



JAMMERBUGT
KOMMUNE

Procedure for gennemgang af medarbejderes data herunder logoplysninger

*Beskrivelse af Jammerbugt Kommunes interne procedure for gennemgang af
medarbejderes data herunder logoplysninger.*

Revisionshistorik

Dato	Ændring	Version	Udført af	Godkendt af
10-09-2024	Dokument oprettet.	1.0	Sikkerhedsrådgiver	Chef for Digitalisering, Borger- service og Indkøb





Denne procedure har til formål at sikre korrekt og sikker håndtering af gennemgang af ansattes personlige oplysninger herunder e-mails, filer og logoplysninger. Det kan ske i forbindelse med, at en medarbejder ikke er i stand til at varetage sit arbejde, og at kommunen har brug for at tilgå oplysningerne for at kunne varetage sin myndighedsudøvelse. Det kan også ske i forbindelse med mistanke om en ansats misbrug af adgange, hvor kommunen er nødt til at undersøge sin mistanke via en gennemgang af logs. Behandlingsgrundlaget for offentlige arbejdsgivere er for begge scenarier forordningens artikel 6, stk. 1, litra e.

For begge situationer gælder det, at medarbejderne på forhånd - på en klar og utvetydig måde – skal være informeret om, at registreringen/logningen finder sted, og at registrering af adgange i it-løsninger, hjemmesidebesøg og brug af e-mails eventuelt vil blive gennemset som led i en kontrol ved mistanke om brug i strid med arbejdspladsens retningslinjer.

Fratrådte, fristillede eller fraværende medarbejders personlige data

Hvis en medarbejders ansættelse er ophørt, uden kommunen har sikret en tilstrækkelig overlevering, vil der i nogle tilfælde opstå praktiske udfordringer, som medfører, at kommunen får sværere ved at kunne levere sine ydelser og udføre sin myndighedsopgaver.

I forbindelse med orlov eller længerevarende fravær på grund af sygdom e.l. (NB: gælder ikke ferie) kan der også være et behov for, at afdelingen gennemgår en medarbejders personlige oplysninger, herunder får adgang til brugerkontoens it-skrivebord, Microsoft-konto, kalender, filer mv. med henblik på at varetage en kontinuerlig sagsbehandling.

I sådanne tilfælde har en leder mulighed for at tilgå den fratrådte medarbejders personlige oplysninger, hvis lederen samtidig sikrer overholdelse af nedenstående regler.

Der henvises desuden til dokumentet 'Princip om adgang til medarbejders data herunder logoplysninger', som yderligere beskriver, hvilke hensyn der skal tages ved gennemgang af medarbejders data.

Inden gennemgang

1. Leder skal forsøge at skaffe sig oplysningerne via den ansatte eller via andre veje, fx via borger, myndighed eller hovedpostkasse i kommunen.
2. Eventuelle oplysninger om en direkte e-mailadresse til den pågældende bør hurtigst muligt fjernes fra arbejdspladsens hjemmeside og fra andre offentligt tilgængelige informationssteder.
3. Leder orienterer den ansatte om den kommende gennemgang af de personlige data. Den ansatte skal tilbydes mulighed for at deltage i gennemgangen eller at fjerne fortrolige mails/filer før gennemgangen. Lederen skal også oplyse den fratrådte medarbejder om, at adgangen til brugerkontoen kun holdes åben i den periode, der er nødvendig for at sikre, at vigtig information ikke går tabt.





Under gennemgang

1. Brugerkontoen må kun holdes aktiv i en periode, der er så kort som muligt. Periodens længde fastsættes under hensyntagen til den fratrådte medarbejders stilling og funktion og kan maksimalt være på 12 måneder.
2. Under gennemgangen skal der indsættes et autosvar i Outlook med besked om medarbejderens fratræden og eventuel anden relevant information, fx *'Du har sendt en mail til en mailkonto, som er lukket. Din mail videresendes ikke. Du kan sende din mailmeddelelse på ny til [indsæt mailadresse].'*
3. Brugerkontoen må kun benyttes til at fremsøge og læse relevante oplysninger. Man må således ikke benytte kontoen til at oprette nye filer eller sende mails fra.
4. Kun en enkelt eller ganske få betroede medarbejdere bør have adgang til den fratrådte medarbejders konto. Nærmeste leder bestemmer, hvem og hvor mange der skal have adgang.
5. Under gennemgangen (dvs. når der logges på medarbejderens konto) skal en medarbejderrepræsentant, fx en tillidsrepræsentant, være til stede.

Ledere opretter en sag ved ServiceDesk, hvori det fremgår, hvem der skal have adgang til den fratrådte medarbejders brugerkonto, og i hvor lang tid adgangen skal foregå.

Brugerkonti tilhørende fristillede ansatte håndteres på samme måde som beskrevet ovenfor.

Mistanke om kriminelle forhold og/eller alvorlige brud på interne regler

Jammerbugt Kommune kan som arbejdsgiver tilgå ansattes personlige data og logoplysninger om den ansattes handlinger i relevante it-systemer, hvis kommunen mistænker den ansatte for kriminelle forhold eller alvorlige brud på interne regler.

I så fald skal nedenstående procedure følges. HR-afdelingen er primært ansvarlige for at håndtere sådanne sager, mens Digitalisering, Borgerservice & Indkøb understøtter den tekniske undersøgelse af hændelser.

Det er vigtigt, at alle sager om mistanke om kriminelle forhold eller alvorlige brud håndteres med en høj grad af fortrolighed, hvor kun få medarbejdere inddrages i håndteringen af sagen.

Procedure for håndteringen

1. Leder, som mistænker en medarbejder for kriminelle forhold eller alvorlige brud på kommunens interne retningslinjer, retter henvendelse til HR-afdelingen.





2. HR-afdelingen vurderer, hvorvidt mistanken er tilstrækkelig alvorlig og begrundet til, at man kan tillade en gennemgang af medarbejderens personlige data herunder logoplysninger. Vurderingen kan ske ud fra strafferetslige eller personalejuridiske betragtninger, fx alvorlige brud på forvaltningsloven.
3. Hvis HR-afdelingen mener, at man skal gennemgå logoplysninger, kontakter HR-chefen personligt chefen for Digitalisering, Borgerservice & Indkøb. HR-chefen oplyser i denne forbindelse følgende:
 - a. Hvilke handlinger, data og systemer der skal undersøges? Fx hvilke filer eller emner er relevante.
 - b. Eventuelt øvrige oplysninger som datoer, hvor den kriminelle handling skulle være foretaget, cpr.nr. på borgere, hvis oplysninger har været involveret i den formodede hændelse, eller andre relevante oplysninger, som er nødvendige for undersøgelsen.
4. Digitalisering, Borgerservice & Indkøb foretager fremsøgningen af relevante oplysninger, hvor så få ansatte som muligt inddrages i sagen.
5. Efter fremsøgningen af logoplysninger overdrager chefen for Digitalisering, Borgerservice & Indkøb relevante oplysninger til HR-chefen, som derefter vurderer, hvilke handlinger gennemgangen evt. giver anledning til (herunder politianmeldelse, personalesag, afskedigelse mv.).
6. HR-chefen er ansvarlig for at gemme relevant dokumentation fra gennemgangen på personalesagen, indtil det ikke længere er relevant. Oplysningerne må kun gemmes, så længe en aktuel sag er aktiv. Når sagen er afsluttet eller overdraget til Politiet, skal oplysningerne slettes. Dog kan HR-chefen og chefen for Digitalisering, Borgerservice & Indkøb i fællesskab drøfte mulighed for at gemme yderligere logudtræk i tilfælde af, at dokumentationen senere vil kunne blive relevant.
7. Den mistænkte medarbejder skal orienteres om sagen, så snart det er muligt, uden at dette kompromitterer kommunens mulighed for at undersøge sin mistanke. Hvis kommunen har grund til at tro, at medarbejderen på baggrund af en orientering om sagen kan misbruge sin adgang og sin position som ansat i kommunen, afventer kommunen en orientering til undersøgelsen er afsluttet. Nærmeste leder er ansvarlig for at orientere sin medarbejder efter aftale med HR-chefen.

