Informationssikkerhed i Københavns Kommune

Du skal som offentligt ansat passe godt på borgernes og kommunens oplysninger. Derfor er det vigtigt, at du følger råd og regler i denne pjece.

ADGANGSKODER - PASSWORD

Adgangskoder til it-systemer er personlige og strengt fortrolige.

- Del aldrig dit brugernavn og adgangskode med andre.
- Brug forskellige adgangskoder til de forskellige it-systemer.
- Dine adgangskoder skal være svære at gætte for andre. Skriv dem ikke ned og lad ikke browseren huske dem – lær dem udenad.
- Skift straks din adgangskode, hvis du har mistanke om, at andre har kendskab til den.

Ved mistanke om, at adgangskoden er blevet misbrugt, så ring straks til Koncern IT på tlf. 7080 8000.

LÅS ALTID DIN PC NÅR DU FORLADER DEN

Husk at låse din PC når du forlader den, så din adgang ikke kan benyttes af andre og eventuelt misbruges.

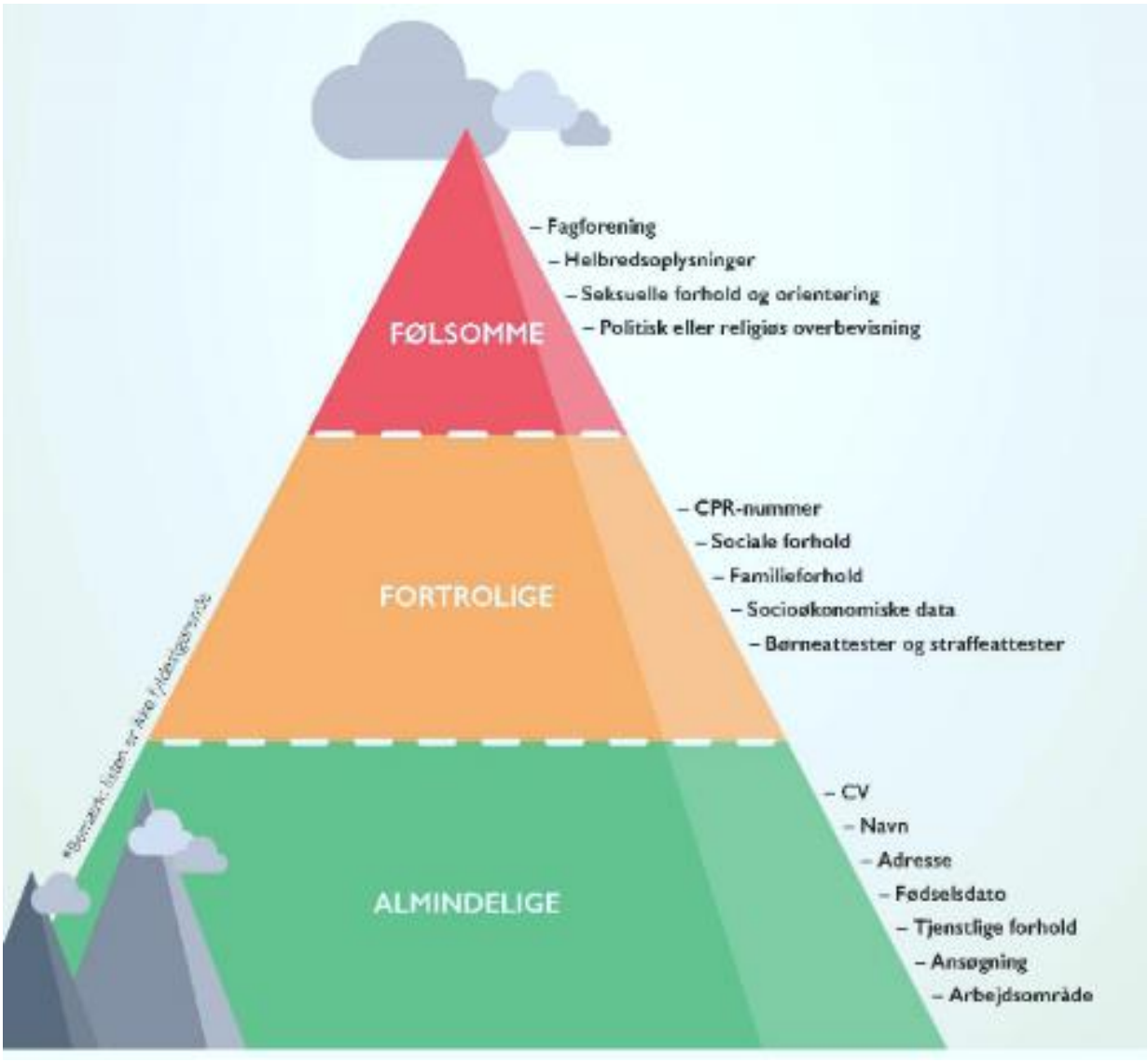
Tryk på  +  for at låse din pc.

Personoplysninger og kommunens værdidata skal beskyttes

PERSONOPLYSNINGER OG VÆRDIDATA - DATABESKYTTELSE EFTER KATEGORIER

I Københavns kommune arbejder vi med mange slags oplysninger. Nogle kategorier af oplysninger kræver særlig beskyttelse. Det drejer sig om personoplysninger og kommunens værdidata.

Personoplysninger er alle former for oplysninger, der kan henføres til en bestemt fysisk person.
Pyramiden illustrerer de kategorier af personoplysninger, vi arbejder med i kommunen og giver eksempler på hvilke personoplysninger, der tilhører de enkelte kategorier. Vi skal beskytte alle personoplysninger, men de følsomme og fortrolige kræver ekstra beskyttelse. Vær opmærksom på, at **kommunens værdidata** fx kontrakter, forretningskritiske processer og it-infrastruktur beskrivelser, skal beskyttes i samme grad som følsomme personoplysninger.



Åbne oplysninger: Omfatter alt, hvad der ikke er omfattet af ovenstående. Fx alle oplysninger der er egnet til almen offentliggørelse, åbne dagsordner, borger- og erhvervsinformation. Åbne oplysninger kræver ingen særlig sikring, de er åbne for alle.

KØBENHAVNS KOMMUNE ER ANSVARLIG FOR DATA

Københavns Kommune er ansvarlig for alle de oplysninger, der gemmes i it-systemer og på medarbejdernes it-udstyr. Kommunen har ret til frit at anvende disse informationer inden for lovens rammer.

- Har du private e-mails eller filer, så marker dem med "privat" i emnefelt eller mappe. Kommunen må kun anvende privat markerede e-mails og filer under særlige forhold.

OPBEVARING AF OPLYSNINGER

Personoplysninger og værdidata skal opbevares sikkert og forsvarligt.
Borgernes personoplysninger og kommunens værdidata skal derfor opbevares i kommunens sikre journal- og fagsystemer. De kan undtagelsesvis opbevares i kommunens opbevaringsløsninger som fx OneDrive eller SharePoint - dog højst i 30 dage - herefter skal de slettes.

- Gem ikke oplysningerne lokalt på din enhed eller pc fx C-drev eller skrivebordet.
- Gem aldrig oplysningerne på netværkstjenester som fx Dropbox eller på bærbare medier som fx USB-stik.
- Er du i tvivl om, hvordan oplysninger skal behandles og opbevares, så spørg din nærmeste leder.

MOBILE ENHEDER

Kommunens sikkerhedsløsning til mobile enheder skal være installeret, hvis du skal have adgang til din kalender, læse e-mail, intranet m.v.
Du har et ansvar for at beskytte de oplysninger, der ligger på dine mobile enheder.

- Mobilen skal altid sikres med pinkoder.
- Lås enheden, når du går fra den, og hav den altid under opsyn i det offentlige rum.
- Gem ikke borgernes oplysninger lokalt på dine mobile enheder.
- Ryd op på enheden, så der ikke lokalt ligger fortrolige noter, billeder eller filer.

Bliver din mobile enhed stjålet, så ring straks til Koncern IT på tlf. 7080 8000.

SEND SIKKERT

- Skal du sende personoplysninger eller værdidata til borgere eller eksterne samarbejdspartnere, så SKAL du sende enten via et fagsystem, funktionen "send sikkert" i Outlook eller doc2mail. Disse funktioner sørger for, at oplysningerne bliver krypteret under transporten og ender hos de rette modtagere.

SOCIALE MEDIER

- Benytter du sociale medier som fx Facebook i dit arbejde, så vær opmærksom på aldrig at udveksle personoplysninger eller udføre sagsbehandling via disse kanaler.

FYSISK SIKKERHED

Den fysiske sikring af person- og værdioplysninger er vigtig. Sørg for at uvedkommende ikke kan se med på din skærm eller få adgang til de fysiske dokumenter.

- Opbevar fysiske dokumenter med person- og værdioplysninger sikkert fx i aflåst skab. Lad dem ikke ligge frit fremme på skrivebordet. Når dokumenterne ikke længere skal benyttes, skal de makuleres, smid dem aldrig i papirkurven.

OPSLAG I IT-SYSTEMER – AKTIVITETER REGISTRERES/LOGGES

Alle opslag i kommunens fagsystemer med følsomme og fortrolige oplysninger bliver logget og gemt. Derudover sker der løbende registrering af aktiviteter på netværket, af hensyn til kommunes drift og sikkerhed. Dermed er det muligt at se, om der er sket misbrug.

- Du må kun behandle/fremsøge personoplysninger, der er relevante for dit arbejde.
- Du må ikke lave opslag på dig selv, familie, venner eller lignende.

TAVSHEDSPLIGT

Medarbejdere i Københavns Kommune har tavshedspligt.
De følsomme og fortrolige oplysninger, du får kendskab til gennem dit arbejde, må ikke uberettiget videregives til andre eller komme til uvedkommendes kendskab.

- Tavshedspligten gælder både under og efter din ansættelse.

VIRUS, PHISHING OG SUSPEKTE HJEMMESIDER

Kommunens it-udstyr er beskyttet mod virus, phishing, ransomware, spam m.v., men ikke alle angreb fanges af kommunens sikkerhedsforanstaltninger.

- Modtager du en mistænkelig e-mail, så slet den. Svar ikke på den og åbn aldrig vedhæftede filer eller links.
- Besøg ikke suspekte eller anstødelige hjemmesider. Vær kritisk, opmærksom og brug altid din sunde fornuft.
- Bliver du ramt, eller er du i tvivl, så kontakt Koncern IT på tlf. 7080 8000.

FÅ MERE VIDEN

Du finder mere information om it-sikkerhed og databeskyttelse på KKintra: IT-sikkerhed og Pas på vores data
Alle medarbejdere i Københavns Kommune skal gennemføre obligatoriske uddannelse/e-læring om it-sikkerhed og databeskyttelse, kontakt din leder om tilmelding.
Har du brug for at kontakte os, er du velkommen til at skrive til: it-sikkerhed@ks.kk.dk

Med venlig hilsen
Vejledende Sikkerhed,
Koncern IT, Økonomiforvaltningen