

Databeskyttelse og informationssikkerhed

– er vores fælles ansvar



Som medarbejder har du et medansvar for at sikre kriminalforsorgens informationer og data. Du er ansvarlig for at beskytte de informationer, som vi behandler. Pas godt på dem; det er til gavn for os alle.



Det er desuden værd at notere sig, at manglende overholdelse af regler kan få ansættelsesretlige konsekvenser.

Forord

Sikkerhed er et nøgleord i kriminalforsorgen. Vi har mure, vi har hegn, vi har kameraer og adgangskontrol – og vigtigst af alt, har vi dygtige medarbejdere, der arbejder professionelt og dedikeret med både sikkerhed og resocialisering.

Men hvor der er mennesker, sker der fejl. Og ligesom med fængselssikkerheden, så er menneskelige fejl også en af de hyppigste årsager til sikkerhedsbrud, når kriminalforsorgen håndterer fortrolige og følsomme oplysninger. Det kan for eksempel være, at en mail med personlige oplysninger bliver sendt til en forkert modtager, eller at en medarbejder klikker på et link, som aktiverer skadelig software. Det kan også være følsomme oplysninger om kriminalforsorgens forretning, som for eksempel detaljer om vores it-systemer eller plantegninger over vores fængsler, der ikke er beskyttet godt nok.

Persondata er private oplysninger, som vi låner af borgerne og vores ansatte. Det er nødvendigt, for at vi kan løse vores opgaver som myndighed. Men når man låner private ting af andre, skal man selvfølgelig også passe godt på dem. Man skal opbevare dem omhyggeligt, man må ikke videreudlåne dem til andre uden at have lov, og man skal aflevere dem ubeskadigede tilbage igen – dvs. slette dem – når man ikke længere har brug for dem.

Bryder man de regler, kan det i værste fald få alvorlige konsekvenser for både vores klienter, indsatte og ansatte – og derigennem for hele kriminalforsorgen som organisation. Derfor er vi pålagt en række krav om databeskyttelse og informationssikkerhed, som vi skal leve op til, og derfor bliver der ført tilsyn med os af blandt andet Datatilsynet.

I denne folder kan du læse retningslinjerne for, hvordan du lever op til reglerne for databeskyttelse og informationssikkerhed i kriminalforsorgen.

Du kan også finde mere information under Databeskyttelse og Informationssikkerhed på intranettet.

God læselyst!

Ina Eliassen

Direktør i Kriminalforsorgen

Databeskyttelse og informationssikkerhed er alles ansvar

Denne folder indeholder retningslinjer og regler, der skal overholdes af alle medarbejdere.

Typer af personoplysninger

Personoplysninger er et bredt begreb og kan overordnet set opdeles i to kategorier; almindelige og følsomme oplysninger. Derudover er der en række af oplysningerne, der kan betragtes som fortrolige. Det afgørende for, om en oplysning skal anses for fortrolig, vil være en vurdering af, om oplysningen efter den almindelige opfattelse i samfundet bør kunne forlanges unddraget offentlighedens kendskab.

Følsomme personoplysninger er blandt andet oplysninger om race, etnisk oprindelse, politisk og religiøs overbevisning, seksuel orientering med videre.

Fortrolige personoplysninger er for eksempel oplysninger om strafbare forhold (herunder mistanke om), CPR-nummer, privatøkonomiske forhold, sociale problemer med videre.

Almindelige personoplysninger kan også være fortrolige i nogle tilfælde, mens de i andre tilfælde ikke er det. Det gælder eksempelvis telefonnummer og adresse, der kan være "hemmelige".

I kriminalforsorgen behandler vi mange fortrolige og følsomme personoplysninger, og vi har derfor et generelt højt beskyttelsesbehov. På de næste sider får du et overblik over reglerne inddelt i fire områder:

- | Generelt på arbejdspladsen | Arbejde ved pc, mobil eller tablet |
- | Sagsbehandling | Uden for arbejdspladsen

Du kan læse mere om, hvilke kategorier som findes af personoplysninger og de grundlæggende regler og principper ved behandling af persondata under Databeskyttelse og informationssikkerhed på intranettet.

Hvad er en personoplysning?

En personoplysning er enhver form for information, der kan henføres til en bestemt person, herunder blandt andet navn, CPR-nummer, registreringsnummeret på en bil, finger-aftryk og oplysninger om en persons helbred.



Personoplysnings-trekanten

Følsomme

Race og etnisk oprindelse, filosofisk, religiøs, politisk overbevisning, fagforeningsmæssigt tilhørsforhold, genetiske data, biometriske data, helbredsoplysninger, seksuelle forhold og orientering.

Fortrolige

Straffedomme eller lovovertrædelser
CPR-nummer, privatøkonomi, sociale problemer... m.fl.

Almindelige

Familieforhold, bolig, bil, ansøgning, stilling, arbejdstelefon, navn, adresse, fødselsdata... m.fl.
I nogle situationer er almindelige personoplysninger fortrolige.

Klassifikation af oplysninger

For at sikre den korrekte beskyttelse af informationer bliver disse i mange tilfælde påført en klassifikationsgrad. Klassifikationsgraden styrer bl.a., hvem informationerne må deles med, hvor de må behandles, og hvordan de skal gemmes og slettes. Kriminalforsorgen har tre klassifikationsgrader:



Jo længere man kommer op i klassifikationsgrad, des strengere krav er der til beskyttelse af informationerne. For at behandle oplysninger korrekt skal du kende til klassifikationsgraderne, så du kan behandle informationer korrekt, uanset om du modtager dem eller selv formidler dem videre. Klassifikationsgraden bør fremgå tydeligt, for eksempel af forside på et dokument og sidehovedet.

Klassifikation	
☐	Skærpet
☒	Internt
☐	Offentligt

Du kan læse mere om kriminalforsorgens ramme for klassifikation under Databeskyttelse og informationssikkerhed på intranettet (vælg Politikker og retningslinjer – Klassifikation).

Vær opmærksom på, at når der efterfølgende i denne folder tales om forskellige og følsomme oplysninger, vil der være tale om oplysninger, der som minimum kategoriseres som "Internt" i henhold til kriminalforsorgens ramme for klassifikation.

På arbejdspladsen

Adgangskort

Dit adgangskort identificerer dig som ansat i kriminalforsorgen. Kortet fungerer visse steder samtidig som en elektronisk nøgle til arbejdspladsen.

De steder, hvor medarbejdere har adgangskort, skal disse altid bære adgangskortet synligt. Adgangskortet er personligt og må kun benyttes af dig. Du må ikke oplyse koden til adgangskortet til andre. Tag ansvar for, at uvedkommende ikke går med, når du åbner døre med dit adgangskort.

Mister du adgangskortet, skal du straks melde det til serviceenheden på din arbejdsplads.

Gæster udefra

Venter du besøg af for eksempel håndværkere, leverandører eller konsulenter, som ikke har eget adgangskort, skal receptionen eller vagten orienteres, og hvis der er mulighed for det, skal du gæsteregistrere. Hvis du er forhindret i at hente dine gæster, skal du sørge for, at nogen henter dem.

Gæster skal altid ledsages rundt på arbejdspladsen og følges ud, når besøget er overstået. Du må ikke udlevere dit personlige adgangskort til en gæst.

Bredt tilgængeligt materiale

Reglerne for håndtering af personoplysninger omfatter også oplysninger som gøres tilgængelige via f.eks. plakater, vagtplaner, belægstavler, ferieplaner, diplomer osv.

Vær i den forbindelse opmærksom på, hvad der hænges op, og hvem der kan se oplysningerne

Skrivebordet

I videst muligt omfang skal du holde dit skrivebord fri for dokumenter, der indeholder personoplysninger eller andre fortrolige informationer, når du ikke er i nærheden af det. Brugen af fysiske udskrifter af dokumenter, der allerede findes i elektronisk form, bør være begrænset.

Du skal rydde dit skrivebord for fortrollige informationer, når du går hjem. Fortrolige dokumenter skal være låst inde, f.eks. i et skab eller arkivrum. Dokumenter, der indeholder personoplysninger eller andre fortrollige informationer, skal du bringe til makulering dagligt.

Du kan læse mere om kriminalforsorgens ramme for opbevaring og sikring af fysiske dokumenter under Databeskyttelse og informationssikkerhed på intranettet (vælg Politikker og retningslinjer – Fysisk sikring af informationsaktiver og persondata).

Printer

Benyt Print-On-Demand ved udskrivning af dokumenter med personoplysninger eller andre fortrollige informationer.

Hvis Print-On-Demand ikke er muligt, skal du hente dine udprintede dokumenter med det samme. Tjek altid, at du sender dit print til den korrekte printer. Du skal ikke lade papirer med personoplysninger eller andre fortrolige oplysninger ligge tilgængelige i printeren.

Gør brug af skærmsfilter

Sørg for, at uvedkommende ikke kan følge med i dit arbejde på skærmen, når du arbejder, hvor din skærm kan ses udefra for eksempel i receptionen eller på gadeniveau. Det kan også være relevant at have skærmsfilter, hvis man sidder sammen i kontorer, hvor man ikke er beskæftiget med samme arbejdsområde. Et skærmsfilter hindrer andre i at se din skærm, mens du ser alt tydeligt. Tal med din leder om, hvorvidt du har behov for et skærmsfilter til dit arbejde.



Arbejde ved pc, mobil og tablet

Sikker adgangskode

Adgangskoder er personlige og må ikke deles med andre eller genbruges på tværs af systemer. Svar ikke på mails, der beder om dine adgangskoder og indtast dem kun i forbindelse med login.

Hvis du har mistanke om, at andre har fået kendskab til din adgangskode, skal du straks ændre den.

Vi anbefaler, at du bruger en sikker adgangskode på mindst 10 tegn med tal, store og små bogstaver samt specialtegn (for eksempel # eller %).

På din mobiltelefon eller tablet skal du benytte biometrisk identifikation (fingertryk el. lign.) eller en kode på minimum 6 cifre.

Benyt kun kriminalforsorgens it-udstyr

Brug kun it-udstyr, som du har fået udleveret af kriminalforsorgen til at udføre dit arbejde, og udlån ikke udstyret til andre. Brug ikke dit private it-udstyr som for eksempel privat pc eller telefon til at udføre dit arbejde.

Pc, mobil og lignende, der ikke er udleveret af Center for IT og Digitalisering, må ikke tilsluttes kriminalforsorgens pc'ere, andet udstyr eller kablede netværk.

Lås pc, mobil og tablet, når du ikke bruger den

Lås altid pc'en, når du forlader skærmen. Lås mobil eller tablet, når den ikke bruges.

Du låser hurtigt din pc ved at trykke "⏻+L".

Sørg for, at pin- eller adgangskode altid er aktiveret på din mobil eller tablet, så uvedkommende ikke kan få adgang til oplysninger, hvis enheden mistes.

Hvis pc, mobil, tablet eller andet udliveret udstyr bliver stjålet eller bortkommer, skal du straks kontakte Servicebureauet. Enten ved at ringe 4444 eller via Servicebureauet

Brug din mobil og/eller tablet varsomt

Vær opmærksom på sms fra ukendt telefonnummer, også kaldet smishing. Vær opmærksom på opkald fra udenlandske numre – det kan være "robotopkald", der kan ende med at koste mange penge. Svar ikke på opkald og ring ikke tilbage på opkaldene.

Du skal udvise varsomhed ved download af apps på din mobil, så du undgår uønsket adgang blandt andet til kamera og mikrofon.

Skriv ikke fortrolige oplysninger i din Outlook-kalender

Tænk over hvilke oplysninger, du skriver og deler i din Outlook-kalender. Kalenderne er åbne, så alle medarbejdere kan se de oplysninger, der fremgår i din kalender. Bemærk, at når du sætter mødelokale på mødeindkaldelsen, så vil information om mødet kunne ses i mødelokalets kalender, selvom mødet er markeret 'privat'. Derfor må du ikke skrive fortrolige eller følsomme personoplysninger eller fortrolige oplysninger generelt i kalenderen.

Skriv aldrig fortrolige og følsomme oplysninger i emnefeltet på mails

Emnefeltet vises meget tydeligt i Outlook, så uvedkommende også lettere kan se informationerne. Desuden er den tekniske beskyttelse af informationer, der står i emnefeltet, på et lavere niveau end den øvrige tekst i mailen. Derfor må du aldrig skrive CPR-numre eller andre fortrolige eller følsomme oplysninger i emnefeltet på mails.

Videresend ikke til din privatmail

Du må ikke videresende arbejdsoplysninger, der indeholder fortrolige eller følsomme oplysninger, til din private e-mail.



Tjek at det er den korrekte modtager

Du skal gøre det til en vane altid at dobbelttjekke din modtager. Hvis du er kommet til at sende mail med fortrolige informationer eller personoplysninger til forkert modtager, skal du straks anmelde hændelsen i Servicebureauet under Anmeldelse af informationssikkerhedshændelse.

Phishing-mails og andet spam

Du skal være meget varsom med at klikke på links eller vedhæftede filer i mails, hvis de ser mistænkelige ud. Hvis det ikke er en sikker kilde, eller indholdet er for godt til at være sandt, så undlad at klikke på links og vedhæftede filer, da det kan resultere i virus, og at data bliver misbrugt. Svar ikke tilbage på mistænksomme mails. I stedet skal du højreklikke på mailen og vælge uønsket og derefter bloker afsender. Mailen vil derefter blive rykket til uønsket mail. Hvis du er kommet til at klikke på linket, skal du kontakte Servicebureauet via Servicebureauet eller ringe på 4444.

Modtager du spam, kan du anmelde det. Det er vigtigt, at du følger nedenstående vejledning:

1. Marker e-mailen
2. Vælg **Filer**
3. Vælg **Gem som**
4. Vælg **Filtype Outlook-meddelelsesformat – Unicode (*.msg)**
5. Vælg **Gem**
6. Opret en ny e-post med emnet "Spam". Vedhæft den gemte spam og send e-posten til: spam@krfo.dk

En anmeldelse bidrager til at optimere spamfilteret. Der gives ikke retur svar ved fremsendelse til postkassen.

Spot en phishing-mail

Phishing-mails ligner til forveksling mails fra offentlige myndigheder, organisationer eller personer. Følg disse råd, når du skal vurdere, om en mail kan være et forsøg på phishing:

- Tjek afsenderen – afsenderadressen er ofte en efterligning af en officiel adresse (eks. @krfo-dk.dk i stedet for @krfo.dk)
- Er der en personlig hilsen? Manglende personlig hilsen er ofte et tegn på phishing
- Dårligt sprog. Nærlæs teksten, dårlig grammatik og ringe sprog fra automatiserede oversættelser kan tyde på udenlandske hackere
- Tidsfrister og konsekvenser. Stramme tidsfrister kan være tegn på phishing

Er det for godt til at være sandt?

Se efter mistænkelige telefonnumre eller manglende kontaktinformation. Pas på vedhæftede filer. Åbn ikke en vedhæftet fil, hvis du ikke venter en eller har tillid til afsenderen

Tjek links inden du klikker. Hold musen over linket inden du klikker – ser det mistænkeligt ud, så lad være med at klikke på linket

Du skal udvise samme agtpågivenhed ved modtagelse af sms'er.

På PC:

1. Kontakt Servicedesk på 4444 med det samme
2. Følg Servicedesks anvisninger

På Mobil:

1. Sluk for Wi-Fi og mobildata
2. Luk appen eller web-browseren
3. Kontakt Servicedesk på 4444 med det samme

Brug internettet og onlinetjenester med omtanke

Brug omtanke og almindelig sund fornuft, når du bruger internettet og onlinetjenester. Overvej hvilke hjemmesider du besøger, og hvilke links du klikker på for at minimere risiko for virus og misbrug af data.

Du må kun udfylde oplysninger på hjemmesider, der har https i adressen. Disse sider genkendes på, at der er en lås i adressefeltet:



Uden lås og https:

Du må ikke indtaste fortrolige eller følsomme oplysninger på siden.

Installer kun programmer og software, der fremgår af Serviceportalens Software Shop.

Følg kriminalforsorgens politik om brug af sociale medier, som du kan finde på intranettet.

Du må ikke gemme arbejdsdokumenter på private cloud-tjenester såsom iCloud, Dropbox, Google drev eller lignende.

Opdatér dit it-udstyr løbende

Din pc skal løbende opdateres, så den er beskyttet bedst muligt. Du skal derfor slukke din pc dagligt, så den løbende opdateres. Sluk også din pc, hvis du skal have den med til møde på en anden lokation.

Opdatér løbende din mobil og tablet med nye opdateringer. Hvis din mobil eller tablet ikke er sat op til automatiske opdateringer, skal du løbende manuelt sørge for det. Slår du automatiske opdateringer til, skal du stadig kontrollere, at opdateringerne rent faktisk gennemføres i praksis.

Sagsbehandling

Brug journal- og/eller fagsystem

Du skal bruge kriminalforsorgens journal- eller fagsystemer til at gemme personoplysninger eller andre typer af oplysninger, der er journaliseringspligtige.

Sikker brug af USB nøgle

Du må kun benytte USB nøgler, som er udleveret af kriminalforsorgen, og disse må kun benyttes på kriminalforsorgens udstyr. Det er ikke tilladt at benytte eksterne USB nøgler eller anvende USB nøgler, som har været brugt på eksternt udstyr. Eksterne USB nøgler kan indeholde skadelig software. Skal du opbevare kriminalforsorgens data på en USB-nøgle, skal den være krypteret (beskyttet med adgangskode). USB nøgler skal opbevares sikkert.

Journaliser og derefter slet mail

Du skal journalisere og/eller slette mails med fortrolige eller følsomme personoplysninger hurtigst muligt og senest 30 dage efter modtagelse eller afsendelse. Gør det til en god vane løbende at rydde op i din mailbox, så der ikke ligger fortrolige eller følsomme personoplysninger tilgængelige her.

Indhent og del kun oplysninger, når der er et arbejdsbetinget behov

Du må kun indhente og dele personoplysninger, når der er et fagligt behov. Hvis der ikke er et fagligt behov for, at informationen bliver delt, skal du afstå fra at dele. Vær opmærksom på, at din adfærd på pc'en bliver logget.

Du må ikke skaffe dig adgang til personoplysninger eller andre fortrolige informationer, der ikke er nødvendige for udførelsen af dine arbejdsopgaver.

Husk, at alle medarbejdere har tavshedspligt under og efter ansættelsen.

Send med sikker mail

Du skal altid sende følsomme og fortrolige oplysninger med sikker mail. Sikker mail afsendes via "Send Digitalt" i Outlook. Du kan læse mere om, hvordan du sender sikker mail på intranettet.



Tjek altid, at du sender mail til den korrekte modtager.

Arbejdsdokumenter på fællesdrev

Det er vigtigt at være opmærksom på, hvad der bliver placeret på fællesdrevet. Du må som udgangspunkt ikke gemme personoplysninger på fællesdrevet, og du må ikke foretage sagsbehandling vedrørende klienter eller medarbejdere på fællesdrevet.

Læs mere herom på intranettet under dokumenthåndtering.

Uden for arbejdspladsen

Adgangskort

Du må ikke bære arbejdskortet synligt for andre mennesker uden for arbejdspladsen.

Hold fortroligheden når du er på farten

Du skal afstå fra at drøfte følsomme eller fortrolige emner, hvis der er uvedkommende inden for hørevidde – det gælder også ved telefonsamtaler og samtaler i det offentlige rum.

Hvis det er nødvendigt for dig at medtage dokumenter med personoplysninger eller andre fortrolige informationer, skal du sikre, at materialet er opbevaret forsvarligt.

Gør brug af skærmlister

Sørg for, at uvedkommende ikke kan følge med i dit arbejde, når du arbejder offentlige steder. Brug et skærmlister, som hindrer andre i at se din skærm, men du ser alt tydeligt. Tal med din leder om, hvorvidt du har behov for et skærmlister til dit arbejde.

Pc, mobil og/eller tablet skal være under opsyn

Efterlad aldrig dit mobile udstyr uden opsyn, heller ikke i en låst bil. Når du rejser, skal pc, mobil og/eller tablet være i håndbagagen.

Brug kun sikker WiFi og VPN-adgang

Når du arbejder på din pc uden for kriminalforsorgen, så gør kun brug af sikre WiFi med kodeord og din VPN-adgang. Undgå offentlige internet-opkoblinger til at udveksle og tilgå personoplysninger. Opret i stedet et hotspot fra din tjenestetelefon, hvis du har fået en sådan udleveret.

Du må aldrig benytte fremmed it-udstyr til at udveksle og tilgå personoplysninger og udlån aldrig dit it-udstyr til fremmede personer.

Når du ikke længere arbejder i kriminalforsorgen, skal du huske, at du ved din ansættelse har underskrevet en erklæring om tavshedspligt. Pligten er gældende, også efter du er stoppet i kriminalforsorgen.

Adgangskort skal afleveres ved ansættelsens ophør.

Udleveret it-udstyr og mobile enheder skal afleveres til kriminalforsorgen.



Hvis uheldet skulle være ude...



Opdager du brud på persondatasikkerheden

ELLER:

Bliver du opmærksom på
informationssikkerhedshændelser



Benyt Serviceportalens formular:

Anmeldelse af informationssikkerhedshændelse

Hvis det IKKE er muligt at udfylde formularen,
så kontakt Servicedesk på 4444

Eksempler på
hændelser du skal
være opmærksom
på og reagere på:

- Tyveri af udstyr
- Systemfejl
- Forsyningssvigt – strømafbrydelse
- Brud på adgangskontrol
- Misbrug af systemer eller data
- Virus, spam, phishing, smishing, spyware og spear phishing.
- Hvis du har sendt oplysninger til en forkert modtager, eller det har været sendt med for lav sikkerhed





Læs mere på intranettet om
Databeskyttelse og informationssikkerhed

Direktoratet for Kriminalforsorgen

Center for IT og Digitalisering

Servicedesk 4444

