

# Håndbog i beskyttelse af persondata for de folkevalgte



# Hvorfor er beskyttelse af persondata vigtig?

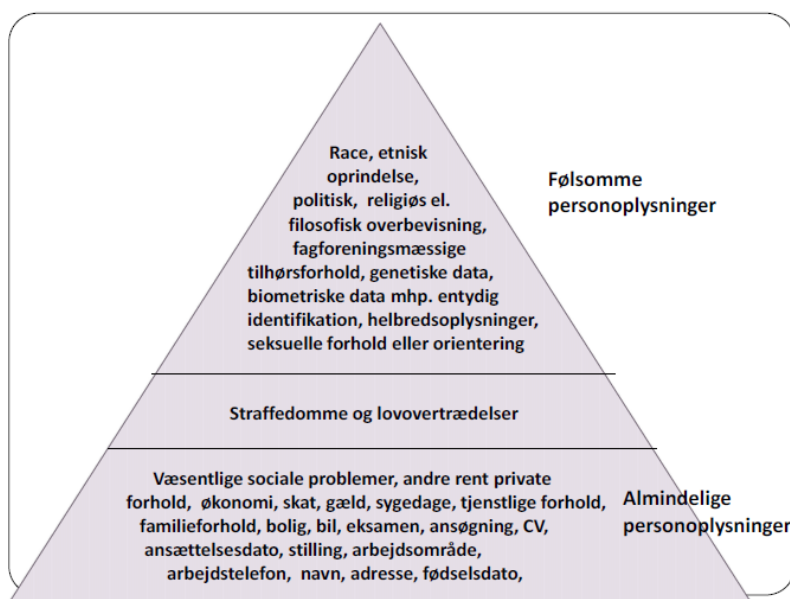
**P**ersondata er dine og mine personlige oplysninger.

Datatilsynets definition på en personoplysning er: Enhver form for information om en identificeret eller identificerbar fysisk person, også selv om personen kun kan identificeres, hvis oplysningen kombineres med andre oplysninger.

Personoplysninger kan for eksempel være personnumre, registreringsnumre, et billede, et fingeraftryk, en stemme, lægejournaler eller biologisk materiale, når det i praksis er muligt at identificere en person ud fra oplysningerne eller i kombination med andre. Man siger, at oplysningen er "personhenførbart".

Databeskyttelsesforordningen opdeler personoplysninger i tre typer:

- Almindelige oplysninger
- Oplysninger om straffedomme og lovovertrædelser
- Særlige kategorier af oplysninger (følsomme oplysninger)



Figur 1: En anden måde at se de forskellige kategorier af personoplysninger på. Jo højere oppe i trekanten oplysningerne er, desto strengere betingelser for at behandle dem.

Opdelingen findes, fordi der gælder forskellige betingelser og procedurer for behandling af personoplysninger afhængig af oplysningernes følsomhed.

Du kan læse mere om personoplysninger og hvordan de skal behandles på <https://www.datatilsynet.dk/generelt-om-databeskyttelse/hvad-er-personoplysninger/> .

Personoplysninger skal vi sørge for at passe rigtig godt på, så uvedkommende personer ikke kan læse med og tilegne sig viden de ikke er berettiget til.

Som folkevalgt i en boligorganisationen støder man hovedsageligt på persondata i forbindelse med kontakten til de andre beboere i afdelingen og i kontakt med medarbejdere i boligorganisationen.

De regler, vi alle er underlagt, findes i Databeskyttelsesforordningen og Databeskyttelsesloven og i Datatilsynets vejledninger og retningslinjer. Den 25. maj 2018 kom der helt nye regler som betyder ændringer i lovgivningen for persondatabeskyttelse.

Det vigtigste for dig er dog at vide, at du kan gøre nogle ganske få ting i hverdagen, der kan have stor betydning.

Mange af tingene gør du måske i forvejen, men med denne lille håndbog får du nogle gode metoder til at beskytte persondata.



# Indledning

**D**e nye regler er trådt i kraft den 25. maj 2018.

Databeskyttelsesforordningen er en forordning der er fælles for alle EU landene, og som alle EU landene skal følge.

Databeskyttelsesloven (den tidligere persondataloven) er et tillæg til databeskyttelsesforordningen og som er vedtaget af regeringen og dronningen. Databeskyttelsesloven er strammet i forhold til tidligere lov og bøderne for ikke at overholde loven er blevet betragteligt højere end de har været tidligere.

Boligselskabet har altid været meget omhyggelig med behandling af persondata, men med den nye lov er det derfor endnu mere vigtigt, at vi alle tænker over hvad vi skriver og hvordan vi behandler oplysninger i forhold til databeskyttelsesloven.

Vi har alle et fælles ansvar, såvel bestyrelser som medarbejdere, til at overholde loven og ikke offentligt ”pege fingre” eller oplyse om information som endnu ikke er offentligt.



Databeskyttelses-  
forordningen

I denne håndbog er samlet 11 overordnede metoder til at beskytte persondata i hverdagen.

Emnerne i håndbogen er:

- God databehandlingssskik
- Skærm- og skrivebords politik
- Dine adgangskoder
- Låse dokumenter inde
- Elektronisk arkiv
- E-mail
- Bortskaffelse af dokumenter
- Sikkerhedsbrud
- Hjemmeside og andre digitale platforme
- Hvis du er i tvivl
- Henvisninger

På de følgende sider bliver de 11 emner beskrevet i detaljer. Det kan forhåbentlig hjælpe dig til at tænke persondatabeskyttelse med ind i hverdagen i dit arbejde i bestyrelsen.



# God databehandlingskik





**D**en gode databehandlingskik er beskrevet i

Databeskyttelsesloven. Kort fortalt går den ud på, at man skal respektere og beskytte de personoplysninger, man arbejder med. Den gode databehandlingskik dækker over følgende begreber:

- **Sagligt formål:** Du skal have en reel 'god grund' til at arbejde med personoplysningerne.
- **Nødvendighed:** Du må kun arbejde med persondata, hvis det er nødvendigt for at udføre den opgave du er sat til at løse.
- **Proportionalitet:** Der skal være ligevægt mellem det arbejde, du skal udføre og de oplysninger, du bruger.
- **Rigtige oplysninger:** Den person, vi behandler oplysninger på, har krav på, at de er korrekte – sørg derfor altid for at rette og opdatere oplysninger, så vidt det er muligt.
- **Beskyt enkeltpersoner:** For at beskytte beboere og personale (jmf. Lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesloven)), vil vi ikke tillade at der bliver skrevet personer ved navns nævnelse i referater o.l. som skal offentliggøres. Der må heller ikke henvises til situationer, hvor enhver kan ledes frem til enkelt personer. Her skal man skrive f.eks. administration, boligselskabet, driften o.l.

# Skærm- og skrivebordspolitik

**D**in skærm er et digitalt stykke "papir" og det er vigtigt at de oplysninger der er på skærmen ikke bliver videregivet til andre.

- **Låste skærme:** For at beskytte de data man har på sin computer, skal man altid, sætte skærmlås med kode på sin computer når man forlader den. Dette for at ingen uvedkomne kan gå ind og trække/læse data fra din computer uden at du selv ved dette. Man kan aktivere skærmlås ved at trykke på  +  =  (Windows tasten + L). Når man skal tilbage og arbejde, trykker man på  (Esc) og taster sin kode ind.

- **Aktive skærme:** For at beskytte de data man har på sin computer, skal man altid gøre hvad man kan for, at andre ikke kan se de oplysninger der er på din skærm når du sidder og behandler persondata. Luk skærbilledet ned når du taler med en anden person. Dette er specielt vigtigt ved skranken, men samtidigt også vigtigt ved alles skriveborde.

- **Dit skrivebord:** Når der kommer en person hen til dit skrivebord skal du altid lige tjekke hvad du har liggende og evt. vende papirer, samt lukke skærbilleder ned hvor der er personoplysninger på.



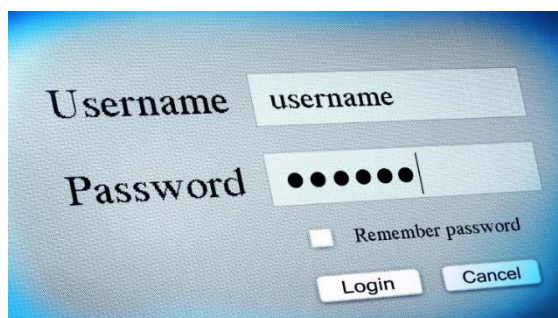
# Dine adgangskoder

**D**ine adgangskoder til computer, iPad, telefon osv. er dine - og kun dine, hvis du har personoplysninger på disse enheder i forbindelse med dit bestyrelsesarbejde. Derfor skal du gøre alt for at passe på dem og sørge for, at andre ikke får fat i dine koder.

Det nemmeste er jo at kunne koden i hovedet, men da det jo ikke er en selvfølge, at man kan det, skal man sørge for et godt alternativt gemmested.

3 gode råd med på vejen:

- Giv aldrig din adgangskode til andre – skal de have adgang til et system, skal de selv have en kode.
- Koden må aldrig ligge et frit tilgængeligt sted – eksempelvis nedskrevet på et papir, der er offentligt tilgængeligt.
- En lap papir med koden under tastaturet eller musemåttten er ikke et godt gemmested.





# Husk at låse dokumenter inde der indeholder personoplysninger

**E**r du en af dem, der nogen gange printer dokumenter, der indeholder personoplysninger?

Så skal du huske at tage nogle forholdsregler:

- Dokumenter i papirform må aldrig ligge frit fremme på dit skrivebord eller andre steder i lejligheden, når du ikke er til stede.
- Dokumenter af fortrolig art skal altid låses inde eller gemmes forsvarligt, når du forlader dem.
- Husk at opbevare nøglen til skuffen eller skabet et forsvarligt sted, som andre ikke har adgang til.

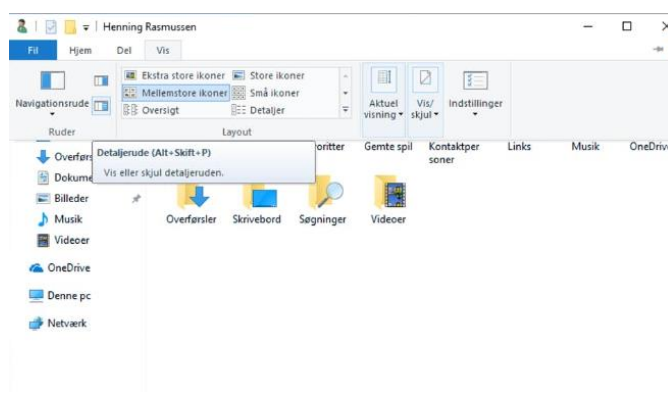


# Når du skal gemme dokumenter i et elektronisk arkiv

**A**t gemme dokumenter i et elektronisk arkiv (eller system) er næsten det samme som med dokumenter i papirform - bare på computeren.

Husk derfor:

- Hvis der er tale om et elektronisk drev, så husk altid at gemme på et lukket drev, som kun du har adgang til.
- Hvis der er en ekstern harddisk, skal denne opbevares forsvarligt.
- Hvis det er et system med adgangskoder – så husk de generelle gode råd under punktet ”dine adgangskoder”.



# Når du skal sende oplysninger videre...

**H**vis du skal sende personoplysninger videre elektronisk, er det meget vigtigt, at du tænker over, hvordan og til hvem, du sender dem. Husk altid princippet om god databehandlingskik.

- E-mails til privatperson er ikke beskyttet – husk derfor altid at slette personoplysninger, hvis du skal sende en almindelige e-mail.
- Send aldrig for meget information – hvis du eksempelvis skal sende en fødselsdato, er der ingen grund til at sende et CPR nummer. Husk altid princippet om proportionalitet.
- Tænk over hvad du skriver i en mail.
- Sender du mail til flere modtagere, så sæt dig selv under til og sæt alle de andre modtagere under BCC



# Bortskaffelse af fortrolige dokumenter

**N**år du skal skille dig af med fortroligt papirmateriale, hvad enten det indeholder personoplysninger eller ej, er det ikke bare lige at smide det ud i den almindelige skraldespand til papir.

Papirer med fortrolige oplysninger eller persondata på papir, skal bortskaffes på korrekt vis. Det kan man på to forskellige måder:

- En makuleringsmaskine, så man selv kan makulere dokumenterne med det samme.
- Har man ikke en makuleringsmaskine, skal man rive papiret så meget i stykker at man ikke kan genskabe det.

Korrekt bortskaffelse af personoplysninger er lige så vigtigt som korrekt opbevaring.



# Sikkerhedsbrud

**E**t sikkerhedsbrud også kaldt persondatabrud, er et brud på sikkerheden, der gør at persondata bliver tilgængelige for andre end de personer der har lov til at arbejde med dem.

Vi har som virksomhed 72 timer til at melde et brud videre til datatilsynet, fra vi opdager bruddet.

Eksempler på persondatabrud kan være:

- Glemmer du din telefon, et usb-stik, din iPad e.l. et sted, og der er fare for at andre har kunnet tilegne sig viden de ikke skulle have, er dette et brud.
- Hvis I ved en fejl kommer til at sende en mail til forkert person og der er persondata beskrevet i mailen, er dette et brud.
- Bliver der indbrud i din bil eller i dit hjem og din computer, iPad, telefon o.l. bliver stjålet, og der er risiko for at andre tilegner sig viden de ikke skulle have, er dette et brud.
- Forsvinder der et dokument som indeholder persondata, har nogen været inde på din computer uden opsyn osv., er dette et brud.
- Dette er bare nogle eksempler på hvad et brud kan være.

Ved en hver tvivl om sikkerhedsbrud, skal du kontakte Palle Andersen, Hilde Hansen eller ledelsen for boligselskabet, så vi kan få klarlagt om der er en risici forbundet med bruddet.

# Hjemmeside og andre digitale platforme

**D**en digitale verden vi lever i, har gjort det meget nemt at distribuere viden rundt til mange mennesker på meget kort tid. Dette stiller også nogle krav til os som boligselskab og som mennesker.

Det skrevne ord er magtfuldt og det stiller større krav til hvad vi skriver og distribuerer – også på boligselskabets hjemmeside og andre digitale platforme.

Vi skal sikre os at det vi skriver om:

- er faktisk rigtigt.
- er sagligt.
- har et formål.
- skal være almen viden.
- ikke skal hænge enkeltpersoner ud.

Vi skal tænke personbeskyttelse i alt det vi skriver, men samtidig skal vi kunne informere om alt det der er vigtigt for boligselskabet.



## Hvis du er i tvivl



**H**vis du har spørgsmål til denne håndbog eller et hvilket som helst andet emne inden for beskyttelse af persondata, skal du henvende dig til Sundby-Hvorup Boligselskab – de vil prøve at svare på dine spørgsmål og giver et godt råd med på vejen.

Hilde Hansen, kan kontaktes på mail: [hh@sundbyhvorup.dk](mailto:hh@sundbyhvorup.dk) eller pr telefon på telefon nr. 98 17 30 66.

Palle Andersen, kan kontaktes på mail: [pas@sundbyhvorup.dk](mailto:pas@sundbyhvorup.dk) eller pr telefon på telefon nr. 98 17 30 66.

## Henvisninger

**H**ar du lyst til selv at finde yderligere information omkring beskyttelse af persondata? Så kan du med fordel besøge [www.datatilsynet.dk](http://www.datatilsynet.dk) – her kan du finde link til både Databeskyttelsesloven og Databeskyttelsesforordningen, og læse om de nye regler og meget, meget mere.

Der kan se en hel del vejledninger hvis du går ind på:

[www.datatilsynet.dk/generelt-om-databeskyttelse/vejledninger-og-skabeloner/](http://www.datatilsynet.dk/generelt-om-databeskyttelse/vejledninger-og-skabeloner/)

og på

[www.sundby-hvorupboligselskab.dk/om-boligselskabet/haandtering-af-persondata.aspx](http://www.sundby-hvorupboligselskab.dk/om-boligselskabet/haandtering-af-persondata.aspx)





Sundby-Hvorup Boligselskab

Lindholm Søpark 4

9400 Nørresundby

Tlf.: 98 17 30 66

E-mail: [info@sundbyhvorup.dk](mailto:info@sundbyhvorup.dk)

[www.sundby-hvorupboligselskab.dk](http://www.sundby-hvorupboligselskab.dk)

Redigeret: 04-03-2022