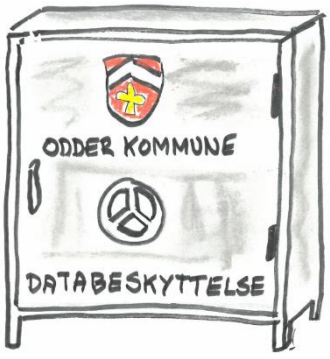
Værd at vide om databeskyttelse - for leder



Lederens ansvar

Som leder har du ansvaret for at reglerne i Databeskyttelses-forordningen (GDPR) overholdes i din afdeling. Det indebærer at:

- de ansatte har den fornødne uddannelse
- de registreredes oplysninger behandles på en forsvarlig måde
- databeskyttelse jævnligt kommer på dagsordenen i afdelingen, sådan at der dannes en GDPR-kultur.

Databeskyttelsesrådgiveren

- Også kaldet DPO'en

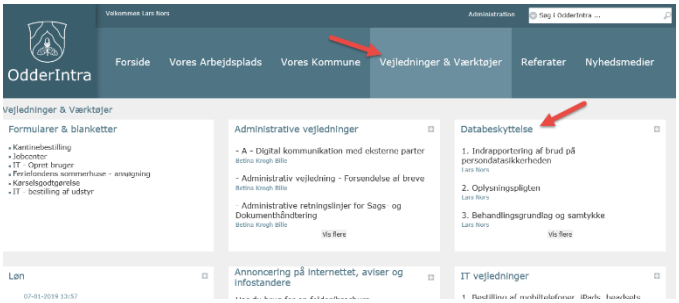
Databeskyttelsesrådgiverens opgaver er:

- At rådgive ansatte om kommunens behandling af personoplysninger og om reglerne i Databeskyttelses-forordningen og Databeskyttelsesloven
- At være kontaktperson for borgere, der vil vide hvordan kommunen behandler deres personoplysninger
- At påse at reglerne om god databeskyttelse overholdes i Odder Kommune.
- At være kontaktperson for Datatilsynet

Har du spørgsmål om databeskyttelse kan du kontakte DPO'en på dpo@odder.dk eller tlf: 20902026

Hvor kan jeg finde information?

Du kan finde information på OdderIntra på fanebladet Værktøjer & Vejledninger i informationsboksen ”Databeskyttelse”



Hvad er personoplysninger?

Personoplysninger er oplysninger der kan føre til identifikation af en person.

Personoplysninger opdeles i:

- Almindelige personoplysninger: F.eks. navn, telefonnummer, mailadresse, køn, skostørrelse, nummerplade, IP-adresse ...
- Særlige personoplysninger: Race, etnisk oprindelse, politisk, religiøs, filosofisk eller seksuel overbevisning, fagforeningsforhold, genetiske eller biometriske oplysninger, helbredsoplysninger
- Oplysninger om strafbare forhold
- Fortrolige oplysninger: Personnummer, økonomiske forhold, interne familieforhold, arbejds- ansættelses og uddannelsesforhold

De 3 sidste kategorier af personoplysninger skal vi passe ekstra godt på. Læs mere om typer af personoplysninger på OdderIntra

Hvad er behandling?

Behandling af personoplysninger er næsten alt det vi gør i vores kommunale sagsbehandling.

- Indsamling, registrering, organisering, systematisering, opbevaring, tilpasning eller ændring, genfinding, søgning, printning, forsendelse via mail eller digital post, formidling på internettet, sammenstilling eller samkøring, begrænsning, sletning eller tilintetgørelse.

Den Registrerede

Den person hvis personoplysninger vi behandler kaldes:
”Den Registrerede”

I Odder Kommune vil det typisk være en borger eller en ansat der er Den Registrerede hvis personoplysninger vi behandler. Vi kan også have en skoleelev, et barn i daginstitution eller en beboer på et plejecenter som Den Registrerede.

Behandlingsgrundlag og samtykke

Du må kun behandle personoplysninger, hvis du har et legitimt formål til det – altså et behandlingsgrundlag.

Behandlingsgrundlaget kan findes hvis:

- der er lov der foreskriver, at du skal behandle oplysninger som led i myndighedsudøvelse
- du modtager et samtykke fra borger til at behandle oplysninger

Vi skal kun have et samtykke, hvis ikke vi må behandle oplysninger som led i myndighedsudøvelse!

Der er en række krav til samtykke som du kan læse mere om på OdderIntra

Som leder har du ansvaret for at der er et behandlingsgrundlag for al behandling at personoplysninger i din afdeling/virksomhed.

OBS!
Den Registrerede kan trække et samtykke tilbage!

Oplysningspligt og privatlivsinformation

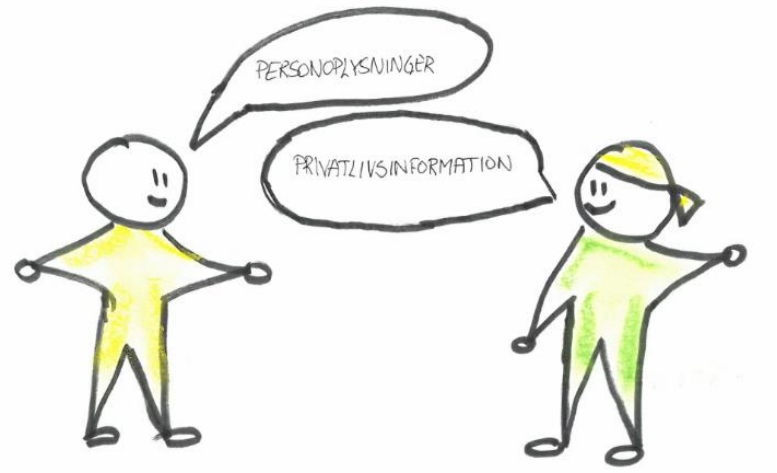
Borgeren har ret til at få oplyst, hvordan vi vil behandle deres personoplysninger. Du har pligt til aktivt at oplyse borgeren:

1. Når du modtager personoplysninger fra Den Registrerede
2. Når personoplysninger modtages fra andre end Den Registrerede f.eks. fra en anden myndighed.

De oplysninger borgeren skal have kaldes privatlivsinformation.

Ofte bliver oplysningspligten opfyldt hvis borgen anvender en blanket eller en selvbetjeningsløsning til at give os personoplysningerne, men hvis ikke det er tilfældet, har du pligt til at give borgeren privatlivsoplysningerne.

Læs mere om hvilke oplysninger en privat-livsinformationen skal indeholde på OdderIntra



Den Registreredes øvrige rettigheder

Den Registrerede har en række rettigheder i forhold til de personoplysninger, som du behandler, herunder ret til:

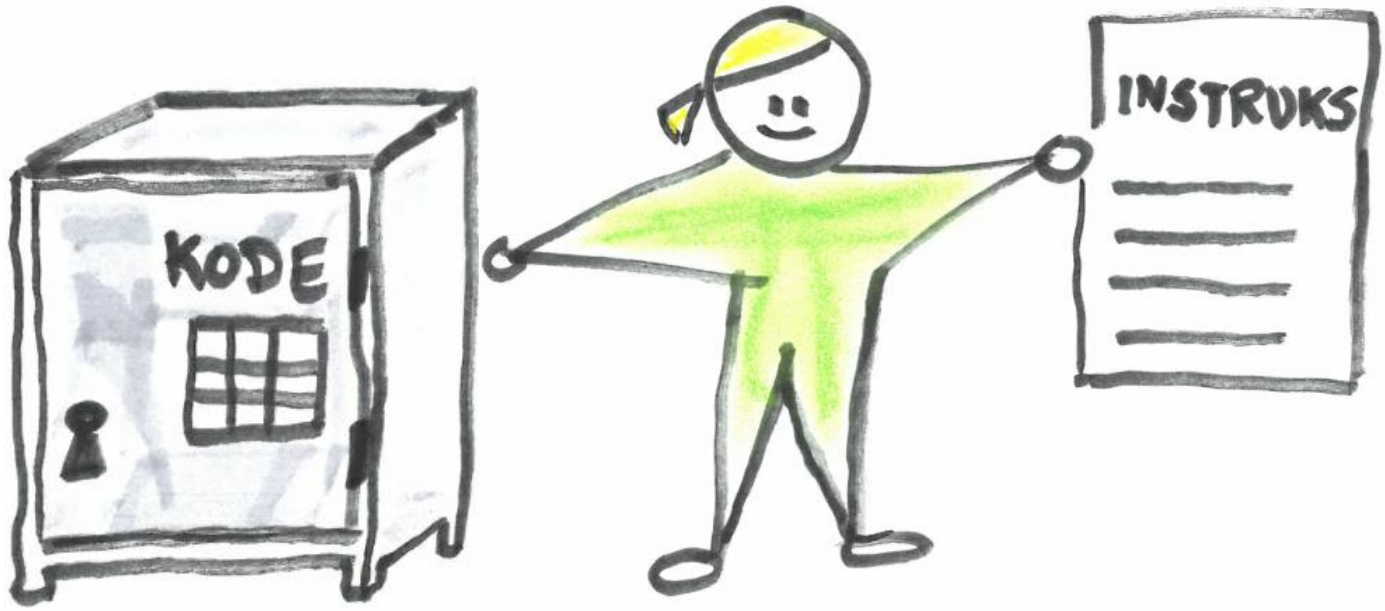
- Indsigt i hvilke oplysninger vi behandler i kommunen.
  - Indsigtsanmodninger behandles af kommunens DPO!
- Berigtigelse af data - hvis kommunen behandler forkerte oplysninger
- i visse tilfælde at få slettet eller begrænset de oplysninger kommunen behandler
- at gøre indsigelse imod behandling af personoplysninger

Passende sikkerhedsforanstaltninger

For at have en sikker behandling af personoplysningerne er det nødvendigt at der er opsat passende tekniske og organisatoriske foranstaltninger der minimerer risikoen for sikkerhedsbrud.

Et brud på sikkerheden er en hændelse, der fører til hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er sendt, opbevaret eller på anden måde behandlet. Et alvorligt sikkerhedsbrud kan have store konsekvenser for Den Registrerede.

Det er vigtigt at du som leder sørger for at implementere de sikkerhedsprocedurer i afdelingen, der meldes ud fra IT-afdelingen, Ledelse og Udvikling og DPO'en, samt at gennemgå jeres procedurer for behandling af personoplysninger med en risikobaseret tilgang, hvor I vurderer om sikkerheden er passende i alle procedurens led.



Sikkerhedsbrud – Hvad gør jeg?

Hvis du eller en af dine ansatte kommer ud for et brud skal I:

1. Dokumentere bruddet[*1]
2. Stoppe bruddet
3. Ringe til DPO'en tlf.: 20902026 og anmelde bruddet

DPO'en koordinerer den videre sagsbehandling herunder vurderer om de registrerede skal underrettes.

Et alvorligt brud skal anmeldes til Datatilsynet af DPO'en inden for 72 timer, det er derfor vigtigt at ringe hurtigt.

- De fleste sikkerhedsbrud i Odder Kommune sker ved at en sagsbehandler ved en fejl giver uvedkommende adgang til personoplysninger f.eks. ved at sende oplysningerne til en forkert modtager.

Efter et brud på datasikkerheden er det en god idé at tale om bruddet med afdelingen og finde måder at undgå brud på i fremtiden.

I tvivl?

Hvis du er i tvivl om du er ude for et sikkerhedsbrud er det bedre at ringe til DPO'en en gang for meget end en gang for lidt.

[*1] De fleste brud på sikkerheden kan have konsekvenser for de registrerede, og det kan være nødvendigt at kontakte de registrerede efter bruddet. Derfor er det vigtigt at vi får registreret og dokumenteret hvilke registrerede der er udsat for bruddet og med hvilke personoplysninger.

Dataansvarlig og databehandler

Når vi behandler de registreredes personoplysninger vil det næsten altid være Odder kommune der er dataansvarlig.

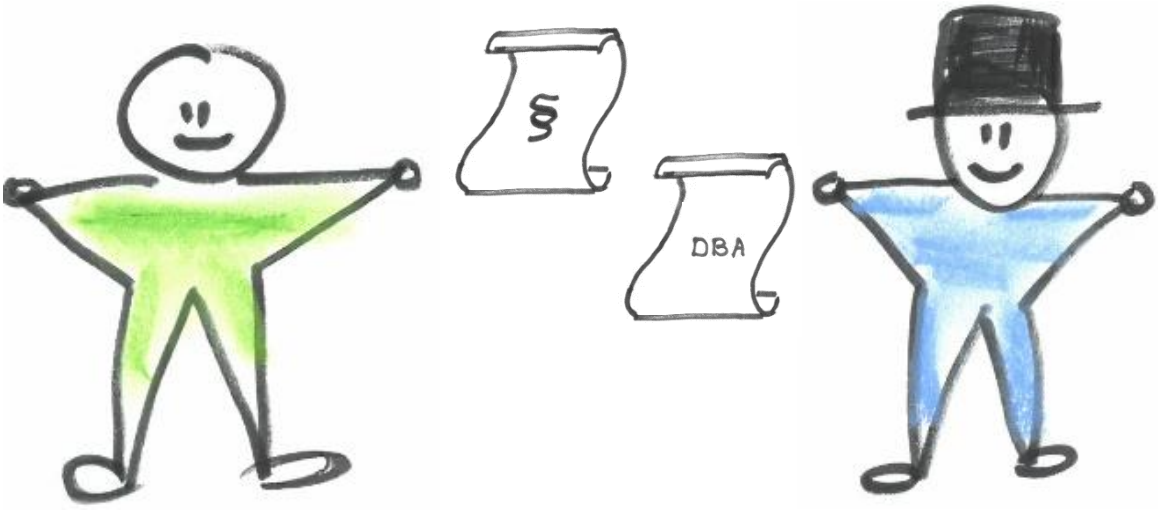
Hvis vi beder en samarbejdspartner om at behandle oplysningerne for os er samarbejdspartneren databehandler. En Databehandler kan typisk være leverandøren af et IT system eller en konsulent.

Når der indgås en aftale om et samarbejde mellem kommunen og en samarbejdspartner skal der ud over kontrakten også udfærdiges en Databehandleraftale.

En databehandleraftale indeholder en række beskrivelser af hvordan databehandler skal behandle de data, som vi er ansvarlige for, ligesom der også er krav til de sikkerhedsforanstaltninger vi kræver hos databehandleren.

En databehandleraftale skal altid kontrolleres af Ledelse og Udvikling og af IT-afdelingen inden IT-chefen underskriver den.

Du kan finde en vejledning i at afgøre om din samarbejdspartner er databehandler eller selvstændig dataansvarlig på OdderIntra hvor du også kan finde proceduren for behandling af databehandler-aftaler.



Fortegnelser over behandlingsaktiviteter

Odder kommune har pligt til at have en komplet fortegnelse over alle de aktiviteter i kommunen, hvor der sker behandling af personoplysninger.

Det er DPO'en der administrerer fortegnelsen, men du har ansvar for at fortælle DPO'en, hvis fortegnelsen skal ændres.

Hvis du får nye opgaver i din afdeling, hvor der behandles personoplysninger eller der falder opgaver bort, skal fortegnelsen opdateres. Fortegnelsen skal også opdateres hvis I begynder at behandle nye kategorier af registreredes oplysninger, hvis I begynder at behandle andre kategorier af personoplysninger, eller hvis I begynder at dele oplysninger med nye kategorier af modtagere.

Nye IT-systemer

Ved indkøb af nye IT-systemer bør DPO'en altid inddrages i beslutningsprocessen.

Der bør gennemføres en systematisk risikovurdering af systemet og om der bør gennemføres en konsekvensanalyse. Der er mere oplysning om risikovurdering og konsekvensanalyse senere.

Når vi køber nye IT systemer er det også et krav, at de har indbygget databeskyttelse via design og via standardindstillinger. Det vil sige at IT systemet skal være designet til at overholde reglerne i GDPR, og at databeskyttelsen skal være slået til som en standardindstilling.

Læs mere om fortegnelsen og databeskyttelse via design på OdderIntra.

Tilsyn med GDPR

En gang årligt i efteråret gennemfører DPO'en interne tilsyn i organisationen, der skal give et overblik over hvor godt Odder kommune opfylder reglerne i GDPR. Overblikket rapporteres videre til kommunens ledelse.

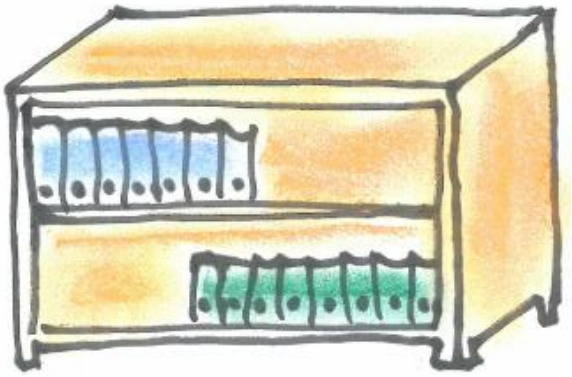
Der er også en sandsynlighed for at Datatilsynet kommer på anmeldt tilsyn på en af kommunens virksomheder eller afdelinger.

Dokumentation

Det er vigtigt at dokumentere afdelingens arbejde med databeskyttelse. For det første er det godt selv at have en historik over hvilke emner I har arbejdet med inden for GDPR, men det er også vigtigt af gemme dokumentationen til at kunne fremvise hvis DPO'en kommer på internt tilsyn eller hvis Datatilsynet kommer på anmeldt tilsyn.

Hvis I har gennemgået et område og konkluderet at sikkerheden omkring behandlingen af personoplysninger er passende, er det vigtigt også at få det skrevet ned. Det er meget bedre at vurdere lidt forkert på sikkerheden end ikke at foretage en vurdering, og det er derfor vigtigt at kunne dokumentere, at I har foretaget vurderingen.

Læs mere om dokumentation af GDPR på OdderIntra.



Risikovurdering og konsekvensanalyse

Risikovurdering er et helt centralt begreb i hele GDPR. Hver gang vi tænker persondatasikkerhed skal det være med udgangspunkt i en vurdering af risikoen for at data på den ene eller anden måde kompromitteres ved et brud på datasikkerheden. Risikoen er egentlig en samlet vurdering af sandsynligheden for et brud og de mulige konsekvenser for de registrerede hvis bruddet sker.

Der bør altid gennemføres en systematisk risikovurdering når der indkøbes nye IT-systemer eller indføres nye procedurer i afdelingen.

Konsekvensanalyse er en systematisk analyse af risikoen hvor der lægges en vurdering ind på, om risikoen er for høj i forbindelse med behandling af personoplysninger. Hvis risikoen vurderes som uacceptabel høj, skal der iværksættes foranstaltninger til at nedsætte risikoen for behandlingen. Analysen gennemføres inden for 3 kategorier for behandling af personoplysninger: Tilgængelighed, fortrolighed og integritet.

I nogle tilfælde skal dataansvarlige altid gennemføre en konsekvensanalyse. Det skal ske når der er tale om:

- Behandling af biometriske, genetiske eller lokationsdata
- Anvendelse af nye teknologier
- Automatisk behandling af data herunder profilering
- Systematisk overvågning
- Behandling af personoplysninger om sårbare personer
- Behandling med direkte effekt på personers helbred eller sikkerhed.

Når der skal gennemføres en konsekvensanalyse skal Databeskyttelsesrådgiveren altid inddrages!

Læs mere om risikovurdering og konsekvensanalyse på OdderIntra.