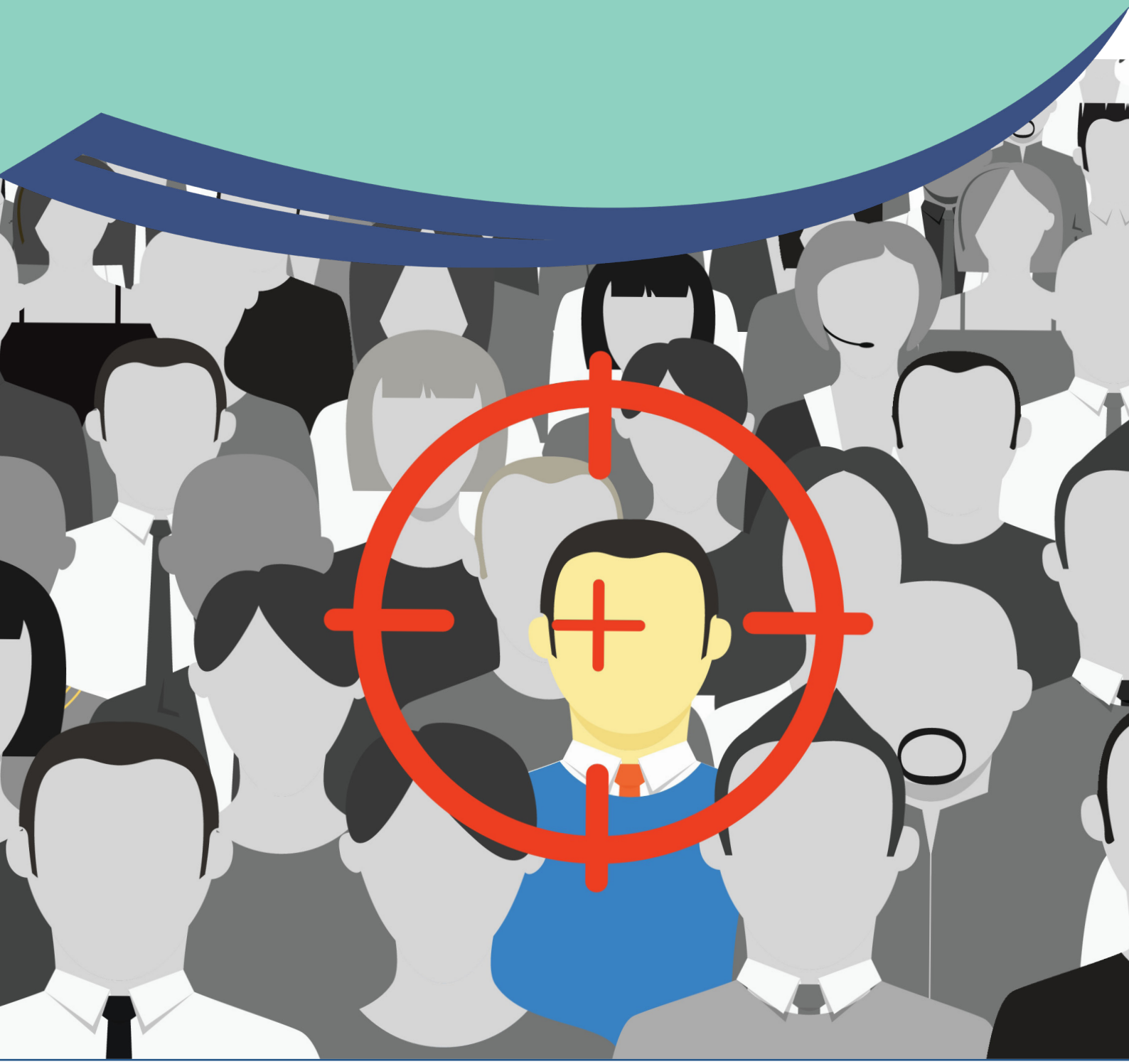
# Personoplysninger

## – Sådan gør vi



PRAKTISERENDE LÆGERS ORGANISATION
Region Sjælland

lollandkommune

BLF
Business Lolland-Falster

GULDBORGSUND

REGION SJÆLLAND
– vi er til for dig

# Forord

Den 25. maj 2018 trådte Databeskyttelsesforordningen i kraft. Den bliver populært kaldet Persondataforordningen eller GDPR efter det engelske navn: General Data Protection Regulation.

Forordningen udgør sammen med supplerende dansk lovgivning og vejledninger nu den samlede lovpallet.

Som noget nyt skal vi fremover dokumentere skriftligt, hvordan vi overholder loven. Vi har derfor samlet overvejelser, procedurer og interne regler for, hvordan vi indsamler, håndterer, anonymiserer og sletter data i denne vejledning.

Samtidig vil vi undervejs introducere termerne omkring personoplysninger og databeskyttelse, således at rapporten også kan benyttes som vejledning og opslagsværk.

*Bemærk - Hvis der er uoverensstemmelse mellem denne vejledning og lokale retningslinjer på egen arbejdsplads, skal man som udgangspunkt følge reglerne fra eget ansættelsessted, med mindre reglerne her dækker et højere sikkerhedsniveau.*

I Bilag 1 har vi samlet dokumentation for hjemmel, hvilke typer af oplysninger vi håndterer i Broen, hvordan vi opbevarer dem og hvornår de bliver slettet.

Både bilag og vejledning er dynamiske dokumenter, som vi opdaterer løbende efter behov.

## Afgrænsning

Denne vejledning dækker Broen til Bedre Sundheds sekretariat, vores ledelsesinformation, drift og projekter under Interventionsstyregruppen. Ikke Broen til Bedre Sundheds forskningsaktiviteter.

I praksis arbejder Broen til Bedre Sundhed med en bred vifte af personoplysninger. Fra overordnet statistik i vores ledelsesrapport til analyser af helbredsoplysninger på individniveau i vores projekter. I både anonymiseret, pseudonymiseret og ikke-anonymiseret form.

Vi arbejder desuden med personoplysninger på tværs af vores partnerskab: Mellem Region Sjælland, Lolland og Guldborgsundhed Kommuner, de praktiserende læger og det lokale erhvervsliv.

## En løbende proces

Denne vejledning er udgivet i maj 2018, hvor visse procedurer stadig er nye og ikke helt på plads endnu. Vi afventer f.eks. pt. en afklaring af en intern arbejdsgang mellem IT Sikkerhed, PFI og KU i Region Sjælland.

Vejledningen vil derfor blive løbende opdateret og indtil da arbejder vi ud fra de retningslinjer, der er beskrevet her.

## Anvendelse

Vejledningens information er primært hentet fra Datatilsynets hjemmeside, PFI i Region Sjælland, Region Sjællands retningslinjer og fra Kammeradvokaten.

Andre afdelinger er velkomne til at hente inspiration i Broens retningslinjer, men anvendelse sker på eget ansvar. Broen til Bedre Sundhed kan ikke gøres ansvarlig for eventuelle fejl og mangler, eller for senere ændringer, der vil kræve at dokumentet skal opdateres.

## God læselyst

Har du spørgsmål til indhold og brug af vores vejledning, er du velkommen til at kontakte Broens analysekonsulenter:

Helle Bergholdt
E-mail: hekb@regionsjaelland.dk
Telefon: 93 57 00 17

Ditte Rasmussen
E-mail: dira@regionsjaelland.dk
Telefon: 24 41 82 14

God fornøjelse.

# Anmeldelse af projekter

## Sådan gør vi

Ved forskningsprojekter:

Alle forskningsprojekter skal anmeldes til PFI, ligesom der skal udarbejdes databehandler-aftaler efter behov.

Anmeldelsen skal følge PFI's retningslinjer, som er beskrevet på deres hjemmeside.

Ved kvalitetsprojekter:

Kvalitetsprojekter i Broen til Bedre Sundhed skal (indtil videre) anmeldes i Broens Sekretariat, da det pr. maj 2018 er uafklaret hvilken enhed i Region Sjælland, der skal stå for at håndtere kvalitetsprojekter.

I praksis anvender vi samme blanketter (fra PFI) som ved forskningsprojekter. Det gør det muligt at flytte materialet til en anden enhed, når den endelige opgaveplacering er på plads.

Er du i tvivl, kan Sekretariatets analysekonsulenter hjælpe.

## Det siger reglerne

Med den nye Persondataforordning skal vi ikke længere anmelde projekter til Datatilsynet.

Til gengæld skal vi til hver en tid dokumentere skriftligt, at vi lever op til gældende lovgivning. Herunder oplyse hvilke data vi behandler og hvordan.

Alle projekter skal derfor anmeldes internt i Region Sjælland

Skemaerne sendes til analysekonsulenterne i Broens Sekretariat og journaliseres i Fics. Skema over aktiviteter i Bilag 1 opdateres.

Det skal fremgå tydeligt af både projektbeskrivelse og anmeldelse, hvordan data vil blive opbevaret og hvor længe.

Hvis du vil ændre eller forlænge dit projekt, skal du indsende en revideret anmeldelse.

# Databeskyttelsesrådgiver

## Sådan gør vi

Region Sjællands Data Protection Officer (DPO) hedder Helle Jeppesen og er placeret i Koncern IT. Kontakt derfor Koncern IT ved spørgsmål.

I Guldborgsund Kommune varetages rollen som DPO pr. maj 2018 af et team af advokater hos advokatfirmaet Bech-Bruun. I Lolland Kommune er det endnu uafklaret, hvem der varetager rollen.

Brug derfor i stedet denne vejledning, som bliver løbende opdateret. Giv Sekretariatets analysekonsulenter besked, hvis der er fejl eller mangler.

## Det siger reglerne

Med Persondataforordningen skal alle offentlige institutioner ansætte en Data Protection Officer (DPO), som skal:

- Understøtte instutionen i at overholde reglerne i Persondataforordningen.
- Rådgive egen organisation.
- Være uafhængig.
- Være kontaktperson ved besøg fra datatilsynet.
- Være kontaktperson ved sikkerhedsbrud.

# Brud på sikkerheden

## Det siger reglerne

For at kunne reagere på et sikkerhedsbrud, skal man først og fremmest kunne genkende ét. I Persondataforordringen defineres et brud på persondatasikkerheden således:

*"Et brud på sikkerheden, der fører til hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller anden måde behandlet."*

Et brud på persondatasikkerheden forekommer, når uautoriserede (gælder både i og uden for egen organisation) får adgang til eller kommer i besidelse af oplysningerne.

F.eks. hvis IT-systemerne ikke er tilstrækkeligt sikret mod at udefrakommende får adgang (hvis en server bliver hacket) eller manglende kryptering af en hjemmeside medfører at data bliver tilgængelige for offentligheden.

Ved et databrud, som medfører en risiko for personers rettigheder eller frihedsrettigheder (omfatter diskrimination, idenitetstyveri eller svindel, økonomisk tab, skade på omdømme, tab af fortrolighed af data underlagt tavshedspligt eller enhver anden væsentlig økonomisk eller social ulempe for den registrede) skal datatilsynet underrettes uden unødig forsinkelse og om muligt senest 72 timer efter at den dataansvarlige er blevet bekendt med bruddet.

Den dataansvarlige skal straks efter at være blevet bekendt med bruddet på persondatasikkerheden vurdere sandynligheden for, at bruddet indebærer en risiko for de berørte fysiske personers rettigheder.

Følgende aspekter skal indgå i denne risiko-vurdering:

- Typen af sikkerhedsbrud, herunder om der er sket tab af oplysninger, brud på fortroligheden eller en integritetskrænkelse.
- Oplysningernes art og omfang.
- Risikoen for at registrerede kan identificeres.
- Konsekvenser bruddet kan have for de registrerede.
- Hvorvidt bruddet omfatter særlige registrerede (f.eks. hvis der er tale om børn eller særligt udsatte).
- Antallet af berørte fysiske personer.

## Sådan gør vi

Hvis man bliver bekendt med et brud på persondatasikkerheden, har vi pligt til at reagere omgående. Også selvom vi har fri.

Når ulykken er sket:

- Stands ulykken: Luk sikkerhedsbrudet. Og vær sikker på, at det bliver lukket korrekt. Få eventuelt hjælp fra IT helpdisk.
- Flyt data til et sikkert sted.
- Alarmer: Orienter din nærmeste leder og den dataansvarlige på projektet.
- Orienter analysekonsulenterne i Broen til Bedre Sundheds sekretariat og husk at journalisere din henvendelse.

  Analysekonsulenterne orienterer herefter DPO og IT Sikkerhedsgruppen i Region Sjælland (it-sikkerhed@regionsjaelland.dk), som orienterer Datatilsynet (Husk at journalisere alle henvendelser).

  I visse tilfælde skal de personer, hvis oplysninger er berørt af sikkerhedsbruddet også blive orienteret.

# Type af personoplysninger

## Det siger reglerne

Personoplysninger er enhver form for information (f.eks. CPR, lægejournal, biologisk materiale, et billede eller et fingeraftryk), der kan henføres (direkte eller indirekte) til en fysisk person. Også selvom personen kun kan identificeres, hvis oplysningen kombineres med andre oplysninger. F.eks. når blodprøvesvar kobles til et personnummer. Man betegner i så fald oplysningen som "personhenførbar".

Databeskyttelsesforordningen opdeler personoplysninger i tre typer:

- Særlige katergorier af oplysninger (følsomme oplysninger).
- Oplysninger om straffedomme og lovovertrædelser eller tilknyttede sikkerhedsforanstaltninger.
- Almindelige oplysninger.

## Sådan gør vi

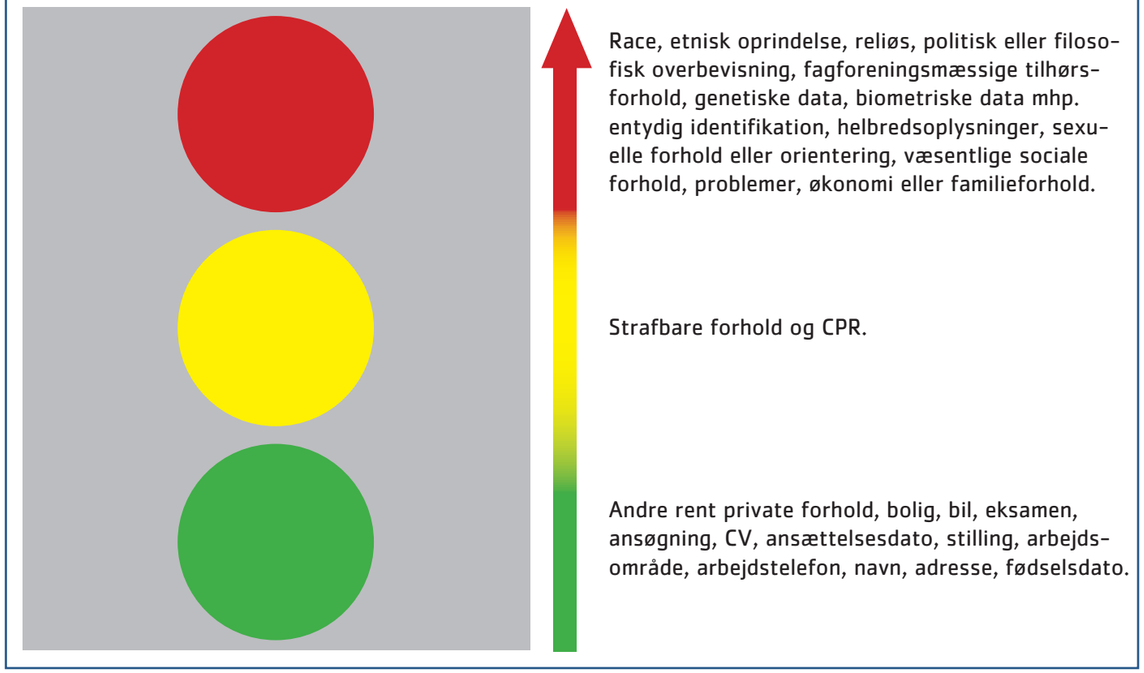
I Broen til Bedre Sundheds Sekretariat arbejder vi med personoplysninger og data, som har forskellige grader af følsomhed. Praksis for hvordan vi behandler oplysningerne varierer derfor, alt afhængig af opgave og projekt.

Figur 1 illustrerer, hvordan vi definerer graden af følsomhed af oplysninger og data, med udgangspunkt i Datatilsynets og PFI's vejledninger.
Hvis man kan koble oplysninger fra den grønne kategori til oplysninger i en gul eller rød kategori, ændrer den grønne oplysning karakter og bliver henholdsvis gul eller rød. Dermed skal oplysningen behandles som følsom.

I tvivlstilfælde anbefaler vi, at man følger vejledningen for følsomme oplysninger; altså den mest restriktive retningslinje for, hvordan oplysningerne skal opbevares og behandles.

Figur 1: Oversigt over oplysninger

Rød: Følsomme personoplysninger. Gul: Oplysninger om strafbare forhold. Grøn: Almindelige personoplysninger.



# Følsomme personoplysninger

## Det siger reglerne

En oplysning er følsom, hvis den ikke egner sig til offentligt kendskab. Det gælder:

- Helbred
- Religion/filosofisk overbevisning
- Seksualitet
- Etnicitet
- Politisk overbevisning
- Fagforeningsmæssige tilhørsforhold
- Strafbare forhold (grænseland)
- Væsenlige sociale problemer
- Interne familie forhold (fx stridigheder, selvmordsforsøg og ulykkestilfælde)

Herudover kan oplysninger om indtægts- og formueforhold, arbejds-, uddannelses- og ansættelsesmæssige forhold også være fortrolige.

Adgang til at indhente og behandle følsomme oplysninger er mere restriktiv end ved almindelige personoplysninger.

## Sådan gør vi

I Broen til Bedre Sundhed arbejder vi ofte med helbredsoplysninger som er særdeles følsomme og skal derfor behandles derefter.

# Strafbare forhold

## Det siger reglerne

Oplysninger om strafbare forhold anses efter Persondataforordningen for almindelige personoplysninger og er særskilt reguleret i databeskyttelsesloven.

## Sådan gør vi

Broen til Bedre Sundhed behandler strafbare forhold og CPR som personfølsomme oplysninger.

# Almindelige personoplysninger

## Det siger reglerne

Almindelige personoplysninger kan være identifikationsoplysninger som f.eks. navn og adresse, oplysninger om økonomi, skat, gæld væsentlige sociale problemer, kundeforhold, familieforhold, tjenstlige forhold, bolig, ansøgning og CV.

## Sådan gør vi

Vi har et ekstra fokus på hvorvidt almindelige personoplysninger kan kobles til følsomme oplysninger, så det bliver nødvendigt også at håndtere de almindelige oplysninger som følsomme.

# Behandling af oplysninger

## Det siger reglerne

Begrebet "behandling" omfatter enhver form for indsamling, registrering, systematisering, opbevaring, søgning, brug/analyse, videregivelse, samkørelse og/eller sletning af oplysninger.

Behandling kan også være offentliggørelse af oplysninger på en hjemmeside eller registrering af oplysninger i et elektronisk sags- og dokumenthåndteringssystem.

## Sådan gør vi

Broens sekretariat håndterer data efter følgende model:

- Følsomme oplysninger må ikke fremgå af Outlook i mere end 30 dage. Når mails med følsomme oplysninger modtages (via sikker e-post), gemmes data på de relevante placeringer (se Bilag 1). Ved oprydning i Outlook skal man kontrollere både indbakke, udgående mails og arkivmapper for korrespondance indeholdende følsomme oplysninger.
- Generelle oplysninger, som let kan kobles med følsommeoplysninger, behandles som værende følsomme og gemmes som angivet i Bilag 1. Herefter slettes mail fra postkasse, og slettet post tømmes.
- Der må ikke gemmes følsomme oplysninger i åbne mapper på O-drev eller i Fics.
- Følsomme oplysninger til brug for tværsektorielle projekter gemmes på projektets Teamsite.
- Billeder og video gemmes i låste mapper på O-drevet.
- Analysekonsulenterne foretager halvårligt tjek af O-drev, Fics samt Broen til Bedre Sundheds postkasse for korrekt dataopbevaring.

Når man behandler personoplysninger, skal man overholde følgende grundlæggende principper:

- *Lovlighed, rimelighed og gennemsigtighed:* Man skal overholde reglerne for behandling af oplysninger og give let tilgængelig information om denne behandling. Det betyder blandt andet, at den person, der behandles oplysninger om, som udgangspunkt skal have oplyst, hvem der er ansvarlig og hvad der er formålet med databehandlingen.
- *Formålsbegrænsning:* Man skal sikre sig, at alle oplysninger kun bliver indsamlet til saglige formål. Der må ikke indsamles oplysninger med den begrundelse, at det måske senere kan vise sig nyttigt at have oplysningerne.

  En vurdering heraf foretages blandt andet ved at bedømme, om indsamlingen sker i forbindelse med løsningen af en opgave, som man som myndighed skal løse.
- *Dataminimering:* Behandlingen af personoplysninger skal begrænses til det, der er nødvendigt for at opfylde formålet.
- *Rigtighed:* Oplysningerne skal være rigtige og ajourførte, og hvis oplysningerne viser sig at være urigtige, skal de som udgangspunkt slettes eller berigtiges.
- *Opbevaringsbegrænsning:* Personoplysninger skal slettes eller gøres anonyme, når det ikke længere er nødvendigt for den dataansvarlige at have oplysningerne.
- *Integritet og fortrolighed:* Oplysninger skal beskyttes mod uautoriseret eller ulovlig databehandling, ligesom det skal sikres, at oplysninger ikke går tabt eller bliver beskadiget. Dette sikres bl.a. gennem adgangskontrol til systemer og backup af data.

# Hjemmel til indsamling og behandling af personoplysninger

## Det siger reglerne

Persondataforordningen nævner en række betingelser for, at man lovligt kan behandle personoplysninger. Det skal f.eks. være tydeligt, hvem der har hjemmel til at indsamle og efterfølgende behandle data.

Der skeldnes mellem tre former for hjemmel;
- Hjemmel via lov.
- Hjemmel via myndighedsudøvelse.
- Hjemmel via samtykke.

Hvis man behandler personoplysninger er man "dataansvarlig" eller "databehandler", alt efter hvilken rolle man har. Og ens hjemmel afhænger af hvilken type oplysninger, der er tale om og af hvorfor oplysningerne skal behandles.

## Ved følsomme personoplysninger

Særlige kategorier af følsomme personoplysninger kan behandles uden samtykke, hvis den registrerede tydeligt selv har offentliggjort samme oplysninger på forhånd.

Særlige kategorier af følsomme oplysninger kan desuden behandles, hvis det er nødvendigt af hensyn til:

- Den dataansvarliges eller den registreredes arbejds-, sundheds-, og socialretlige forpligtelser og rettigheder.
- Den registreredes eller en anden fysisk persons vitale interesser, hvis det er umuligt at give samtykke.
- En politisk, filosofisk, religiøs eller fagforeningsmæssig non-profit organisations behandling af medlemsoplysninger eller regelmæssige kontaktoplysninger. (Omfatter ikke videregivelse uden for organisationen).
- Et retskravs fastlæggelse eller behandling.
- Væsentlige samfundsinteresser.
- Behandling af sundhedsfaglig karakter inden for sundhedssektoren.

Behandling til arkiv, videnskabelige eller historiske forskningsformål eller til statistiske formål.

## Ved strafbare forhold og CPR-numre

Oplysninger om strafbare forhold og CPR må ikke behandles, med mindre det er nødvendigt for at varetage en myndigheds opgave.

Oplysningerne må heller ikke videregives, medmindre:

- Den registrerede har givet sit udtrykkelige samtykke til videregivelsen.
- Videregivelsen sker for at varetage private eller offentlige interesser, der klart overstiger hensynet til de interesser, der begrunder hemmeligholdelse, herunder hensynet til den, oplysningen angår.
- Videregivelsen er nødvendig for at udføre en myndigheds virksomhed eller påkrævet for en afgørelse, som myndigheden skal træffe.
- Videregivelse er nødvendig for at udføre en persons eller virksomheds opgaver for det offentlige.

Offentlige myndigheder kan behandle oplysninger om CPR med henblik på en entydig identifikation eller som journalnummer.

CPR-numre må ikke offentliggøres, medmindre der er givet samtykke.

## Ved almindelige personoplysninger

Almindelige personoplysninger kan behandles uden samtykke, hvis det er nødvendigt af hensyn til:

- En kontrakt.
- Den dataansvarliges retlige forpligtelser.
- Den registreredes eller en anden persons vitale interesser.
- En opgave i samfundets interesse eller offentlig myndighedsudøvelse.
- En legitim interesse, som ikke overgås af den registreredes interesser eller rettigheder.

Det sidste punkt gælder ikke for offentlige myndigheders behandling af personoplysninger, og bør som oftest ikke anvendes ved behandling af personoplysninger om børn.

## Ved særlige former for behandling

En række behandlinger er underlagt særlig regulering i databeskyttelsesloven. Det drejer sig om:

- Retsinformationssystemer (§ 9).
- Behandling med henblik på statistiske eller videnskabelige undersøgelser (§ 10).
- Ansættelsesforhold (§ 12).
- Markedsføring (§ 13).
- Arkiv (§ 14).
- Kreditoplysningsbureauer (§§ 15-21).

Læs mere på datatilsynets hjemmeside.

## Sådan gør vi

Broen til Bedre Sundhed er et tværsektorielt partnerskab, der arbejder med data og oplysninger på tværs af sektorgrænser.

Vores hjemmel ligger i en samarbejdsaftale. Den giver os lov til f.eks. at behandle kommunale data i Broens sekretariat, også selvom Sekretariatets medarbejdere organisatorisk er ansat i Region Sjælland.

Se desuden Bilag 1.

# Samtykke

## Sådan gør vi

I Broen til Bedre Sundhed bruger vi samtykker, når der ikke er hjemmel til databehandling i myndighedsydøvelse, lovgivning eller ved brug til administration.

Samtykker i Broen til Bedre Sundhed skal overholde følgende kriterier, som er i overenstemmelse med de generelle retningslinjer for samtykke:

- De skal være skriftlige.
- De skal være lette at forstå – lav et tjek hos kommunikationskonsulenten.
- De skal være lette at trække tilbage, og der skal foreligge en skriftlig beskrivelse af, hvordan man gør.
- De skal beskrive hvilke oplysninger der bliver indhentet (f.eks. helbredsoplysninger, registre, spørgeskemaer), hvor længe de bliver opbevaret og hvordan de bliver behandlet og anvendt.
- De skal beskrive om oplysningerne præsenteres i anonym eller i pseudonymiseret form.

## Samtykke

Broen til Bedre Sundhed anvender altid skriftligt samtykke, når borgere deltager i vores projekter, for at vi kan efterleve kravet om dokumentation.

Analysekonsulenterne opbevarer alle følsomme data på Broens sikre server eller Teamsites, som kun kan tilgås af medarbejdere med godkendelse.

Data som sendes ud af huset, leveres altid i aggrigeret og anonymiseret form, medmindre den enkelte modtager har tilladelse til at få data udleveret i ikke-anonymiseret form. I så fald vil data blive delt via Teamsite eller sendt med sikker mail.

# Samtykke ved børn

## Det siger reglerne

Som udgangspunkt skal børn være over 15 år, før de kan give samtykke selv. Det afhænger dog altid af en vurdering af modenhed og om der arbejdes efter serviceloven eller sundhedsloven.

Hvis børn og unge ikke selv kan give samtykke, skal deres forældre give samtykke.

Dog må sundhedsplejersker gerne tale med yngre børn uden deres forældres samtykke.

## Sådan gør vi

I Broen til Bedre Sundhed giver forældre samtykke til børn til og med 15 år, medmindre de enkelte projekter har anden hjemmel. I så fald skal dette beskrives og lægges i Fics.

Børn fra 16-17 år giver selv samtykke, men ofte indhenter vi forældrenes samtykke også. Ved tvivl tager vi en jurist med på råd.

## Ved indirekte oplysninger

Indirekte oplysninger indhentes, når vi f.eks. spørger børn om forhold vedrørende deres familiesituation.

Her opstår et potentielt konfliktområde. Som udgangspunkt behandles disse oplysninger som enhver anden følsom oplysning, men ved hvert projekt skal vi overveje, hvorvidt oplysningerne er relevante for projektet, eller det giver bedre mening at spørge forældrene.

## Hvem indhenter samtykke

Som hovedregel er det den dataansvarlige, som indhenter samtykker.

I de tilfælde, hvor sekretariatet er databehandler af kommunale data, er det kommunernes ansvar at indhente samtykker eller sikre at der er anden hjemmel.

Ved projekter som er forankret i Region Sjælland, indhenter Sekretariatet samtykke eller sikrer at der er anden hjemmel.

I de tilfælde, hvor kommunerne videregiver data til Sekretariatet, som beriger data med andre datakilder, overgår dataansvaret til sekretariatet og dermed Region Sjælland. Men det er stadig kommunernes ansvar at indhente samtykke.

# Formålsbegrænsning

## Det siger reglerne

Ifølge Persondatabeskyttelsesforordningens §10 skal der være et specifikt formål med at indhente oplysninger/data, og efterfølgende må disse oplysninger/data kun bruges til det indsamlede formål.

## Sådan gør vi

Broen til Bedre Sundhed må ikke videregive eller anvende data/oplysninger der er indsamlet til ét projekt til andre projekter uden forudgående ansøgning og godkendelse.

Det betyder f.eks. at data, der er indsamlet til forskning kun må bruges til det godkendte projekt, ligesom data, der er indsamlet til ledelsesinformation kun må bruges til ledelsesinformation.

# Databehandleraftaler

## Sådan gør vi

Broen til Bedre Sundhed udarbejder databehandleraftaler i alle tilfælde, hvor data bliver behandlet i en anden organisation, end den der har det juridiske ansvar/er dataansvarlig.

Det er en problematik, der er særlig relevant for Broen, fordi vi arbejder med data på tværs af sektorgrænser. F.eks. ved skolesundhed.dk, hvor data bliver indsamlet i de to kommuner, men bliver behandlet i Broens sekretariatet, der organisatorisk er placeret i Region Sjælland.

Broen benytter enten PFI's vejledninger til databehandleraftaler eller kommunernes skabeloner. Vejledningerne kan fåes ved kontakt til PFI.

Vi udarbejder desuden altid databehandleraftaler, når data bliver flyttet fra en organisation til en anden. Det gælder både internt i vores partnerskab og ved brug af eksterne databehandlere, som f.eks. forskningsinstitutioner.

Ved brug af eksterne databehandlere er vi forpligtet til at kontrollere at de eksterne databehandlere overholder lovivningen. En kontrolfunktion der varetages af Broens analysekonsulenter.

## Det siger reglerne

Der skal indgås databehandleraftaler med de databehandlere, som behandler personoplysninger på den dataansvarliges vegne.

I Persondataforordningen er der nye krav til Databehandleraftalerne (Artikel 28 stk. 3).

Der er pr. maj 2018 indgået følgende databehandler aftaler i Broen til Bedre Sundhed):

- Databehandleraftale Sund Uddannelse – evaluering af Sund Uddannelse. Lolland – og Guldborgsund Kommuner.
- Gælder også evalueringen af Hjernemad.
- Sammen om min vej – Lolland og Guldborgsund Kommuner, tilladelse til udlevering af data til os. Databehandler aftaler omkring tilgåelse af sharepoint.
- Sammen om min vej - SDU.
- Alkohol – databehandler aftaler, kommunale på regionale server. Lolland og Guldborgsund Kommuner.

Kommende aftaler:

- Sammenhængende patientforløb.
- Ledelsesrapport; Skolesundhed.dk/BørnUngeLiv.
- Skolesundhed.dk/BørnUngeLiv – projekter, generel tilladelse.

# Pseudonymisering

## Det siger reglerne

Med en krypteringsnøgle kan CPR-numre parres med deltagerkoder. Når man anvender deltagerkoder istedet for CPR-numre er de enkelte personoplysninger ikke direkte henførbare til et fysisk individ. Det kaldes psedonymisering.

Pseudonymiserede data skal dog fortsat behandles som følsomme oplysninger, da man med en krypteringsnøgle kan låse dem op igen.

De pseudonymiserede data bliver først anonyme, når krypteringsnøglen er slettet og der ikke er andre muligheder for at identificere individet bag de enkelte oplysninger.

## Sådan gør vi

I Broen til Bedre Sundhed behandler vi oplysninger, der er pseudonymiserede via krypteringsnøgler, som følsomme, så længe krypteringsnøglen findes.

Først når data er fuldt anonymiserede og ikke længere kan låses op via en krypteringsnøgle, vil de blive behandlet som "ikke-følsomme" data.

Pseudonymiserede data opbevares på sikre Teamsites. Kun godkendte medarbejdere kan få adgang.

# Anonymisering og sletning af personoplysninger

## Det siger reglerne

Personoplysninger kan anonymiseres, så man ikke længere kan identificere enkelte personer ud fra oplysningerne eller i kombination med andre oplysninger. F.eks. ved at fjerne alle personoplysninger og karakteristika, og slette baggrundsfiler og krypteringsnøgler.

Anonymisering skal være uigenkaldelig. Man skal derfor være opmærksom på, om andre kan være i besiddelse af oplysninger, der gør det muligt at identificere den enkelte. F.eks. hvis de kender målgruppen. En lærer må f.eks. ikke kunne genkende en elev ud fra en case-beskrivelse.

Persondataforordningen sidestiller anonymisering af data med at slette data. På lige fod med overdragelse til Rigsarkivet og fysisk destruktion af papirdokumenter. Fuldt anonymiserede data kan derfor deles frit.

## Sådan gør vi

I Broen til Bedre Sundhed anonymiserer vi altid oplysninger ved ekstern formidling (f.eks. en konference), medmindre borgerne har givet særskildt tilladelse til ikke at være anonyme (f.eks. hvis en projektdeltager deltager i en film).

# Opbevaring, behandling og deling af personoplysninger i Broen til Bedre Sundhed

## Det siger reglerne

Vi skal kunne dokumentere overfor Datatilsynet, at vi har sikret data/personoplysninger med passende tekniske og organisatoriske foranstaltninger, så utilsigtede og/eller ulovlige behandlinger undgås.

Reglerne for opbevaring af data varierer alt efter typen af data (se definition af data).

## Sådan gør vi

### Cloud-løsninger

I Broen til Bedre Sundhed benytter vi Cloud-løsningen Teamsite til at opbevare, udlevere og modtage personoplysninger. Det er en løsning, der anbefales af IT i Region Sjælland.

Vi opbevarer IKKE følsomme personoplysninger i andre cloud-løsninger (som f.eks. dropbox).

### Fics

Fics er Region Sjællands journaliseringssystem. Det kan tilgås af alle medarbejdere med adgang.

I Broen til Bedre Sundhed journaliserer vi derfor kun fuldt anonymiserede oplysninger i FICS. Aldrig følsomme oplysninger.

Vi anvender til gengæld FICS til at journalisere dokumenter, mails m.m., der er relevante i forhold til at overholde vores journaliseringspligt.

### SharePoint Teamsite

Broen til Bedre Sundhed benytter SharePoint Teamsite til at lagre oplysninger til brug i vores projekter. Også følsomme personoplysninger.

Teamsites er en sikker løsning, al adgang bliver logget og det kan tilgås af medarbejdere på tværs af vores partnerskab. Ikke kun fra Region Sjælland. Når man opretter et teamsite, skal man meddele IT, hvilken type oplysninger det skal rumme (almindelige eller følsomme) og hvem der skal have adgang (interne eller eksterne medarbejdere).

### Server

Broen til Bedre Sundhed har en server, der kan håndtere store mængder data, af både almindelig og følsom karakter.

Den blev oprettet som et led i projektet Sammen om min vej og kan kun tilgås af Broen til Bedre Sundheds analysekonsulenter og driftspersonale fra IT.

For at sikre, at IT's driftspersonale ikke kan tilgå de enkelte oplysninger, er alle data imellem opdateringsfaserne lagt i en zipmappe med kode. De bliver låst op ved indlæsning, men bliver derefter inzippet igen.

Serveren rummer seperate mapper for de respektive projekter under Broen til Bedre Sundhed og anvendes, når eventuelle følsomme personoplysninger skal analyseres.

Det er kun de medarbejdere, som har lov til at tilgå projekt-data (jf. dataaftaler/godkendelser), som har adgang til den pågældende mappe med data på serveren. Adgangen ophører ved projektafslutning og/eller ansættelsesophør.

Eksterne samarbejdspartnere kan få adgang til data, hvis der bliver indgået en databehandleraftale. F.eks. har vi en ekstern databehandler tilknyttet databasen fra Sammen om min vej. Adgangen ophører ved projektets afslutning.

### SurveyXact til dataindsamling

Broen til Bedre Sundhed benytter det elektroniske spørgeskema-værktøj SurveyXact til at indsamle data.

Ved indtastning af oplysninger benyttes deltager-id (peseudonimiseret data). Krypteringsnøglen med deltager-ID og CPR opbevares i Teamsite og på Broens server.

Når dataindsamlingen er slut, trækkes data ud

og gemmes i projekternes mappe på serveren eller projektets teamsite, hvorefter data i SurveyXact-programmet slettes.

## Oplysningerne på papir

Broen til Bedre Sundhed tilstræber ikke at have følsomme personoplysninger i papirformat.

Når det alligevel forekommer, vil papirerne blive opbevaret i aflåste skabe/skuffer og destrueres efter brug.

Proceduren skal beskrives i datagodkendelsen for projekterne.

## Sikker E-mail

Når vi sender følsomme personoplysninger, som f.eks. datasæt til database-opbygning, benytter vi sikker E-mail.

Data bliver herefter lagt på vores server eller Teamsite og efterfølgende slettet fra vores mailbokse.

## E-mails indenfor partnerskabet

E-mails afsendt mellem to mailadresser i samme organisation er sikre. De må derfor gerne bruges til at afsende følsomme personoplysninger.

Mails skal efterfølgende slettes indenfor 30 dage.

## Databearbejdning i statistikprogrammer

Broen til Bedre Sundhed benytter flere forskellige programmer til at analysere data. Disse programmer lagrer midlertidige filer på computeren, mens de arbejder.

Filerne er ikke tilgængelige bagefter, og vores brug af statistikprogrammerne er derfor i overensstemmelse med praksis i resten af Region Sjælland.

Broens analysekonsulenter holder sig løbende opdateret om denne praksis, ved at deltage i det regionale datasikkerhedsnetværk.

## Sociale medier

Broen til Bedre Sundhed benytter sociale medier på overordnet plan (f.eks. Broen til Bedre Sundheds sider på Facebook og Linkedin) og på projektniveau (f.eks. Sund Uddannelse), ligesom vi har interne medarbejder-grupper.

Følgende er Broen til Bedre Sundheds retningslinjer for brug af billeder og film på de sociale medier:

- Stemningsbilleder og film af borgere/brugere (f.eks. ved en event eller konference) må behandles frit, hvis blot deltagerne har fået en generel information om, at der vil blive taget billeder/film. F.eks. med et skilt ved indgangen eller som tekst i en invitation forud for den enkelte event).
- Billeder, film og beskrivelser hvor det enkelte individ udgør den primære del af et foto/film, kræver tydeligt samtykke, hvor det præciseres hvad billederne må bruges til og hvor længe.
- Billeder af medarbejdere i Broen deles frit, under forudsætning af mundtligt samtykke ved ansættelse. Hvis samtykket skal trækkes tilbage er det medarbejderens ansvar at give besked til resten af Broen til Bedre Sundhed.

# Egenkontrol

## Sådan gør vi

Broen til Bedre Sundhed skal dokumentere at vi behandler personoplysninger korrekt og vi har pligt til at kontrollere eksterne samarbejdspartneres behandling af vores data.

I praksis sker det efter følgende model:

- Broens analysekonsulenter udfører halvårligt en elektronisk kontrol, hvor både interne og eksterne projektledere og databehandlere bliver bedt om at udfylde en erklæring og en tjekliste, der viser hvordan man håndterer oplysninger. Begge dokumenter skal underskrives og sendes retur til analysekonsulenterne.

  Erklæring og tjekliste er under udarbejdelse.

- En gang årligt foretager analysekonsulenterne et internt tilsyn ved fysisk fremmøde i projekterne.

Al korrespondance journaliseres i Fics: Broen – Egen Kontrol.

### Det siger reglerne

I Persondataforordningen skal dataansvarlige foretage og dokumentere egenkontrol af både egen praksis samt af eksterne databehandlere.

Hvis reglerne ikke bliver overholdt, kan analysekonsulenterne udstede et påbud. Hvis påbudet ikke bliver fulgt hurtigt, vil adgang til data blive lukket.

Kontrol af log-filer i Teamsites og på Broens server:

På Broen til Bedre Sundheds server og alle Teamsites registreres aktiviteter i log-filer. Her er det dokumenteret, hvem der har haft adgang og hvornår.

Logfilerne bliver løbende tjekket af Region Sjællands IT afdeling. Uvedkommende adgang bliver håndteret af Region Sjællands IT-afdeling.

# 5. Nyttige links og referencer

- Europa/Parlamentets og Rådets forordning (EU, 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse) (EØS/relevant tekst): www.kortlink.dk/u55b.
- EU reform af data, 2018: www.kortlink.dk/u556.
- EU, GDPR org: www.kortlink.dk/u558.
- Brud på persondatasikkerheden. Datatilsynet. www.kortlink.dk/u533.
- Databeskyttelsesforordning og arbejdet med compliance, Oplæg af Kammeradvokaten, Temadag om Datasikkerhed 20. april 2017: www.kortlink.dk/u3xf.
- Datatilsynet, databeskyttelse generelt: www.kortlink.dk/u554.
- PFI, Region Sjælland, vejledning: www.kortlink.dk/u555.
- Region Sjaelland IT-infrastruktur vejledninger: www.kortlink.dk/u534.
- Datatilsynet – vejledning i DPO: www.kortlink.dk/u55e.
- Datatilsyn – Vejledning i Samtykke, november 2017: www.kortlink.dk/u55a.

Broen til Bedre Sundhed
Maj 2018

Region Sjælland
Alleen 15
4180 Sorø

www.regionsjaelland.dk/broen
broen@regionsjaelland.dk