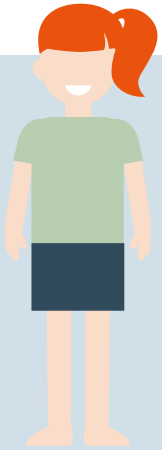
GDPR- og IT-sikkerheds-håndbog

Sådan beskytter du borgernes oplysninger



Jammerbugt Kommune skal passe på borgernes personoplysninger, når vi løser vores myndighedsopgaver.

Denne håndbog fortæller, hvordan kommunens IT-udstyr betjenes på en sikker måde og giver generel viden om god IT-adfærd, datahåndtering og databeskyttelse.

Som medarbejder har du pligt til at sætte dig ind i og overholde de til enhver tid gældende retningslinjer for IT-sikkerhed og GDPR. Overtrædelse af informationssikkerhedsreglerne kan få ansættelsesretslige konsekvenser.

Du har desuden pligt til at bidrage til kommunens sikkerhed. Det gør du ved løbende at deltage i relevante kurser, webinarer og møder, som kommunen afholder, og at holde dig opdateret på kommunens intranet TRYK under "GDPR og IT-sikkerhed". Hvis du oplever sikkerhedsmæssige fejl/uhensigtsmæssigheder eller steder, hvor kommunens retningslinjer ikke overholdes, skal du orientere din leder og kommunens sikkerhedsrådgiver.

Overtrædelse af informationssikkerhed

Hvis du som medarbejder overtræder kommunens informationssikkerhedspolitik eller tilhørende retningslinjer, vil din nærmeste leder vurdere, hvad der er sket, og hvor alvorligt det er.

Ved mindre, utilsigtede overtrædelser vil du blive gjort opmærksom på fejlen og få en påmindelse om reglerne. Alvorlige eller gentagne overtrædelser kan medføre sanktioner.

Når du fratræder eller skifter rolle, skal du stadig overholde visse sikkerhedsforpligtelser. Du vil blive informeret om, hvad der gælder for dig, og kommunen sikrer, at disse regler bliver fulgt.

Hvad er person-oplysninger?

Personoplysninger er oplysninger, som kan bruges til at identificere en bestemt person. Det betyder, at oplysningerne kan kobles direkte til en specifik person alene.

Som ansat skal du passe på alle slags personoplysninger. Du skal dog være særlig forsigtig med de **fremhævede** oplysninger.

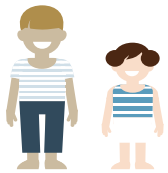
Almindelige personoplysninger, som bl.a. er:
Navn, alder, adresse, uddannelse, kontaktoplysninger, CV, jobansøgning m.m.

Følsomme personoplysninger, som altid er:

- Race og etnisk oprindelse
- Politisk overbevisning
- Religiøs eller filosofisk overbevisning
- Fagforeningsmæssige tilhørsforhold
- Genetiske data
- Biometriske data med henblik på entydig identifikation
- Helbredsoplysninger
- Seksuelle forhold eller seksuel orientering

Oplysninger om straffedomme og lovovertrædelser eller tilknyttede sikkerhedsforanstaltninger

Fortrolige personoplysninger, som kan være:



- CPR-numre
- Børn og sårbare personers almindelige personoplysninger
- Indtægts- og formueforhold
- Arbejds- og ansættelsesmæssige forhold
- Væsentlige sociale problemer, familieforhold og andre rent private forhold

Mange forskellige oplysninger kan være fortrolige, og det er din opgave at vurdere, hvornår der er tale om fortrolige oplysninger, og hvor du derfor skal være endnu mere påpasselig.

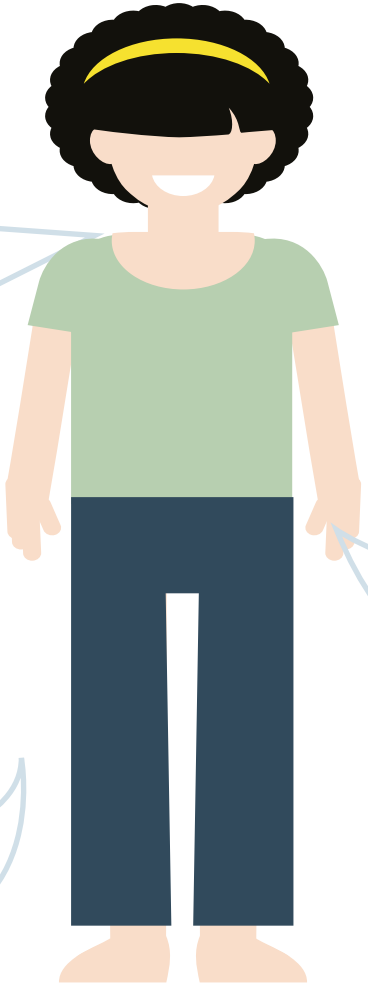
Sikker brug af IT-udstyr

Som ansat hos Jammerbugt Kommune kan du have adgang til forskelligt IT-udstyr som computere, mobil eller iPads, og derfor har du pligt til at følge disse retningslinjer:

Du skal låse eller slukke din computer, mobil eller iPad, når du efterlader den.

Du må ikke tilkoble private enheder som pc'er, telefoner, bærbare harddiske og USB-stiks til det kablede netværk eller til den kommunale PC.

Når en medarbejder stopper sin ansættelse ved Jammerbugt Kommune, skal alt it-udstyr afleveres til IT-afdelingen, som vil "nulstille" udstyret og sikre, at alle data på udstyret slettes. Ved bortkomst af udstyr, f.eks. ved tyveri, skal IT-servicedesk eller IT-vagt straks kontaktes, så udstyret kan låses, og data slettes.



Du skal være opmærksom på gæsters og borgeres færden, så ikke-ansatte eskorteres, hvis de har ærinde på kontorer, printerrum eller andre steder, hvor der kan være følsomme eller fortrolige oplysninger. Du skal være opmærksom, så du ikke kommer til at lukke uvedkommende ind på områder, hvor der ikke er offentlig adgang, f.eks. ved at uvedkommende personer "sniger sig med ind", efter du har åbnet døren med din nøglebrik.

For hjemmearbejdspladser gælder de samme retningslinjer som for kommunens almindelige IT-arbejdspladser. Du har pligt til at beskytte det IT-udstyr, du bruger i hjemmet, mod hærværk, tyveri, brand m.v. IT-udstyr må ikke anvendes af ikke-ansatte.

Det er ikke tilladt at anvende uautoriserede og usikre datamedier, f.eks. Dropbox og andre cloud-baserede datamedier, til udveksling, opbevaring eller arkivering af Jammerbugt Kommunes persondata. Der må ikke behandles eller opbevares personhenførbare eller fortrolige informationer på IT-udstyr, der ikke tilhører Jammerbugt Kommune. Du må maksimalt have 2 GB samlet på dine personlige drev. Det gælder både OneDrive, H:- og M:-drev samt eventuelt andre personlige fildrev, som Jammerbugt Kommune stiller til rådighed. IT-afdelingen forbeholder sig retten til at kontakte vedkommende og få datamængden nedbragt.

Sikker kommunikation

Når du sender personoplysninger, er det vigtigt, at du har øje for sikkerheden:

- **E-mails fra din mailkonto er ligesom dine andre dokumenter arbejdsredskaber og derfor i sidste ende kommunens ejendom.** Kommunen har derfor mulighed for - bl.a. hvis du fratræder eller langtidssygemeldes - at tilgå din IT-bruger og mailkonto, hvis det er vigtigt for kommunens videre arbejde, og at arbejdsopgaver m.m. ikke går tabt. Denne tilladelse skal gives af en direktør og skal være velbegrundet. Hvis du har private arbejdsrelaterede mails - f.eks. vedr. din egen ansættelse - liggende i din Outlook, som du i givet fald vil undgå, at andre læser, så kan du f.eks. lave en folder, som du kalder 'Privat'.
- **Online-møder er blevet en stor og vigtig del af vores dagligdag.** Når du skal holde online-møder med eksterne samarbejdspartnere eller borgere, skal du benytte Microsoft Teams eller (i skolernes tilfælde) Google Meet.
- **Som udgangspunkt skal du bruge fagsystemer til at kommunikere med borgere eller anvende Digital Post/Send Sikker i Outlook.**
- **Du sender altid sikkert, når du skriver fra en @jammerbugt-mail til en @ jammerbugt-mail.** Skriv aldrig CPR-nr. eller øvrige følsomme/fortrolige oplysninger i emnefeltet i mails, uanset om mailen sendes sikkert eller ej.
- **Det er tilladt at skrive til almindelige/usikre mailadresser, hvis der ikke sendes følsomme eller fortrolige oplysninger.** Du skal dog være opmærksom på, at du skal gå over til en sikker kommunikationskanal, hvis du eller borger har brug for at dele fortrolige eller følsomme oplysninger.
- **SMS og sociale medier er usikre kommunikationskanaler og må ikke anvendes til sagsbehandling.**
- **Din Outlook-arbejdskalender må ikke indeholde borgeres personoplysninger, f.eks. CPR.** Du må kun notere initialer, journalnumre eller andre anonyme oplysninger på borgere i mødeindkaldelser.

Sikkerhedsbrud

Du har som ansat pligt til at indberette sikkerhedsbrud. Det gør du ved at orientere din nærmeste leder og udfylde et skema, som du altid kan finde på siden 'Sikkerhedsbrud' på TRYK. Det udfyldte skema sender du til sikkerhedsbrud@jammerbugt.dk **med det samme**, du opdager bruddet.

Det er vigtigt, at du handler hurtigt, så snart du bliver opmærksom på et muligt sikkerhedsbrud. På den måde kan skaden begrænses mest muligt, ligesom Datatilsynet også stiller krav om at blive orienteret senest 72 timer efter, en alvorlig hændelse er konstateret.

Eksempler på sikkerhedsbrud:

- Følsomme eller fortrolige personoplysninger sendes til en borgers private mail
- Fysisk eller digital post med personoplysninger sendes til en forkert person
- Personoplysninger offentliggøres utilsigtet på internettet
- Uvedkommende får kendskab til adgangskoder
- Du mister IT-udstyr med personoplysninger
- Du har adgang til personoplysninger, som du ikke har brug for i dit arbejde

Hvis du er i tvivl om, hvorvidt det er et brud, så reagér, som om det er!

Fortrolighed og tavsheds-pligt

Som medarbejder i kommunen har du **tavshedspligt** om de oplysninger, du får kendskab til gennem dit arbejde, medmindre du er berettiget til at videregive dem, f.eks. ved aktindsigt inden for Offentlighedslovens rammer, eller fordi den, oplysningerne vedrører, har givet sit samtykke. **Det er strafbart uberettiget at videregive oplysninger**, man har fået kendskab til gennem sin ansættelse hos Jammerbugt Kommune, til uvedkommende.

Som led i arbejdet kan der være behov for at indsamle personoplysninger om borgere eller brugere. **Du må ikke indsamle flere oplysninger end de, der er relevante og tilstrækkelige for at løse din arbejdsopgave**. Med andre ord må du altså ikke "snage" i oplysninger, du ikke har brug for i forbindelse med dit arbejde.

Du må kun tilgå information, der er **nødvendig** for, at du kan udføre dit arbejde. Det betyder bl.a., at du ikke må slå dig selv eller folk, du kender privat, op i fagsystemer. Bemærk i øvrigt, at **kommunen har ret og pligt til at registrere (logge) medarbejdernes bevægelser på netværket, i programmer samt ved internetbrug**. Mht. personoplysninger gælder skærpede krav til logning og stikprøvekontrol, hvor kommunen kontrollerer, at personoplysningerne kun behandles af de relevante medarbejdere.

Hvis en kollega fra en anden afdeling spørger, om du vil sende borgers oplysninger, skal du altid sikre dig, at du har **hjemmel til delingen**. Det samme gælder, hvis en offentlig myndighed, samarbejdspartner eller borger ønsker at modtage personoplysninger. Det kan til tider være svært at gennemskue, hvornår det er tilladt at videregive en oplysning til andre. Inddrag derfor en af kommunens jurister for yderligere vejledning, hvis behovet opstår.

Adgange og koder

Når du logger ind i IT-systemer indeholdende personoplysninger, skal du altid anvende multifaktor (som du kender det fra privat brug af MitID). Alt afhængig af hvilket system du skal logge ind i, kan multifaktoren bestå af f.eks. brug af en app eller nøgleviser.

Du skal tildeles adgang med de nødvendige systemadgange og rettigheder til de systemer, som du har brug for adgang til for at løse deres arbejdsopgaver. Det er din nærmeste leder, som skal sikre, at du bliver oprettet i systemer og får tildelt nødvendige rettigheder.

Du er ansvarlig for, hvad dit login har været benyttet til på kommunens IT-systemer. Hvis det IT-udstyr, du anvender, skal bruges af en kollega, skal du logge dig af, før du overlader udstyret til din kollega. Og forlader du dit IT-udstyr, skal du låse udstyret - også ved kortvarigt fravær.

Har du mistanke om, at din adgangskode er blevet misbrugt, skal du straks underrette IT-afdelingen.

Når du logger på IT-udstyr, skal det altid ske med adgangskode (PC) eller pinkode (mobile enheder).

Længere og simplere adgangskoder er nøglen til sikkerhed:

- Din adgangskode skal bestå af minimum 15 tegn
- Der er intet krav til kompleksitet – brug af særtegn, tal og bogstavsstørrelser er altså frivilligt
- Der er intet krav om regelmæssige adgangskodeskift – dog skal din adgangskode ændres minimum én gang årligt

Gode råd og opmærksomhedspunkter:

- Din adgangskode bør aldrig indeholde sensitiv information om dig selv eller dit arbejde
- Genbrug aldrig dine tidligere eller nuværende adgangskoder på tværs af systemer
- Din adgangskode er personlig og må ikke deles med andre
- Den gode adgangskode er nem for dig at huske, men svær for andre at gætte

Opbevaring af oplysninger

Du skal sørge for at rydde op på dit IT-udstyr. Følsomme og fortrolige personoplysninger må maksimalt ligge uden for fagsystemer i 30 dage. Almindelige personoplysninger må ligge, indtil de ikke længere er relevante. Du skal derfor løbende sørge for at journalisere relevante dokumenter og slette dem fra din mail og dine drev.

Du skal altid hente dine prints med det samme, så du undgår, at uvedkommende kan læse med. Brug om muligt SKY-print, hvor dokumentet først printes ud, når du er fysisk til stede ved printeren.

Som medarbejder er du ansvarlig for at bortskaffe papirmateriale med personoplysninger eller forretningskritisk materiale, som ikke længere anvendes. Du skal enten bruge en lokal makulator eller lægge materialet i særlige beholdere, der opbevares aflåst indtil destruktion.

Husk, at printet papirmateriale med personoplysninger altid skal være aflåst eller under opsyn, herunder er det ikke tilladt at efterlade dokumenter med personoplysninger, f.eks. i dueslag, hvis der er adgang for personer uden et arbejdsbetinget behov.

Kort om ophavsret

- Brug kun billeder, lyd og tekst, hvis du har fået lov af den, der ejer rettighederne.
- Kopiér ikke fra bøger, artikler eller rapporter uden tilladelse.
- Husk: Du har selv ansvar for at overholde reglerne – både for kommunens og andres materiale.dig, og kommunen sikrer, at disse regler bliver fulgt.

Malware og virus

Malware betyder malicious software og er en betegnelse for computerprogrammer, der gør ondsindede, skadelige eller uønskede ting dér, hvor de er installeret. Begrebet dækker over alle kategorier af skadelige programmer, herunder virus og orme. Malware kan finde vej til vores IT-udstyr på et væld af måder; internet, mails, USB, DVD m.v. Oftest kræver det dog, at en bruger foretager en aktiv handling og f.eks. klikker på et link eller åbner en vedhæftet fil. Det er dog også muligt at blive inficeret blot ved at besøge en tilfældig inficeret hjemmeside. Brug altid din sunde fornuft, og vær kritisk, når du står i situationer, der kan indebære en sikkerhedsrisiko, som f.eks.:

E-mails med vedhæftede filer eller links i
Undlad at klikke på links eller vedhæftede filer, medmindre du er helt sikker på mailens ægthed. Vores SPAM-filter sorterer rigtig mange mails fra, men nogle få uautoriserede mails vil altid slippe igennem. Vær derfor altid på vagt, når du får mails med vedhæftede filer eller links, som du bliver bedt om at klikke på. Selv mails fra en kollega eller en person, du kender privat, kan udgøre en risiko.

Gratisprogrammer
Som udgangspunkt skal du benytte de fag- og sagssystemer, der stilles til rådighed af kommunen. Disse programmer er godkendte og sikre at bruge. Og arbejder du med personoplysninger skal dette altid ske i disse programmer. Du må ikke installere gratisprogrammer på din PC, da der kan følge virus og anden malware med i sådan en installation.

Brug af internettet
Kommunens firewall og andre tekniske løsninger begrænser mulighederne for at få uønskede malwareinficeringer fra internettet. Det er dog ikke ensbetydende med, at man risikofrit kan færdes overalt på internettet. Overvej altid, hvilke 'miljøer' du besøger på nettet. Har du mistanke om usikre hjemmesider, så søg alternativer. Spørg IT-servicedesk, hvis du er i tvivl.

Får dit IT-udstyr malware
På trods af de tekniske løsninger og din varsomhed kan uheldet være ude, og dit IT-udstyr kan blive inficeret med skadeligt software. Opdager du det selv, skal du hurtigst muligt slukke for din pc og kontakte IT-servicedesk. Det er også muligt, at IT-afdelingen opdager inficeringen først via kommunens overvågningsværktøjer. I så fald bliver du kontaktet for at få skiftet eller renset din pc. Det er vigtigt, at du følger IT's anvisninger, så en ondsindet virus ikke får lov at sprede sig.

Kontakt

Spørg gerne sikkerhedsrådgiveren om hjælp og vejledning på sikkerhed@jammerbugt.dk

Du kan læse mere i Jammerbugt Kommunes Informationssikkerhedspolitik, som findes på TRYK. Her vil du ligeledes kunne finde konkrete retningslinjer og vejledningerne vedrørende databeskyttelse og GDPR.

JAMMERBUGT KOMMUNE