Håndbog i beskyttelse af persondata for kontorpersonalet

SUNDBY-HVORUP Boligselskab

Hvorfor er beskyttelse af persondata vigtig?

Persondata 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.

Dem skal vi sørge for at passe rigtig godt på, så uvedkommende personer ikke kan læse med. Som medarbejder i en boligorganisationen støder man hovedsageligt på persondata i arbejdet med enten andre medarbejderes, kunders og beboeres personlige oplysninger.

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

De nye regler er trådt i kraft den 25. maj 2018 og Databeskyttelsesloven er strammet og bøderne for ikke at overholde loven er blevet betragteligt højere end de har været tidligere. Det er 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 medarbejdere som samarbejdspartnere og beboere, til at overholde loven.

I denne håndbog er samlet 16 overordnede metoder til at beskytte persondata i hverdagen. Emnerne i håndbogen er:

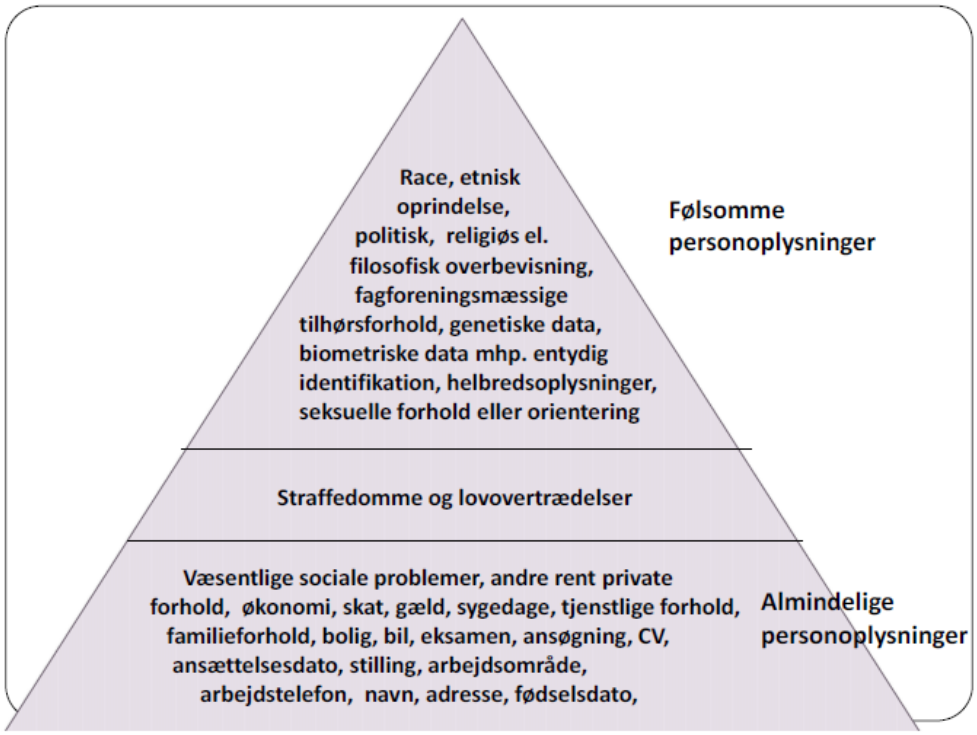
- Hvad er personoplysninger?
- God databehandlingsskik
- Skærm- og skrivebords politik
- Udskrivningspolitik
- Dine adgangskoder
- Låse dokumenter inde
- Elektronisk arkiv
- E-mail
- Bortskaffelse af dokumenter
- Kommunikation med beboere, medarbejdere m.m.
- Sikkerhedsbrud
- Hjemmearbejdsplads og under transport
- Hjemmeside og andre digitale platforme
- Hvordan agerer man udenfor kontoret i embedets medfør?
- Hvis du er i tvivl
- Henvisninger

På de følgende sider bliver de 16 emner beskrevet i detaljer. Det kan forhåbentlig hjælpe dig til at tænke person-databeskyttelse med ind i hverdagen på din arbejdsplads.

Hvad er personoplysninger?

Personoplysninger er enhver form for information, der kan henføres til bestemte personer, også selv om dette forudsætter kendskab til et personnummer, registreringsnummer eller lignende. Også oplysninger i form af f.eks. et billede eller et fingeraftryk er personoplysninger.

Forordningen sondrer mellem følsomme og almindelige personoplysninger.



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.

Begrebet ”behandling” omfatter enhver form for håndtering af personoplysninger. Det er først og fremmest elektronisk behandling af oplysninger, der er omfattet af reglerne. Det kan f.eks. være indsamling, registrering, systematisering, opbevaring, søgning, brug, videregivelse eller sletning af oplysninger.

God databehandlingsskik

Den gode databehandlingsskik er beskrevet i Databeskyttelsesloven. Kort fortalt går den ud på, at man skal respektere og beskytte de personoplysninger, man arbejder med. Den gode databehandlingsskik 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 dit arbejde.

● **Proportionalitet:** Der skal være ligevægt mellem det arbejde, du skal udføre og de oplysninger, du bruger.

● **Rigtige oplysninger:** Den person, vi behandler oplysninger om, 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 medarbejdere og beboerne *(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. Dog må man godt, når det har et sagligt formål og er nødvendig for sagen.

Skærm- og skrivebordspolitik

Din 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 skærmbilledet 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 skærmbilleder ned hvor der er personoplysninger på. Dette er specielt vigtigt ved skranken, hvor der kommer mange mennesker ind i åbningstiden, men det er også vigtigt på alle andre skriveborde.

Når du forlader din plads, skal du altid vende papirer om som kan indeholde personfølsomme oplysninger og når du forlader arbejdspladsen skal disse være låst inde.

Husk at rydde dit skrivebord når du forlader arbejdspladsen.

Udskrivningspolitik

Dine udskrifter kan ofte indeholde persondata og det er derfor vigtigt, at disse udskrifter bliver passet ekstra godt på.

Boligselskabet har derfor investeret i nye printere med en SafeQ løsning. Dette betyder, at alt hvad man printer for eftertiden bliver lagret i en virtuel ”sky” og bliver først printet, når du sætter din brik på printeren eller taster din 4 cifret kode. Nu kan man selv vælge, om man vil udskrive alle de dokumenter, man har sendt til print, eller om man kun vil udskrive det dokument, man lige skal bruge nu. Dette betyder også, at man ikke behøver, at printe dokumenterne før man skal bruge dem, så de kommer ikke til at ligge på ens skrivebord, indtil man har tid til at viderebehandle dem.

Ved at man enten skal sætte sin brik på maskinen eller taste en 4 cifret kode for at blive identificeret, vil der aldrig ligge dokumenter med personoplysninger i printeren, uden at den medarbejder, der har printet det er tilstede.

Dokumenterne vil automatisk blive slettet efter en uge, hvis du ikke sætter dine dokumenter til print.

Når du har printet dine dokumenter, slettes de fra ”skyen”.

Dine adgangskoder

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

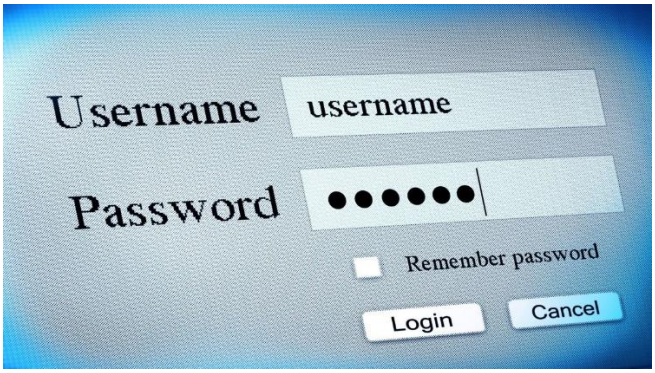
Det nemmeste er jo at kunne koden i hovedet, men da det jo ikke er en selvfølge, at man kan det, skal man sørge for et godt alternativt gemmested.

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 musemåtten er ikke et godt gemmested.



Husk at låse dokumenter inde

Er 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, når du forlader din plads. Hvis du stadig er ved at arbejde med dem, så læg dem med teksten ned mod bordpladen, så man ikke umiddelbart kan læse hvad der står.

● Dokumenter med personoplysninger skal altid låses inde, når du forlader arbejdspladsen.

● 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

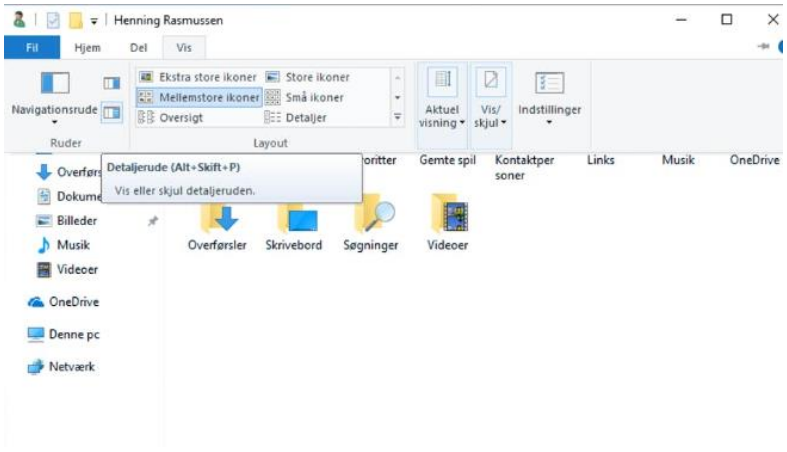
At gemme dokumenter i et elektronisk arkiv (eller system) er næsten det samme som med dokumenter i papirform - bare på computeren.

Husk derfor:

● Hvis der er tale om et elektronisk drev, så husk altid at gemme på et lukket drev, som kun du (evt. dine kollegaer) 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…

Hvis 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 databehandlingsskik.

● E-mails til privatperson er ikke beskyttet – husk derfor altid at slette unødvendige 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

Når 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, skal bortskaffes på korrekt vis. Det kan man på tre forskellige måder:

● På kontoret i Lindholm Søpark er der opstillet blå containere med hængelås, hvor man kan bortskaffe papirer med personoplysninger på.

● En makuleringsmaskine (har vi ude på Ejendomsmester kontorene og i Kvarterets Hus), 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 eller kontakte kontoret for at få en makuleringsmaskine.

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

Kommunikation med beboerne, medlemmer og samarbejdspartnere.

Når du kommunikerer med en anden person, kan dette ske på mange måder (direkte samtaler, pr. telefon, pr. post og pr. mail). Fælles for dem alle er, at der er nogle ting man skal sikre sig inden man kommunikerer med personen.

- Spørg ind til eller tjek en ekstra gang hvem de er.
- Ikke oplys personlige ting om en person, hvis du er i tvivl om, at det er den rigtige person du taler med, med mindre personen har en fuldmagt.
- Hvis en person ringer herind eller kommer ved skranken og du er i tvivl om, at det er den rette person, skal man lade være med at oplyse noget på stedet men sige, at man sender det via mail eller brev.

Sikkerhedsbrud

En hver form for sikkerhedsbrud skal tages alvorligt.

Når databeskyttelsesforordningen finder anvendelse i Danmark og resten af EU fra den 25. maj 2018, vil der – som noget nyt – gælde en generel forpligtelse for alle dataansvarlige til som udgangspunkt at anmelde brud på persondatasikkerheden til Datatilsynet. Anmeldelsen skal ske uden unødig forsinkelse og om muligt senest 72 timer, efter at den dataansvarlige er blevet bekendt med bruddet. Samtidig fastsættes der en forpligtelse, som allerede i dag tolkes ud af persondatalovens grundregel om god databehandlingsskik og Datatilsynets praksis, til som udgangspunkt at underrette de registrerede i tilfælde af brud på persondatasikkerheden.

Begge forpligtelser er udtryk for databeskyttelses-forordningens fokus på ansvarlighed, når det kommer til at overholde databeskyttelsesreglerne. Reglerne har til formål at tilvejebringe gennemsigtighed og især at sikre, at dataansvarlige reagerer, når der opstår et brud på persondatasikkerheden.

“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 på anden måde behandlet.”

Som eksempler på brud på persondatasikkerheden kan nævnes:

1. Andre personer end den eller de personer hos dataansvarlige, der er autoriseret til det, får (uautoriseret) adgang til personoplysninger. Det kan både være personer uden for eller inden for dataansvarliges organisation.
2. Den dataansvarliges medarbejdere ændrer eller sletter personoplysninger ved et uheld.
3. Brud på den dataansvarliges server, hvor uvedkommende har fået indsigt i personoplysninger – f.eks. kundedatabasens CPR-oplysninger, kreditkortoplysninger el.lign.
4. Den dataansvarliges medarbejdere videregiver ubevidst eller bevidst personoplysninger om en borger/kunde til en anden borger/kunde – eller måske ligefrem flere andre uvedkommende personer.
5. Når manglende kryptering af den dataansvarliges hjemmeside indeholdende f.eks. et kundelogin resulterer i, at en eller flere uvedkommende får direkte adgang til kundens personoplysninger.
6. 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.
7. 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.
8. 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.
9. Forsvinder der et dokument som indeholder persondata, har nogen været inde på din computer uden opsyn osv., er dette et brud.

10. Dette er bare nogle eksempler på hvad et brud kan være. Ved den mindste tvivl skal du kontakte ledelsen, Palle Andersen eller Hilde Hansen.

Som udgangspunkt skal alle brud på persondata-sikkerheden anmeldes til Datatilsynet. Det er således kun, hvis det er ***usandsynligt****, at bruddet på persondata-sikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder, at der ikke skal ske anmeldelse.*

Hvad er de mulige konsekvenser af et brud på persondatasikkerheden?

I databeskyttelsesforordningen er nævnt en række eksempler på, hvilke konsekvenser et brud på datasikkerheden kan have for fysiske personer.

Et brud kan, hvis det ikke håndteres på en passende og rettidig måde, påføre fysiske personer fysisk, materiel eller immateriel skade, såsom tab af kontrol over deres personoplysninger eller begrænsning af deres rettigheder, forskelsbehandling, identitetstyveri eller –svig, finansielle tab, uautoriseret ophævelse af pseuddonymisering, skade på omdømme, tab af fortrolighed for oplysninger, der er omfattet af tavshedspligt, eller andre betydelige økonomiske eller sociale konsekvenser for den berørte fysiske person.

Hvad gør du i praksis?

- Hvis du har mistanke om, at der er sket et sikkerhedsbrud, skal du omgående uden unødvendige forsinkelser, kontakte Palle Andersen eller Hilde Hansen. Hvis du ikke kan få fat i os, så kontakt ledelsen og forklare hvad der er sket og evt. om der kan være personer der kan være berørt. Den du taler med, skal have en kort skriftlig rapport omkring hvad der er sket. Rapporten skal indeholde følgende oplysninger:
  - Dato og tidspunkt for bruddet.
  - Hvad er der sket?
  - Årsag til bruddet?
  - Hvilke typer personoplysninger er berørt?
  - Hvilke konsekvenser har bruddet for de berørte personer?
  - Hvilke afhjælpende foranstaltninger er truffet?
  - Er der sket underretning af de berørte personer?
    - Hvis JA, hvorfor?
    - Hvis NEJ, begrundelse for ikke at underrette de berørte personer?

- Vi vurderer sikkerhedsrisici. Boligselskabet skal efter forordningen dokumentere alle sådanne brud på persondatasikkerheden. Med mindre det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder

eller frihedsrettigheder, skal vi endvidere anmelde bruddet til den relevante tilsynsmyndighed inden for 72 timer efter bruddet er opdaget. Sker der forsinkelser, skal disse dokumenteres. De 72 timer tæller fra man bliver opmærksom på sikkerhedsbruddet.

- Hvis det er sandsynligt, at der har været brud på personers rettigheder og det kræver en indberetning, skal Palle Andersen eller Hilde Hansen, der har adgang til systemet, indberette en sikkerhedshændelser for boligselskabet (dog vil Rikke Naur Dybdahl og Vibeke Kristensen være backup). Alle er instrueret i hvad de skal gøre.

- Når sagen er indberettet skal der skrives en rapport og lægges i mappen for DATASIKKERHED.

Hjemmearbejdsplads og under transport

Hvis du ind i mellem arbejder hjemmefra, skal du tage nogle forhåndsregler med hensyn til sikkerheden.

- Vær sikker på, at du har en forsvarligt krypteret router. (som udgangspunkt har de fleste routere brugernavn og password: admin / admin. Dette skal laves om til noget der ikke umiddelbart kan spores.)
- Lad aldrig din computer være tændt når du ikke sidder ved den (som minimum skal der være aktiveret pauseskærm på computer med kode).
- Hvis du har dokumenter med hjem med personoplysninger eller andre følsomme oplysninger, skal disse opbevares forsvarligt.
- Lad aldrig boligselskabets ”ejendele” ligge frit frem i bilen eller i en cykelkurv, hvis du forlader denne. Gem det i bagagerummet hvis du er i bil eller tag det med dig.

Hjemmeside og andre digitale platforme

Den 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 faktuelt 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.

Hvordan agerer man udenfor huset i embedets medfør?

Vi er alle fra tid til andet udenfor huset til møder, kursus, receptioner, på besøg ved beboerne osv.

Til møder, kursus og receptioner skal man altid huske, at man ikke skal omtale identificerbare personer i andres påhør. Dog skal man stadig kunne tale om almindelige og relevante ting. Det kan være hvem der sidder med forskellige opgaver i firmaet, hvem der lige er blevet ansat osv., men ikke personfølsomme oplysninger.

Er man ude ved en beboer, taler man ikke om andre beboere, med mindre det er relevant for den opgave man er ude for at udføre. Når man forlader boligen, fortæller man kun om det man har set eller hørt hvis det har relevans for ens kollegaer eller andre myndigheder.

Hvis du er i tvivl?

Hvis 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.

Det er ikke sikkert man kan svare med det samme, men så vil man undersøge og vende tilbage.

Administration og drift delen:

Palle Andersen, kan kontaktes på pas@sundbyhvorup.dk

Hilde Hansen, kan kontaktes på hh@sundbyhvorup.dk

Personale delen:

Mette Boesen, kan kontaktes på mb@sundbyhvorup.dk

Henvisninger

Har du lyst til selv at finde yderligere information omkring beskyttelse af persondata? Så kan du med fordel besøge www.datatilsynet.dk – her kan du finde link til både Databeskyttelsesloven og Databeskyttelses forordningen, læse om de nye regler og meget, meget mere.

Der er en hel del vejledninger hvis du går ind på:

https://www.datatilsynet.dk/generelt-om-databeskyttelse/vejledninger-og-skabeloner/

Der er også en del oplysninger om GDPR på

www.sundby-hvorupboligselskab.dk.

Sundby-Hvorup Boligselskab

Lindholm Søpark 4

9400 Nørresundby

Tlf.: 98 17 30 66

E-mail: info@sundbyhvorup.dk

www.sundby-hvorupboligselskab.dk

Redigeret: 04-03-2022