



# HR-lederens fortrolige informationer

**HR arbejder med fortrolige og personfølsomme informationer, og det kræver en særlig opmærksomhed og akkurate, at der ikke er dræn fra eller læk i organisationen.**

Af redaktør  
Peter Knoop Christensen

HR har en vital rolle, når det gælder medarbejdernes motivation for at opretholde den ønskede sikkerhed i en organisation. Selv det bedste sikkerhedssystem vil ikke virke, med mindre medarbejderne har forståelse for nødvendigheden af fortrolighed – personligt som kommercielt.

Lækage af fortrolige og følsomme informationer kan føre til dårlig medieomtale, manglende tillid fra medarbejdere og samarbejdspartnere eller påtale fra diverse myndigheder. Ifølge lovgivningen skal personfølsomme informationer behandles på betryggende vis, og man skal tage særlige forholdsregler, når man arbejder med følsomme informationer. I sidste ende kan lækage f.eks. medføre personlige tragedier.

Personfølsomme informationer skal opbevares sikkert, og det vil sige, at de skal opfylde lovkrav og interne instrukser i organisationen. Informationssikkerheden vil naturligvis blive udmøntet forskelligt hhv. i en produktproducerende virksomhed, en videntung organisation eller i en offentlig myndighed. Når det er sagt, er der langt flere ligheder end forskelle mellem de tre nævnte organisationstyper, når det gælder HR's opgave med at opretholde fortrolighed og informationssikkerhed.

## Når medarbejdere bliver ansat

HR's rolle er bl.a. at medvirke, når der ansættes, omplaceres og afskediges medarbejdere, og i disse opgaver er der forhold, HR skal give ekstra opmærksomhed i forhold til organisationens informationssikkerhed:

Når en medarbejder bliver ansat, omplaceret eller får nye opgaver og derigennem får adgang til ny information eller nye systemer, skal organisationen gennemføre en (ny) vurdering af medarbejderens adgang til fortrolig information, og der skal være procedurer og kriterier for en sådan vurdering: Hvem der kan og må udføre den, hvornår og hvorfor vurderingen skal udføres, og om vurderingen skal omfatte en straffeattest eller en særlig sikkerhedsgodkendelse. Der skal gennemføres en tilsvarende vurdering af midlertidigt ansatte.

Som en del af ansættelsen af faste og midlertidige medarbejdere skal arbejdsgiver og arbejdstager underskrive en aftale eller kontrakt, der beskriver organisationens og medarbejderens ansvar og forpligtelser for organisationens informationssikkerhed. I denne forbindelse skal medarbejderne introduceres til organisationens informationssikkerhedspolitik.

## Sikkerhed når medarbejderen fratræder

Ansvar et skal være klart defineret og placeret, når en medarbejder fratræder, således at ansættelsens ophør bliver håndteret korrekt og sikkert. HR skal beskrive procedurer for fratræden, så medarbejderen får afleveret alt udlånt udstyr, og medarbejderens fysiske og elektroniske adgang til organisationen bliver lukket.

Når en medarbejder – frivilligt eller ufrivilligt – fratræder, skal HR informere den fratrådte medarbejder om krav til informationssikkerheden og de juridiske regler, den fratrådte er underlagt. Hvis der i en tavshedserklæring eller en ansættelsesaftale er forpligtelser, der gælder efter fratrædelsen, skal HR informere udtrykkeligt om disse forpligtelser før medarbejderen fratræder.

## Kampagner stiller skarpt på sikkerheden

HR's rolle er også at træne og kompetenceudvikle organisationens medarbejdere. I forbindelse med organisationens informationssikkerhed er HR med til at sikre, at organisationens medarbejdere løbende bliver gjort opmærksomme på og uddannes i organisationens sikkerhedspolitik og -procedurer.

Løbende opmærksomhedskampagner – såkaldt 'awareness' – og træning kan f.eks. indeholde følgende:

- Organisationens krav til informationssikkerhed.
- Ansvar ifølge dansk lovgivning.
- Sikkerhedsforanstaltninger som er knyttet specifikt til organisationens forretningsgrundlag.
- Træning i korrekt anvendelse af organisationens hjælpeværktøjer og systemer, f.eks. log-on-procedurer.
- Organisationens regler om sanktioner.

Oplysning og træning skal være passende og relevant for medarbejdernes arbejdsopgaver og ansvarsområder, og træningen skal informere om aktuelt kendte trusler. Husk også at infor-

mere medarbejderne om, hvem de kan kontakte for yderligere råd om organisationens informationssikkerhed – og til hvem de skal rapportere kritiske hændelser.

HR har også *ansvar for, at organisationens informationssikkerhed ikke krænker personaleretslige (og andre lovgivningsmæssige bestemmelser), interne regler og etiske grænser, når medarbejdernes adfærd overvåges fysisk og på nettet.*

På Uddannelse & Udviklings hjemmeside finder du link til IT- og Telestyrelsens hjemmeside, som har en vejledning om awareness i organisationen og en tilhørende Power Point-præsentation, som HR kan tilrette og bruge i awareness-kampagner (i samarbejde med organisationens informations-sikkerhedsleder). ■

## HR-lederens Sikkerheds-ABC

Arbejdet med fortrolige og personfølsomme informationer kræver særlig opmærksomhed. HR skal sikre at:

- Elektroniske informationer bliver gemt på sikrede netværksdrev eller informationssystemer (f.eks. elektroniske sags- og dokumenthåndteringssystemer), hvor fortroligheden er sikret.
- Informationerne skal arkiveres i de godkendte sagsstyrings-systemer (Outlook er f.eks. ikke et godkendt sagsstyrings-system). Verserende sager kan ligge i en postmappe, så længe sagerne er i gang. Herefter skal dokumenter snarest muligt slettes fra postmappen og arkiveres i et relevant system.
- Udskrifter af fortrolige og følsomme dokumenter må ikke efterlades i printerrum og andre uovervågede lokaler.
- Dokumenter skal mærkes efter graden af krav til fortrolighed.
- Ingen uvedkommende må kunne lytte med, når HR-medarbejdere taler om en fortrolig og følsom sag. Dette gælder også telefonsamtaler.
- HR-medarbejdere låser døren til kontoret, når dette forlades for et kortere eller længere tidsrum i løbet af dagen.
- Fortrolige og følsomme informationer skal krypteres, hvis de skal transporteres på mobilt it-udstyr.
- Kasserede dokumenter skal sikkerhedsmakuleres.
- Kasseret udstyr, herunder USB-nøgler og cd'er, skal afleveres til sikker destruktion. Husk at oplyse, at udstyret har været benyttet til fortrolige og følsomme informationer, så udstyret bliver opbevaret forsvarligt, indtil sletning eller destruktion kan ske.
- Når HR-medarbejdere forlader arbejdspladsen, skal skrivebordet ryddes for fortrolige og følsomme dokumenter. Anbring dokumenterne i et aflåst skab eller en aflåst skuffe.