KØBENHAVNS KOMMUNE

It-sikkerhed og databeskyttelse
Pjece 2

Pas på vores data!

I kommunen oplever vi et stigende antal angreb fra it-kriminelle. EU' s Databeskyttelsesforordning stiller skærpede krav til beskyttelse af personoplysninger. Kommunen skal overholde kravene og kommunens it-sikkerhedsregler så borgere, medarbejdere og virksomheder kan være trygge ved, at vi behandler deres oplysninger sikkert, korrekt og efter loven. Derfor er det vigtigt at kende reglerne for it-sikkerhed og databeskyttelse.

DATABESKYTTELSESFORORDNING

Databeskyttelsesforordningen også kaldet GDPR er en EU-forordning, som er trådt i kraft d. 25. maj 2018. Den **stiller skærpede krav til beskyttelse af personoplysninger**.
Københavns kommune skal overholde kravene, så borgere, samarbejdspartnere og medarbejdere kan være trygge ved at give deres oplysninger til os og have tillid til, at vi behandler dem korrekt og inden for lovens rammer.

HVAD ER PERSONOPLYSNINGER?

Personoplysninger er alle former for oplysninger, der kan henføres til en bestemt fysisk person.
Det kan fx være navn, cpr-nummer, helbredsoplysninger, fingeraftryk eller et foto.
Kommunen skal beskytte alle personoplysninger, men nogle skal beskyttes bedre end andre. Kravene til beskyttelse af følsomme personoplysninger er de strengeste.

Personoplysninger inddeles i tre kategorier:
Følsomme fx race, politisk eller religiøs overbevisning, seksualitet, helbred, fagforening, genetiske data.
Fortrolige fx CPR-nr., straffedomme, sociale forhold, kontonumre, familieforhold, socioøkonomiske data.
Almindelige fx ansættelsesforhold, adresse, navn, tlf.nr., fødselsdato, CV, registreringsnummer.

CPR-nummeret er en fortrolig personoplysning og kommunen kan behandle cpr-numre med henblik på en entydig identifikation af enkeltpersoner eller som journalnummer.

Vær opmærksom på at **kommunens værdioplysninger** fx kontrakter, forretningskritiske processer og it-infrastruktur beskrivelser, skal beskyttes i samme grad som følsomme personoplysninger.

KØBENHAVNS KOMMUNE

BEHANDLING AF PERSONOPLYSNINGER

Når vi siger "behandling" mener vi enhver form for håndtering
fx: Indsamling, registrering, systematisering, opbevaring, tilpasning eller ændring, selektion, søgning, brug, videregivelse, samkøring, sletning.

For at sikre korrekt behandling af personoplysninger er der særligt 5 krav, som skal overholdes:

Lovlighed betyder, at der skal være en hjemmel - altså en lovlig grund - til at behandle personoplysninger. Normalt sker databehandling på baggrund af lovgivningen og kun i helt særlige tilfælde på baggrund af samtykke fra de berørte.
Formålsbegrænsning betyder, at du kun må behandle personoplysninger, hvis der er et udtrykkeligt formål med det, og at data ikke må anvendes til andre formål end det, de er indsamlet til.
Dataminimering betyder, at du kun må behandle de personoplysninger der er nødvendige for at opfylde formålet med behandlingen.
Rigtighed betyder, at de personoplysninger, der behandles, skal være rigtige og ajourført.
Opbevaringsbegrænsning betyder, at data skal slettes, når formålet med deres indsamling og behandling er opnået. Forinden skal det vurderes om data skal arkiveres. OBS. Alle forvaltningerne har slettefrister for deres egne områder - er du i tvivl så tag en snak med din leder.

Hvis du er i tvivl om, hvorvidt i lever op til kravene i jeres afdeling, så tag en snak med din leder

REGLER DER SKAL OVERHOLDES

Du må kun behandle - herunder også søge efter - personoplysninger, der er relevante for dine arbejdsopgaver.

Du må ikke lave opslag på dig selv, familie, venner eller lignende.

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

Hvis du overtræder reglerne kan det få konsekvenser for dit ansættelsesforhold

Du må ikke videregive personoplysninger til uvedkommende.
Publicer aldrig person- eller værdioplysninger på internettet.
Benytter du sociale tjenester i dit arbejde så vær opmærksom på aldrig at udveksle personoplysninger eller udføre sagsbehandling via disse kanaler.

KØBENHAVNS KOMMUNE

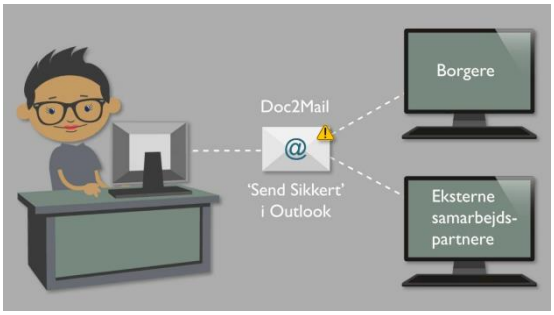
VÆRKTØJER OG RETNINGSLINJER

Personoplysninger og værdioplysninger skal opbevares sikkert og forsvarligt og der er skærpede krav til opbevaring af følsomme og fortrolige oplysninger.

Derfor skal oplysningerne opbevares i **kommunens journalsystemer** eller i **relevante fagsystemer**.
Oplysningerne kan undtagelsesvis opbevares midlertidigt på kommunens netværksdrev - dog højst i 30 dage - hvorefter oplysningerne skal slettes eller placeres i et journalsystem eller fagsystem.

Du må **ikke** gemme oplysningerne lokalt på din enhed eller pc fx **C-drev eller skrivebordet**.
Gem **aldrig** oplysningerne på **netværkstjenester (fx Dropbox)** eller på **bærbare medier (fx USB-stik).**

Når du skal sende personoplysninger eller værdioplysninger elektronisk ud af kommunen, til borgere eller eksterne, SKAL du enten sende via et fagsystem, funktionen "send sikkert" i Outlook eller doc2mail.
Disse funktioner sørger for, at data bliver krypteret under transporten og ender hos rette modtager.



DEN REGISTREREDES RETTIGHEDER

Databeskyttelsesforordningen giver de registrerede en række rettigheder for at skabe åbenhed omkring behandlingen af personoplysninger. De registrerede kan være både borgere, enkeltmandsvirksomheder eller medarbejdere - dig og mig. Her er en kort oversigt over de registreredes rettigheder.
Oplysningspligt – kommunen skal give den registrerede besked om at vi indsamler og behandler deres personoplysninger og hvad formålet er.
Indsigtsret – den registrerede har ret til at bede om at få indsigt i de oplysninger som Københavns Kommune har registreret om dem. Der er ikke nogen formkrav til hvordan en borger kan bede om at få indsigt. Kommunen har en formular på hjemmesiden, som sikrer at den registrerede har let adgang til, at fremsætte sin anmodning om indsigt så præcist som muligt.
Berigtigelse - Retten til at få oplysninger rettet. Hvis kommunen behandler forkerte oplysninger om den registrerede, kan den pågældende bede om at få oplysningerne rettet.

SAMTYKKE

I Kommunen behandler vi som udgangspunkt personoplysninger på baggrund af lovgivningen. I nogle tilfælde sker behandling dog på baggrund af samtykke. Fx samtykke fra forældre om offentliggørelse af barns foto på skolens hjemmeside. En anmodning om samtykke skal være forståeligt og let tilgængeligt. Kommunen skal kunne bevise, at der er givet et samtykke og det skal være muligt at trække samtykket tilbage.

KØBENHAVNS KOMMUNE

DPO

Alle offentlige myndigheder skal udpege en Databeskyttelsesrådgiver (DPO). **I Københavns Kommune er det chefen for Intern Revision der er kommunens DPO**. DPO'en har bl.a. ansvar at understøtte, rådgive og overvåge kommunens overholdelse af Persondataforordningen og behandlingen af persondata og at samarbejde med Datatilsynet når det er nødvendigt.
For at støtte DPO'ens arbejde i kommunen er der udpeget en DPO Business Partner i hver forvaltning. DPO Business Partneren er derfor den person, som i første omgang skal hjælpe dig og din afdeling med at tolke og overholde databeskyttelsesreglerne på netop jeres område.

Sikkerhedshændelser

En sikkerhedshændelse kendes ofte ved, at der er fare for at informationer mistes, er ukorrekte eller kommer til uvedkommendes kendskab.
Eksempler på sikkerhedshændelser:

- Borgeres persondata er publiceret på kommunens websider.
- Medarbejdere deler brugerid og adgangskoder.
- Persondata er sendt ud til forkerte modtagere.
- Følsomme personoplysninger er sendt med ukrypteret e-mail til borgere.
- Medarbejdere videregiver personoplysninger til uvedkommende.

Sikkerhedshændelser skal indberettes - så skaden begrænses - hændelsen håndteres – forbedringer etableres.
Det er vigtigt at reagere hurtigt, da tid kan være en afgørende faktor. Dit bidrag til at sikre indberetning af hændelser er afgørende. Falder oplysninger i de forkerte hænder kan det fx føre til misbrug eller afsløringer af følsomme persondata. Det kan få store menneskelige konsekvenser for de berørte og for kommunens omdømme.

Sikkerhedshændelser skal indberettes i IT-portalen.
Som udgangspunkt skal du selv indberette hændelsen, men det kan også være, at du skal kontakte DPO Business Partner i din forvaltning, som så hjælper dig med indberetningen.
Du skal under alle omstændigheder kende og følge de lokale retningslinjer for, hvordan indberetning af sikkerhedshændelser skal ske i din forvaltning.

Er der brug for akut hjælp i forbindelse med en hændelse, skal du straks kontakte Koncernservice.

Få mere viden

Find mere info om uddannelse, forvaltningernes DPO BP og supplerende materiale på KKintra: Pas på vores data

Med venlig hilsen
Vejledende Sikkerhed
Koncern IT
Økonomiforvaltningen

Pjecen knytter sig til uddannelse / e-læringsforløb om it-sikkerhed og databeskyttelse

Udarbejdet af Koncern IT til Københavns Kommunes medarbejdere maj 2018