenter og informationer, samt adgang og opbevaring.
- Mobile enheder, indhold, anvendelse og beskyttelse

- Fysisk og teknisk it-sikkerhed (behandles også under afsnit 5)
- Eksterne parters (leverandører, gæster, borgere mv.) adgang til SI

Værktøjer

- *Oversigt over flytbare-mobile enheder*

Hvornår søges hjælp

SI anbefales at søge DPO rådgivning,

- Hvis der er usikkerhed om eller praktiske spørgsmål til, etablering af tilstrækkelig fysisk sikkerhed.

2.8. DATABEHANDLERE

Kort fortalt / definition

Databehandlere er eksterne parter, der på grundlag af en aftale modtager og behandler personoplysninger på vegne af SI (dataansvarlige). Afsnittet beskriver regler og retningslinjer i forbindelse med anvendelse af databehandlere, hvornår aftaler skal indgås samt indgåelse af selve aftalen.

Hovedregel

Der skal udarbejdes en databehandleraftale i alle de tilfælde, hvor der overlades personoplysninger til en ekstern part, der IKKE er selvstændigt dataansvarlig og derfor kun har et lovligt grundlag til at modtage de givne oplysninger, hvis det sker på grundlag af en databehandleraftale.

Databehandleraftalen skal udformes, så den lever op til lovgivningens krav hertil. Herunder skal der udarbejdes en udførlig instruks, der angiver hvilke krav til behandling og databeskyttelse databehandleren skal leve op til.

Den databehandlerskabelon, der skal anvendes som grundlag for aftaler, vil til hver en tid kunne rekvireres fra DPO.

Den dataansvarlige (SI) er forpligtiget til løbende at følge op på, at databehandlere lever op til aftalens bestemmelser.

I praksis

Databehandlere kan f.eks. være tilfælde hvor en ekstern part:

- Udfører en intern opgave på vegne af institutionen, f.eks. at en ekstern virksomhed foretager institutionens lønudbetalinger.
- Drifter et IT-system for SI. Der er indgået en driftsaftale med leverandør om support og udvikling af et system, og leverandøren har derfor adgang til de persondata systemet indeholder.
- Stiller et it-system til rådighed for SI (hoster), og dermed opbevarer og som leverandør har adgang til institutionens indtastede oplysninger

Gennem on-boarding processen afdækkes, hvorvidt SI overlader personoplysninger til databehandlere, og om der er indgået tilstrækkelige databehandleraftaler og instrukser.

SI skal efterfølgende sikre at aftalesamarbejdet vedligeholdes med databehandlerne, og at der føres tilsyn min. 1 gang årligt med, at de overholder de indgåede aftaler om håndtering af personoplysninger og databeskyttelse.

Etableres samarbejder med nye databehandlere skal SI sikre, at der indgås en databehandleraftale.

Værktøjer

- *Databehandleraftale skabelon (udleveres ved henvendelse)*

Hvornår søges hjælp

SI anbefales at søge DPO rådgivning,

- Hvis der er usikkerhed om, hvorvidt der er tale om en databehandler og/eller skal indgås en databehandleraftalen
- Når databehandleraftalen og instruks skal udarbejdes
- Når der skal føres tilsyn med/følges op på databehandleren

DPO kan særligt tilbyde:

- At udarbejde databehandleraftaler og instrukser i samarbejde med SI

3. INFORMATIONSSIKKERHED

Kort fortalt / definition

Informationssikkerhed retter sig mod at beskytte personoplysninger, når disse håndteres via it-systemer, gennem manuelle rutiner, elektroniske kommunikations- og informationskanaler og interne & eksterne netværk mv.

Hovedregel

Hovedreglen er, at SI skal sikre lovmedholdelighed, fortrolighed, integritet og tilgængelighed når personoplysninger modtages, behandles og opbevares.

- Med lovmedholdelighed menes, at love og regler for behandling af personoplysninger er korrekt og beskytter borgernes (registreredes) rettigheder.
- Med fortrolighed menes, at personoplysninger i alle tilfælde kun er tilgængelige for de medarbejdere, systemer eller eksterne parter, der har et lovligt arbejdsbetinget behov for at have adgang til oplysningerne
- Med integritet menes, at personoplysninger i alle tilfælde er valide / ikke manipuleret
- Med tilgængelighed menes, at personoplysninger skal være tilgængelige for alle med autoriseret adgang til oplysningerne.

I praksis

Der skal fastsættes passende tekniske og organisatoriske sikkerhedsforanstaltninger, som skal sikre personoplysninger i it-systemer, computere og mobile enheder.

Ved tekniske foranstaltninger forstås, indbyggede funktioner og funktionalitet, der øger sikkerheden for, at uvedkommende ikke kan få adgang til at se eller behandle personoplysninger.

Ved organisatoriske foranstaltninger menes regler, forretningsgange, vejledninger mv. der understøtter databeskyttelse. Det kan også være foranstaltninger som begrænser medarbejderes adgange og rettigheder.

SI's informationssikkerhedsniveau vil blive vurderet ved implementering af SI (on-boarding), hvorefter SI skal udforme konkrete retningslinjer, for de enkelte områder som medarbejderne skal følge og leder føre tilsyn med.

Herunder følger således anvisninger til håndtering af de væsentligste forhold indenfor informationssikkerhedsområdet:

Personalesikkerhed
Alle eksisterende og nye medarbejdere skal instrueres i relevante informationssikkerhedsregler og regler for persondatabeskyttelse.
Medarbejdere med adgang til it-systemer og personoplysninger mv. skal være bekendt med eget ansvar, opgaver i forhold til informationssikkerhed og databeskyttelse.

Styring af systemer og andre enheder
Der skal foreligge en ajourført fortegnelse samt evt. særlige persontilhørsforhold over særligt

- Computere, herunder bærbare PC'ere
- Mobile enheder f.eks. telefoner, tablets, foto-/videoudstyr mv.

DPO har et register over SI's systemer.
Desuden skal der formuleres regler for anvendelse af enheder fx i forhold til anvendelse og opbevaring.

Adgange og rettigheder for brugere
Medarbejdere må kun have adgange og rettigheder til systemer og personoplysninger som de har et arbejdsbetinget behov for. Ændres det arbejdsbetingede behov, skal adgange og rettigheder ændres tilsvarende.
Fratræder medarbejderen skal adgange og rettigheder lukkes.
Autorisationer og rettigheder skal vurderes / godkendes af ansvarlig leder og skal kunne dokumenteres.
Adgange til it-udstyr/systemer skal ske ved brug af individuelle adgangskoder.
Alle arbejdsstationer skal have skærmlås, og skriveborde skal være ryddet for personoplysninger.

Ved tv-og video overvågning skal der træffes de nødvendige foranstaltninger mod, at optagelser kommer til uvedkommendes kendskab eller misbruges. Kun et begrænset antal medarbejdere må have adgang til optagelserne.

Der skal foretages tilsyn med at adgange og rettigheder til anvendelse af systemers funktioner ikke misbruges.

Kommunikationssikkerhed (netværkssikkerhed)
Kommunikation med borgere, virksomheder og andre myndigheder skal ske via sikre linjer (krypteret), sikre digitale mailløsninger, borgernes e-Boks mv. Åbne / usikre kommunikationsformer må ikke indeholde fortrolige eller følsomme personoplysninger.

Værktøjer

- *Skabelon for oversigt over flytbare-mobile enheder*
- *Skabelon for oversigt over medarbejderes adgange og rettigheder*

Hvornår søges hjælp

SI anbefales at søge DPO rådgivning,

- Hvis der er usikkerhed omkring fortolkning og/eller forståelse af hvordan tilstrækkelig informationssikkerhed opnås

4. REGISTREREDES RETTIGHEDER

4.1. INDLEDNING VEDR. REGISTREREDES RETTIGHEDER

Den dataansvarlige (SI) har en række forpligtelser overfor registrerede (borgere og andre personer) såkaldte "registreredes rettigheder".

Disse rettigheder indebærer, at den registrerede

- skal modtage oplysninger om de behandlinger der foretages om vedkommende
- kan rette henvendelse til SI og bede om at få indsigt i oplysninger og gøre indsigelse mod en behandling af deres oplysninger
- kan bede om at få rettet eller slettet oplysninger og
- kan bede om at få udleveret oplysninger, som institutionen behandler om dem.

I det efterfølgende er registreredes rettigheder uddybet.

4.2. GENERELLE REGLER FOR REGISTREREDES RETTIGHEDER

Identifikation af den rette borger
Ved modtagelse af henvendelse fra en registreret, skal SI altid sørge for, at registreret er den person pågældende udgiver sig for.
Hvis det vurderes, at registrerede ikke kan identificeres, fx ved telefonisk kontakt eller ukendt mailadresse, skal man bede om yderligere identifikation.

Yderligere identifikation skal altid foregå på en sikker kommunikationsforbindelse eller ved fysisk fremmøde.

Besvarelse af henvendelser
Besvarelse af henvendelser, der drejer sig om opfyldelse af registreredes rettigheder, bør som udgangspunkt gives på skrift, medmindre den pågældende selv beder om en mundtlig eller telefonisk besvarelse.

Hvis besvarelsen indeholder følsomme eller fortrolige oplysninger, skal SI sikre sig, at besvarelsen bliver afsendt på en sikker måde, f.eks. e-Boks, Sikker Mail eller pr. brev.

Henvendelserne skal som udgangspunkt besvares inden for en måned. Er der særlige forhold der gør sig gældende, kan fristen forlænges til to måneder.

Valg af rette regelsæt – Databeskyttelsesforordningen kontra offentlighedsloven/forvaltningsloven
SI skal ved vurdering af personens rettigheder, tage stilling til hvilket sæt regler, der giver borgeren den bedste retsstilling, og dermed skal institutionen behandle anmodningen efter disse bestemmelser.

4.3. UNDTAGELSER TIL REGISTREREDES RETTIGHEDER

Ved henvendelser fra personer, vedrørende deres rettigheder, skal det vurderes om den givne rettighed kan tilsidesættes som følge af undtagelser til den konkrete situation. Opstår der tvivl om en henvendelse er omfattet af en undtagelse, skal DPO'en kontaktes.

4.4. OPLYSNINGSPLIGT

Kort fortalt / definition
Afsnittet beskriver regler for oplysningspligt, i hvilke tilfælde der er en pligt, og hvad den skal indeholde.

Hovedregel
Alle registrerede har ret til at blive oplyst om hvordan og hvilke behandlinger, der foretages af deres personoplysninger.
Den dataansvarlige (SI) skal sikre at pligten opfyldes, både når institutionen indsamler oplysninger direkte, og når institutionen modtager oplysninger fra andre end den registrerede selv.
Oplysningen af borgeren skal ske første gang, der foretages en indsamling af oplysninger til et konkret formål.

Der skal ikke foretages yderligere oplysning over for borgeren, medmindre oplysningerne anvendes til andre formål, end dem de er indsamlet til, hvis de ikke indgår i normal daglige drift, eller hvis oplysningerne kommer fra en anden person end registrerede selv.
Opfyldelse af oplysningspligten uanset om den er skriftlig eller mundtlig skal kunne påvises.

I praksis
Overholdelse af oplysningspligt gennemgås i on-boarding processen og består hovedsagelig af at udarbejde og formidle en privatlivspolitik for henholdsvis borgere og medarbejdere.

Efterfølgende skal SI udforme og implementere tilstrækkelige retningslinjer for medarbejdere, der sikrer at privatlivspolitikkerne og evt. øvrig oplysningspligt efterleves fremover.

Regler for opfyldelse, undtagelser samt de oplysninger, der skal indgå når registrerede oplyses, fremgår af vejledning til håndtering af oplysningspligt.

Værktøjer
- *Skabelon for cookiepolitik*
- *Privatlivspolitik for borgere/børn og pårørende (BUF, SUF og SOF)*
- *Privatlivspolitik for medarbejdere*

Hvornår søges hjælp
SI anbefales af søge DPO rådgivning
- Når regler om oplysningspligten skal fortolkes og omsættes til praksis
- Når oplysningspligt skal påvises og/eller udarbejdes som skriftlig information

4.5. INDSIGTSRET OG AKTINDSIGT

Kort fortalt / definition
Afsnittet beskriver regler for retten til indsigt, i hvilke tilfælde der er en pligt og hvad den skal indeholde.

Hovedregel
De registrerede borgere, og andre personer, som den dataansvarlige behandler oplysninger om, har ret til at få en række informationer og eller oplysninger udleveret, vedrørende den behandling der foretages.

Grundlæggende er der 3 niveauer af anmodninger fra den registrerede:

1. Ønske om at modtage information om hvilke personoplysninger og til hvilket formål, den dataansvarlige (SI) har registreret/opbevaret personoplysninger. *Dette er en indsigtsanmodning.*

2. Ønske om at modtage kopi af de personoplysninger som den dataansvarlige (SI) har registreret/opbevaret om personen.
   Dette er en indsigtsanmodning.

3. Ønske om at modtage hele sagsagter ikke kun med henblik på at se personoplysninger men hele sagens akter.
   Dette er en aktindsigtsanmodning.

I praksis
Indsigt / aktindsigt
Henvendelse fra en registrerede eller en pårørende, bør umiddelbart altid anses som en anmodning om at få indsigt.

SI skal altid vurdere om der er tale om en indsigtsanmodning eller en aktindsigtsanmodning. Desuden skal det afklares, hvordan henvendelsen skal håndteres, så det giver den registrerede den bedste retsstilling.

Afslutningsvis skal det afklares hvad der søges indsigt i. Det vil det være praktisk at bede om en uddybning af anmodningen. Herefter besvares anmodningen som det fremgår af skabelon herunder og den retmæssige dokumentation medsendes.

Værktøjer
- *Vejledning til besvarelse af indsigtsanmodning*
- *Skabelon til besvarelse af indsigtsanmodning*

Hvornår søges hjælp
SI anbefales af søge DPO rådgivning
- Når regler om indsigt / aktindsigt skal fortolkes, vurderes og besvares

4.6. ØVRIGE RETTIGHEDER

Kort fortalt / definition

Afsnittet beskriver regler for og uddybning af de øvrige områder af registreredes rettigheder, og hvordan disse rettigheder opfyldes.

Hovedregel

- **Ret til berigtigelse** – Den registrerede har ret til at få ændret personoplysninger, som ikke er rigtige eller er mangelfulde.
- **Ret til sletning** – som udgangspunkt har den registrerede ikke ret til at få personoplysninger slettet, når oplysningerne behandles af en offentlig forvaltning, som led i myndighedsudøvelse.
- **Ret til begrænsning** – Den registrerede har som udgangspunkt ret til at få begrænset behandlinger.
- **Ret til dataportabilitet** – Den registrerede har ret til at få udleveret personoplysninger, som behandles om dem, såfremt oplysninger er indsamlet på grundlag af et samtykke eller en kontrakt.
- **Ret til indsigelse** – Den registrerede har ret til at gøre indsigelse – dog kan indsigelsen oftest ikke imødekommes, da myndighedsopgave sker på grundlag af en lovgivning.

I praksis

Retten til berigtigelse (at få rettet oplysninger), retten til sletning og retten til begrænsning af behandling

Den registrerede har i nogle situationer ret til at få rettet, slettet eller begrænset de oplysninger, som SI behandler om dem. SI skal i alle tilfælde lave en konkret vurdering, om de kan efterkomme anmodningen om sletning, rettelse eller begrænsning.

Da SI anses for at være en offentlig virksomhed, er den underlagt et krav om at kunne dokumentere sager. Disse pligter medfører, at det kun i sjældne tilfælde vil være muligt at rette, slette og begrænse de personoplysninger, som institutionen behandler om borgerne, så længe de vedrører den daglige kontakt og håndtering af registrerede, og så længe oplysninger er korrekte.

Derudover er SI underlagt en række lovkrav, der direkte pålægger institutionen at opbevare oplysninger i et givent antal år. Kun i de tilfælde hvor SI har opbevaret oplysninger om en borger længere end det er tilladt, skal personoplysningerne slettes på borgerens anmodning.

Retten til dataportabilitet

Borgere har ret til dataportabilitet. Det vil sige, at personoplysninger, som SI behandler om den registrerede, skal udleveres i et struktureret, almindelig anvendt og maskinlæsbart format, samt at få disse oplysninger overført til en anden dataansvarlig.

Retten til at gøre indsigelse mod en behandling

Retten til at gøre indsigelse, giver borgerne ret til at "protestere" over en ellers lovlig behandling. En indsigelse skal indeholde en redegørelse for den

konkrete situation, hvor borgeren er utilfreds med, at institutionen behandler vedkommendes personoplysninger.

Værktøjer

- Ingen

Hvornår søges hjælp

SI anbefales af søge DPO rådgivning

- Når regler skal fortolkes og håndteres i praksis – særligt hvis der opstår tvivl om, hvilken rettighed borgeren gør brug af

5. PERSONDATABRUD & DATATILSYNET

5.1. PERSONDATABRUD OG ANMELDELSER TIL DATATILSYNET

Kort fortalt / definition
Afsnittet beskriver, hvad der forstås ved et persondatabrud, hvad reglerne er, samt hvordan sikkerhedsbrud håndteres i praksis.

Hovedregel
Et persondatabrud defineres som en episode, der fører til en hændelig eller en ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger.

Dataansvarlig har en række lovbestemte forpligtigelser og et selvstændigt ansvar for håndtering af personoplysninger, der skal sikre en hurtig og effektiv håndtering af brud på persondata.

I praksis
Hændelser, der potentielt kan eller har forårsaget et persondatabrud, skal håndteres med det samme.

Derfor skal ledelsen sikre, at DPO's proces og forretningsgang for persondatabrud er implementeret overfor medarbejderne. Dvs. informationerne om håndtering er tilgængelige og forstået.

Forretningsgangen skal sikre, at medarbejdere anmelder persondatabrud til nærmeste leder, der efterfølgende sørger for at:

- Bruddet stoppes med det samme / gennemførelse af nødplan
- Bruddets årsag og virkning undersøges og håndteres
- De registrerede, hvis personoplysninger der er omfattet af bruddet, bliver underrettet, hvis det er nødvendigt.
- Lave en plan for kommunikation med ledelse/bestyrelse og DPO
- Bruddet anmeldes til Datatilsynet indenfor de lovpligtige tidsfrister på 72 timer fra bruddet er opdaget

Ledelsen skal desuden sikre, at håndtering og overholdelse af tidsfrister kan dokumenteres, samt at der træffes foranstaltninger til at tilsvarende brud ikke sker igen.

Værktøjer

- *Skabelon til indsamling af fakta om brud på persondata*

Hvornår søges hjælp
SI anbefales at søge DPO rådgivning **så snart et faktisk eller potentielt bud opdages**

DPO kan særligt tilbyde:

- Vurdering af om der er tale om et persondatabrud
- Anbefalinger til aktiviteter for at stoppe læk

- Vurdering af om registrerede skal underrettes og hvad der skal underrettes om
- Vurdering af om der skal anmeldes til Datatilsynet og hvad anmeldelsen skal indeholde.

5.2. HÅNDTERING AF HENVENDELSER FRA DATATILSYNET

Beskrivelsen herunder skal tjene som retningslinjer og værktøj ved Datatilsynets tilsynsaktiviteter i selvejende institutioner (SI) med henblik på at sikre at:

- Datatilsynet møder en professionel, struktureret og imødekommende dataansvarlig
- SI og DPO på forkant har afstemt ansvar og opgaver for tilsyn fra Datatilsynet.

Initiering
Datatilsynets henvendelser generelt og vedr. konkrete tilsyn vil i overvejende grad tilgå SI's DPO og vil bestå af

- Planlagte tilsyn jf. offentliggjort årsplan
- Ad hoc tilsyn afledt af særlige observationer / hændelser

Ved evt. henvendelser fra Datatilsynet vedr. tilsyn rettet direkte til en SI, skal SI henvise til DPO'en, der varetager den videre koordinering, når dokumentationen af drift skal vurderes af Datatilsynet.

Afstemning og koordinering
Afstemning og koordinering sker i samarbejde med SI.

DPO'en koordinerer følgende i forlængelse af henvendelser:

- Afdækning / dialog med Datatilsynet om indhold, omfang og tidspunkt for tilsyn der ønskes gennemført
- Fremskaffelse og fremsendelse af forudgående dokumentation
- Planlægning og koordinering af tilsynets gennemførelse (møder mv.)

Tilsyn med compliance
DPO har ansvaret for at koordinere, så Datatilsynet opnår en indsigt i SI's opfyldelse af ansvarlighed ved håndtering af personoplysninger og databeskyttelse.

Med udgangspunkt i tilsynsemnet, inviteres Datatilsynet til at modtage en introduktion til SI's compliance herunder nødvendig fremlæggelse af:

a. Governance (regler, forretningsgange, koncepter, værktøjer mv.)
b. Complianceniveau (legal status)
c. Risikoprofil
d. Dokumentation & rapportering af rådgivning og tilsyn.

Vejledninger og skabeloner
Relevante vejledninger fra Datatilsynet kan findes på: www.datatilsynet.dk
Alle skabeloner henvist til i ovenstående kan findes på vores DPO-hjemmeside.