GDPR Håndbog for god håndtering af Personoplysninger (-:

Her er en folder om dine **forpligtelser** i forhold til **datasikkerhed!**

Databeskyttelsesforordningen sætter nyt fokus på at overholde lovgivningen omkring personoplysninger.

Denne folder samler op på de regler og krav, som lovgivningen om persondata stiller til dig som medarbejder og til din afdelings behandling af personoplysninger.

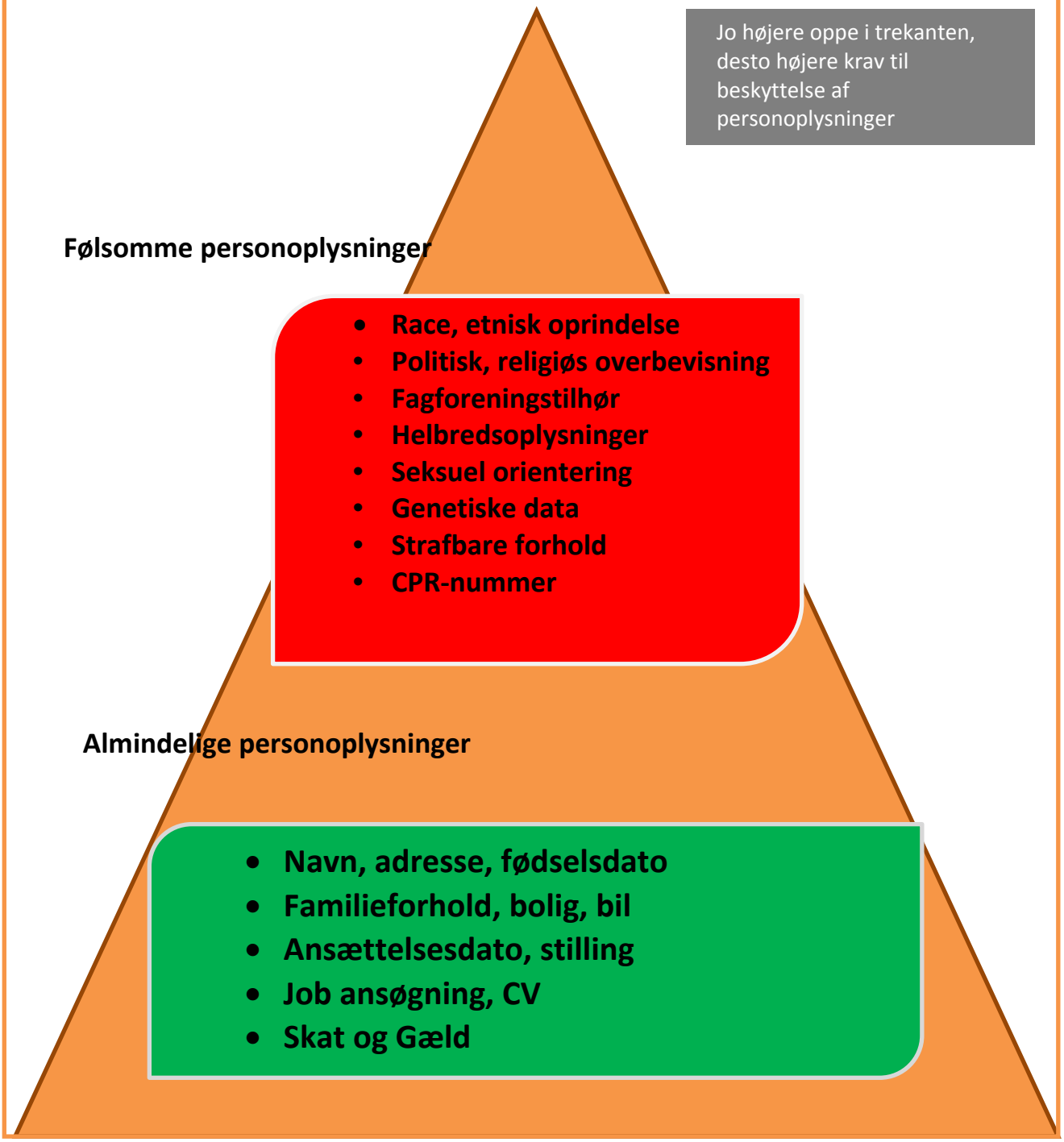
Databeskyttelsesforordningen træder i kraft d. 25. maj 2018 og stiller en række nye krav til behandlingen af persondata. Det handler i høj grad om, at kommunerne skal dokumentere arbejdet med borgernes data, og at borgerne får flere rettigheder i forhold, hvad vi bruger deres data til og, hvordan data behandles og opbevares. Det kommer ikke til at ændre grundlæggende ved dine arbejdsopgaver, men det er vigtigt, at du følger nye regler.

Indholdsfortegnelse

Hvad er personoplysninger?

Personoplysninger er enhver form for information, der kan henføres til fysiske 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.

Der skelnes mellem personoplysninger og "følsomme personoplysninger":



Hvordan må jeg behandle personoplysninger?

Håndtering af personoplysninger
- Du må behandle personoplysninger, hvis du har lovgrundlag for det eller har fået borgerens samtykke

Behandling af CPR-nummer
CPR-numre behandles som følsomme oplysninger og må kun behandles når det er nødvendigt, som følge af lovgivningen, eller der er givet samtykke.

Strafbare forhold
Oplysninger om strafbare forhold må kun behandles, hvis der foreligger samtykke, eller det er nødvendigt for at varetage en berettiget interesse**.**

Behandling af følsomme oplysninger
- er som udgangspunkt forbudt.
Der er dog undtagelser:

- hvis den registrerede har givet udtrykkeligt samtykke,
- hvis det eksempelvis kan beskytte den registreredes eller andres vitale interesser, eller
- hvis det er nødvendigt for at overholde arbejdsretlige forpligtelser (lovbestemt grundlag)

Hvilke personoplysninger må jeg bruge?

- Du må kun behandle personoplysninger, hvis du har lovgrundlag for det eller har fået borgerens samtykke i en erklæring som tydeligt forklarer, hvad data skal bruges til.
- Hvis personoplysningerne skal bruges til flere formål, skal det fremgå tydeligt af samtykkeerklæringen.
- Du må kun indhente personoplysninger, som er nødvendige for at løse din opgave
- Hvis du opdager, at oplysninger er fejlagtige, skal du sørge for, at de bliver rettet – også de steder, hvor data er videregivet til anden part

Hvor må jeg lagre personoplysninger?

Data som indeholder personoplysninger, og som skal gemmes i mere end 30 dage, skal lagres i et fagsystem eller i SBSYS, hvor der er en logning af, hvem der har tilgået og rettet i personoplysningerne, og hvornår det er sket.

Det gælder også for personoplysninger, som du håndterer via Outlook.

Det sikrer også, at personoplysninger er sikkerhedskopieret og kan gendannes ved menneskelige, tekniske fejl eller hackerangreb.

Hvor længe må jeg gemme personoplysninger?

- **Du må ikke gemme personoplysninger længere end det er nødvendigt for at løse opgaven**
- **Din afdeling skal have en beskrevet procedure for, hvor længe du gemmer personoplysninger i hvert enkelt system og/eller sagstype.**
- **Din afdeling skal have en beskrevet procedure for, hvordan personoplysninger slettes inden for tidsfristen.**
- **Hvis data skal sendes til arkiv, skal lokalarkivet sørge for, at det sker inden sletning, og at retningslinjerne for anonymisering af personoplysningerne er opfyldt.**

Hvad skal jeg oplyse borgeren om?

På blanketter, selvbetjeningsløsninger mv. skal borgeren oplyses om følgende:

- **Formålet med behandlingen**
- **Hvilke afdelinger der bruger personoplysningerne**
- **Kontaktoplysninger på afdelingerne**
- **Kontaktoplysninger på Databeskyttelsesrådgiveren**
- **Den lovmæssige hjemmel der ligger til grund for indsamling og behandling af personoplysningerne**
- **Hvem personoplysninger eventuelt videregives til**
- **Hvornår personoplysninger slettes**
- **Klagemulighed og ret til indsigt i behandlingen**

Har borgeren indsigtsret under persondataforordningen

Hvis borgeren spørger, har hun/han krav på at få svar på følgende inden for 30 dage: Det er vigtigt at svaret er let forståeligt og ikke bliver for teknisk.

- **Hvilke personoplysninger kommunen har om borgeren**
- **Hvad vi bruger personoplysninger til**
- **Hvor vi har fået personoplysningerne fra**
- **Hvem der har adgang til personoplysningerne**
- **Med hvilken lov eller samtykke vi har ret til at anvende personoplysninger**
- **Hvor/hos hvem personoplysninger opbevares**

OBS!: Der kan fortsat søges aktindsigt via forvaltningsloven, offentlighedsloven mv.

Hvad gør jeg ved brud på datasikkerheden?

Hvis uheldet er ude og der sker et brud på datasikkerheden, så personoplysninger bliver kompromitteret, skal du gøre følgende:

- **Underet din leder og IT om sikkerhedsbruddet**
- **Datatilsynet skal eventuelt underrettes (via kommunens databeskyttelsesrådgiver) om hændelsen inden for 72 timer med en beskrivelse af**
  - **Hvilke typer personoplysninger**
  - **Hvor mange der er berørt**
  - **Sandsynlige konsekvenser ved bruddet**
  - **Foranstaltninger som er truffet for at håndtere bruddet**
  - **Foranstaltninger for at begrænse skadevirkningen**
  - **Kontaktoplysninger på din databeskyttelsesrådgiver**
- **De berørte borgere skal eventuelt have besked om bruddet og eventuelle konsekvenser for deres privatliv**

Begrænsninger omkring kommunikation ved sikkerhedshændelser: Kommunale medarbejdere eller konsulenter må ikke kommunikere om sikkerhedshændelsen uden en tilladelse fra deres overordnede eller sikkerhedskoordinatoren

Særligt for leder og kontaktpersoner

OBS: En leder er ofte dataansvarlig

Hvordan dokumenterer jeg databehandlinger?

Din afdeling skal have en fortegnelse over de databehandlinger, som finder sted i din opgaveløsning. Den interne informationssikkerhedsgruppe har en fortegnelsesskabelon til formålet. Fortegnelsen skal indeholde:

- **Navn og kontaktoplysninger på dataansvarlig (Chef/leder som er systemejer), og kommunens databeskyttelsesrådgiver**
- **Formålet med databehandlingen**
- **Hvilke kategorier af data du har i din databehandling**
- **Hvem der modtager disse data – fx anden afdeling eller anden myndighed**
- **Hvornår de forskellige kategorier af data bliver slettet fra systemet**
- **Hvilke organisatoriske og tekniske sikkerhedsforanstaltninger der er foretaget i forhold til beskyttelse af personoplysningerne**

Særligt for ledere og kontaktpersoner

Hvem må have adgang til personoplysninger?

- **Det er dit ansvar som leder, at adgang til data kun er muligt for medarbejdere som har brug for det**
- **Der kan være forskel på, om en medarbejder kan se eller rette i personoplysninger**
- **Hver medarbejder har et unikt login og det skal kunne logges, hvem der har læst eller rettet i personoplysningerne**

Særligt for ledere og kontaktpersoner

Hvordan skal jeg som leder sikre personoplysninger?

- **Vurder om personoplysningerne er relevante for løsning af opgaven**
- **Vurder og foretag sikring af fortrolighed, integritet og tilgængelighed**
- **Lav eventuelle nødprocedurer**
- **Vurder om der skal foretages kryptering eller pseudonymisering**
- **Brug ISO 27001 og 27002 som drejebog til at foretage nødvendige organisatoriske og tekniske foranstaltninger og dokumentation**
- **Få underskrevet en leverandørerklæring, hvis eksterne konsulenter skal have adgang til data – kontakt den interne informationssikkerhedsgruppe for at få en blanket til leverandørerklæring.**

Særligt for ledere og kontaktpersoner

Hvad skal jeg gøre med leverandører af it-systemer?

- **Lederen skal sikre sig, at det it-system eller den tjeneste afdelingen indgår aftale om, lever op til databeskyttelsesforordningen fx mht. sikkerhed, hvor personoplysninger lagres, hvilke typer data der håndteres, brugeradgang, sletning, udveksling af data mv.**
- **Der skal indgås en databehandleraftale, hvori leverandøren og Kommunen indgår en skriftlige aftale om, hvordan leverandøren forvalter personoplysninger efter gældende lovgivning og evt. særlige krav.**
- **Kontrakt og databehandleraftale skal indgås i samarbejde med dataansvarlige, IT- afdelingen, leverandøren og din afdeling.**
- **Når personoplysninger opbevares hos ekstern leverandør, skal data ligge i EU. Alternativt skal leverandøren underskrive en erklæring om, at data behandles efter gældende lovgivning i EU.**

Lederen skal sikre og kontrollere, at leverandøren har de fornødne tekniske og organisatoriske tiltag omkring data, og hvem der har adgang til dem. F.eks. Skal medarbejderes adgang til følsomme personoplysninger revideres 2 gange om året af den dataansvarlige.

Særligt for ledere og kontaktpersoner

Hvad med konsulenter og eksterne aktører?

Hvis din afdeling bruger eksterne konsulenter, andre aktører eller leverandører til at løse opgaver, hvor de får adgang til kommunens personoplysninger, skal der indgås en skriftlig aftale, hvor det sikres, at de lever op til de sikkerhedspolitikker og procedurer, der er vedtaget i Kommunen.

Sikkerhedsgruppen kan hjælpe med de rigtige formularer og tavshedserklæringer til eksterne IT - leverandører.

Særligt for ledere og kontaktpersoner

Hvilke personoplysninger kræver særlige foranstaltninger?

Særlige følsomme personoplysninger kræver en konsekvensanalyse som omfatter:

- **Beskrivelse af hvorfor og hvordan du behandler personoplysninger**
- **Vurdering af om behandlingsaktiviteterne er nødvendige og rimelige i forhold til formålet**
- **Vurdering af risici for borgerens rettigheder, hvis personoplysningerne kompromitteres**
- **Beskrivelse af de foranstaltninger der er foretaget for at imødegå risici og for at overholde databeskyttelsesforordningen**

Konsekvensanalysen skal evalueres af kommunens databeskyttelsesrådgiver

Som dataansvarlig, leder eller fagansvarlig, er det dit ansvar, at personoplysninger og fagsystemer anvendes rigtigt og at medarbejderne er instrueret i, hvordan personoplysninger håndteres i opgaveløsningen.

Det er dataansvarliges ansvar, at nødvendig dokumentation til en hver tid er tilgængelig og kan fremvises ved intern audit, ved kontrolbesøg af Datatilsynet og når der i øvrigt er behov for det.

Er du medarbejder, er det vigtigt, at du følger instrukserne vedr. håndteringen af personoplysninger. Er du i tvivl, skal du henvende dig til din leder eller kontakte den interne informationssikkerhedsgruppe.

Definitioner:

»personoplysninger«:
enhver form for information om en identificeret eller identificerbar fysisk person (»den registrerede«); ved identificerbar fysisk person forstås en fysisk person, der direkte eller indirekte kan identificeres, navnlig ved en identifikator som f.eks. et navn, et identifikationsnummer, lokaliseringsdata, en onlineidentifikator eller et eller flere elementer, der er særlige for denne fysiske persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sociale identitet

»behandling«:
enhver aktivitet eller række af aktiviteter — med eller uden brug af automatisk behandling — som personoplysninger eller en samling af personoplysninger gøres til genstand for, f.eks. indsamling, registrering, organisering, systematisering, opbevaring, tilpasning eller ændring, genfinding, søgning, brug, videregivelse ved transmission, formidling eller enhver anden form for overladelse, sammenstilling eller samkøring, begrænsning, sletning eller tilintetgørelse

»pseudonymisering«:
behandling af personoplysninger på en sådan måde, at personoplysningerne ikke længere kan henføres til en bestemt registreret uden brug af supplerende oplysninger, forudsat at sådanne supplerende oplysninger opbevares separat og er underlagt tekniske og organisatoriske foranstaltninger for at sikre, at personoplysningerne ikke henføres til en identificeret eller identificerbar fysisk person

»dataansvarlig«:
en fysisk eller juridisk person, en offentlig myndighed, en institution eller et andet organ, der alene eller sammen med andre afgør, til hvilke formål og med hvilke hjælpemidler der må foretages behandling af personoplysninger; hvis formålene og hjælpemidlerne til en sådan behandling er fastlagt i EU-retten eller medlemsstaternes nationale ret, kan den dataansvarlige eller de specifikke kriterier for udpegelse af denne fastsættes i EU-retten eller medlemsstaternes nationale ret

»samtykke« fra den registrerede:
enhver frivillig, specifik, informeret og utvetydig viljestilkendegivelse fra den registrerede, hvorved den registrerede ved erklæring eller klar bekræftelse indvilliger i, at personoplysninger, der vedrører den pågældende, gøres til genstand for behandling

»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

Før jeg skriver mit navn på tavlen vil jeg vide hvad du vil bruge mit personlige data til!

Hvem er den interne sikkerhedskoordinator eller kontaktperson?

- **Kim Niegsch (sikkerhedskoordninator)**
- **Linne Caramés (kontaktperson)**
- **Jesper Vig Meyer (kontaktperson)**
- **Lene Jensen (kontaktperson)**
- **Jens Erik Nilsson-Møller (kontaktperson)**

Få hjælp

Kontakt sikkerhedsgruppen på itsikkerhed@ishoj.dk for hjælp til kontrakter og leverandøraftaler og spørgsmål om informationssikkerhed

Databeskyttelsesrådgiver for Ishøj Kommune

- Michael Drews Olsen michaelol@htk.dk