Jan Trzaskowski
- www.legalriskmanagement.com -

Politik for medarbejderes brug af virksomhedens IT

Jan Trzaskowski og Benjamin Lundström

Jan Trzaskowski og Benjamin Lundströms artikel og checkliste vedrørende medarbejderes brug af virksomhedens IT. [Artiklen har være publiceret på Computerworld online og i Børsens ledelseshåndbog.]

Ifølge den seneste årsrapport fra American Management Association (www.ama.org) om overvågning på arbejdspladser overvåger mere end ¾ af de større amerikanske virksomheder deres ansatte ved at tjekke e-mail, telefoner, computerfiler eller ved at videoovervåge medarbejderne på arbejdet. Hertil kommer, at ca. ¼ af virksomhederne har fyret ansatte for misbrug af virksomhedens e-mail eller for at have brugt internetforbindelsen til besøg på uautoriserede eller "upassende" Internet sider.

Problemstillingen er også relevant i Danmark, og virksomhederne bør fastlægge klare retningslinier for medarbejdernes anvendelse af IT både af hensyn til arbejdsmiljøet, men også for at overholde lovgivningen. Formålet med denne artikel er at redegøre for nogle af de elementer, som bør overvejes i forbindelse med udarbejdelse af en politik for medarbejderes brug af virksomhedens IT.

Selvom fokus hovedsagelig har været på virksomhedens overvågning af medarbejdernes private brug af virksomhedens IT, er der mindst ligeså relevant at fastsætte retningslinier for medarbejdernes erhvervsmæssige brug af IT. Virksomhedens IT omfatter bl.a. e-mail og world wide web ("Internet"), men også brug af f.eks. tekstbehandling mv.

Ved fastlæggelse af IT-politikken bør man tage højde for lovmæssige rammer herunder persondatalovens regler om overvågning, sikkerhedskopiering og gennemgang af logfiler mv. Derudover bør politikken afstemmes i forhold til virksomhedens personalepolitik og IT sikkerhedspolitik.

1. Den private anvendelse af virksomhedens IT

Hele diskussionen om privat anvendelse af virksomhedens IT starter ved spørgsmålet, om hvorvidt medarbejderen overhovedet må anvende virksomhedens IT til private formål. Der kan være mange saglige grunde til ikke at tillade privat anvendelse af virksomhedens IT. På den anden side kan der være væsentlige fordele ved at tillade privat brug af virksomhedens IT, f.eks. ved den større fleksibilitet der opnås, ved at den ansatte kan anvende

netbanker og online varebestillinger, eller mere generelt ved at medarbejderne ved IT anvendelse også hjælper med kompetenceudviklingen i virksomheden.

Gevinsten ved en liberal og progressiv politik om privat brug af virksomhedens IT vil typisk afspejles i medarbejdertilfredsheden. Virksomheden må dog også forholde sig til sin IT sikkerhedspolitik.

Klare retningslinier for privat anvendelse af virksomhedens IT vil under alle omstændigheder medføre mindre usikkerhed hos medarbejderne om, hvad der er tilladt og vil tillige være en juridisk nødvendighed for at virksomheden kan begrænse, overvåge og sanktionere medarbejderens IT anvendelse. Formålet bør beskrives så præcist som muligt, men der kan ofte være behov for mere bløde vendinger i form af hensigtserklæringer. Retningslinierne bør naturligvis afspejle virksomhedens reelle politik, og direkte forbud bør ikke formuleres blødt.

For det tilfælde, at man tillader privat anvendelse af virksomhedens IT, er første opgave at sikre, at private dokumenter, filer, e-mails mv. tydeligt adskilles fra erhvervsmæssigt materiale. Der bør således fastsættes retningslinier for mærkning og placering af privat materiale.

Dernæst må man tage stilling til om der skal fastsættes regler for omfanget og tidspunkterne for den private anvendelse. Det må f.eks. være en klar forudsætning, at den private brug ikke går udover medarbejderens arbejdsindsats eller f.eks. sker på et tidspunkt, hvor virksomhedens båndbredde bør dedikeres til erhvervsmæssig brug.

Virksomheden må også tage stilling til, hvilke private aktiviteter virksomheden vil tillade. Det må her være en naturlig forudsætning, at medarbejderens aktiviteter er lovlige og at aktiviteterne ikke skader virksomheden, kunder eller andre medarbejdere. Det kan også være, at virksomheden ønsker at hindre besøg på pornografiske sites, rundsendelse af vittigheder eller anvendelse af chatprogrammer.

Virksomheden må også i retningslinierne forholde sig til håndtering af filer, som modtages via mail, downloades fra Internettet eller medbringes på disketter eller CD-rom. Udover at virksomheden naturligvis må sikre sig, at virksomheden eller medarbejderen har de nødvendige licenser, må virksomheden også forholde sig til risikoen for vira. Lagring af filer vil også kunne belaste virksomhedens systemressourcer i uforholdsmæssigt omfang.

I den forbindelse må virksomheden endvidere tage stilling til medarbejderens mulighed for selv at installere programmer mv. på virksomhedens computer. Medarbejderens egen installering kan påvirke EDB systemets stabilitet, og det kan være hensigtsmæssig at fastsætte retningslinier for, hvorvidt og i givet fald hvornår den systemansvarlige skal inddrages.

Virksomheden må også forholde sig til, om medarbejderen må bruge virksomhedens e-mail system til privat brug eller om medarbejderen skal opfordres til at bruge et af de mange webbaserede mailsystemer til privat e-mail korrespondance. Herved undgår virksomheden, at der lagres private e-mails i indbakken sammen med de erhvervsmæssige e-mails. Desuden kommer virksomheden ikke til at stå som afsender, hverken i e-mail adresse eller i autosignaturer.

Endelig bør virksomheden tage stilling til, hvorledes medarbejderen skal rydde op på sin computer og orientere omgivelserne i tilfælde af ophør af ansættelsesforholdet. Det kan f.eks. overvejes om virksomheden skal hjælpe medarbejderen med at gemme privat materiale i sådanne tilfælde. Endelig må der tages stilling til, hvorvidt medarbejderens mailbox skal lukkes, eller e-mail skal videresendes til en bestemt adresse.

Virksomhedens politik for medarbejdernes private brug af virksomhedens IT må nødvendigvis være en afvejning af virksomhedens vilje til at give medarbejderne fleksible rammer og på den anden side beskytte virksomhedens sikkerhed og profil. Retningslinierne må navnlig afvejes i forhold til EDB-anlæggets dimensionering og sikkerhedsniveau, samt den systemansvarliges ressourcer. Systemnedbrud har stor betydning for moderne virksomheder, og man bør derfor sikre et sikkerhedsniveau, der kan matche virksomhedens retningslinier for medarbejderens brug af virksomhedens IT.

2. Den erhvervsmæssige anvendelse af virksomhedens IT

Virksomheder har typisk traditioner eller egentlige standarder for håndteringen af papirbaseret korrespondance. Det samme er sjældent tilfældet for den elektronisk kommunikation. Elektroniske kommunikation er mere flygtig end papir, men er mindst ligeså vigtig for virksomheden, og der er derfor også behov for retningslinier for erhvervsmæssig anvendelse af virksomhedens IT.

Medarbejdernes brug af virksomhedens IT bør tilrettelægges således, at virksomheden let kan få adgang til e-mail, dokumenter, filer mv. i tilfælde af ferie, sygdom og lignende. Det stiller bl.a. krav til den anvendte mappestruktur, som bør være ens for alle medarbejdere. Derudover stiller det også krav til navngivningen af dokumenter og filer, da det bør være forholdsvis simpelt at fastslå, hvilke udkast der er det seneste, og hvornår der er tale om en udgave, der f.eks. er sendt til kunden.

Der bør også laves retningslinier for, hvorledes fravær i forbindelse med ferie, sygdom mv. håndteres. Der skal således tages stilling til, om der skal anvendes autosvar med henvisning til kollegaer i hastende tilfælde eller hvorvidt en kollega skal passe medarbejderens indbakke. De nordiske forbrugerombudsmænd fastslog i 1998, at e-mail bør gøres tilgængelige for virksomheden hurtigst muligt, også selvom adressaten på grund af ferie, sygdom mv. er fraværende.

Et andet fundamentalt forhold, der skal tages stilling til, er hele spørgsmålet om, hvornår kommunikation med interne og eksterne aktører bør foregå elektronisk, og om der i bestemte situationer skal anvendes digitale signaturer og/eller kryptering.

Endvidere bør der tages stilling til brugen af autosignaturer og det sprog, der anvendes i e-mail. Det bør virksomheden, der fastlægger en ensartet politik for anvendelse af autosignaturer og det kan overvejes, om der skal indføres rutiner for korrekturlæsning og godkendelse af e-mail, der traditionelt er skrevet og sendt ganske hurtigt og desuden fyldt med stavefejl og andre sproglige forteelser.

I og med at elektroniske materiale er et vigtig element i virksomhedens korrespondance, bør der tages stilling til spørgsmålet om journalisering, lagring og sletning af e-mail, dokumenter og filer.

Endelig bør der tages stilling til en række spørgsmål omkring anvendelse af virksomhedens IT, herunder dokumenter, e-mail mv. uden for virksomhedens fysiske rammer. Udover den grundlæggende holdning til hjemmearbejde, skal virksomheden bl.a. tage stilling til spørgsmål vedrørende arbejdsmiljø og IT sikkerhed, hvoraf sidstnævnte bør behandles i virksomhedens generelle IT sikkerhedspolitik.

3. Arbejdsgivers overvågning mv.

Virksomhedens registrering og undersøgelse af medarbejderes brug af virksomhedens IT er omfattet af straffeloven, persondataloven og arbejdsmiljølovgivningen, og alene af den grund kan det være hensigtsmæssigt at få lavet retningslinier for især logning, sikkerhedskopiering og gennemgang af lagrede oplysninger.

Ifølge persondataloven skal medarbejderen på en klar og utvetydig måde være informeret om, at registrering/logning af personhenførbare oplysninger finder sted, og at det registrerede eventuelt vil blive gennemset som led i en kontrol ved mistanke om brug af virksomhedens IT i strid med arbejdspladsens retningslinier herom. Det fremgår endvidere af bekendtgørelse om arbejde ved skærmterminaler, at der ikke må anvendes kvantitativ eller kvalitativ kontrol uden de ansattes vidende.

Man behøver ikke at lave en egentlig aftale med den enkelte medarbejder, men det anbefales, at virksomheden er omhyggelig med at sikre at alle medarbejdere orienteres om retningslinierne. Retningslinierne bør som minimum vedlægges ved ansættelsen og fremgå af virksomhedens intranet.

Et af de grundlæggende krav i persondataloven er, at indsamling af oplysninger kun må ske til udtrykkeligt angivne og saglige formål, og senere behandling ikke må være uforenelig med disse formål. Desuden er det et krav, at behandlingen nødvendig for, at arbejdsgiveren kan forfølge berettigede interesser, og hensynet til de ansatte ikke overstiger arbejdsgiverens interesser. Som eksempel på en berettigede interesser kan f.eks. være tekniske og sikkerhedsmæssige hensyn, samt hensynet til kontrol af medarbejdernes brug af Internettet.

Af politikken bør det fremgå, at der foretages logning og i hvilke situationer virksomheden vil gennemgå logfiler, e-mail eller dokumenter. Det kan f.eks. være i tilfælde af mistanke om kriminel handling eller andre handlinger i strid med retningslinierne for anvendelse af virksomhedens IT. I den forbindelse er det vigtig at være opmærksom på, at en gennemgang ikke må stride mod formålet for registreringen af oplysningerne. Det er derfor vigtigt at være omhyggelig med formuleringen af formålet.

Fremgangsmåden for gennemgangen af logfiler mv. bør præciseres i retningslinierne, herunder om der i visse situationer skal ske varsel eller efterfølgende orientering. Det kan være, at medarbejderen, tillidsrepræsentanten eller den personaleansvarlige skal være tilstedes under

gennemgangen. Endelig kan der være behov for at medarbejderen f.eks. skal have mulighed for at kommentere eventuelle konklusioner af gennemgangen.

Ved at have klare retningslinier for markering og placering af privat materiale og en generel regel om at medarbejderen skal anvende webbaserede e-mailsystemer til privat post, begrænses omfanget af personoplysninger til logningen af medarbejderens brug af IT, og der er derfor ikke overhængende risiko for kompromittering af medarbejderens private materiale.

For en god ordens skyld skal det understreges at det efter straffeloven som udgangspunkt er strafbart at læse eller unddrage nogen deres breve og lignende, herunder e-mail. I det omfang en e-mail er af privat karakter, er arbejdsgiveren således som udgangspunkt uberettiget til at gøre sig bekendt med indholdet eller at omdirigere e-mailen.

Hvis ikke e-mailen er markeret i overensstemmelse med retningslinierne, må det dog i praksis accepteres, at arbejdsgiveren læser så meget af en privat e-mail, at han rent faktisk kan identificere e-mailen som privat.

4. Checkliste (grundelementerne i en IT politik)

Checklisten er en ikke udtømmende oversigt, der giver et overblik over nogle af de væsentligste forhold, der skal tages stilling til ved fastlæggelse af en politik for medarbejderes brug af virksomhedens IT.

4.1. Privat brug af virksomhedens IT

- Tillades privat brug af e-mail, www (”Internet”) og andet EDB udstyr?
- Hvordan markeres og lagres private e-mails, dokumenter og filer?
- Skal den private brug holdes inden for et bestemt tidsrum eller omfang?
- Hvilke aktiviteter er tilladt eller forbudte?
- Holdning til download eller anden håndtering af software og filer.
- Holdning til medarbejderens egen installation af programmer mv.
- Eventuelle grænser for lagerkapacitet, der må bruges privat.
- Krav om anvendelse af webbaseret mailservice til privat e-mail.
- Fremgangsmåde ved ophør af ansættelsesforholdet.

4.2. Erhvervsmæssig brug af virksomhedens IT

- Retningslinier for filplaceringer, mappestrukturer og navngivning.
- Rutiner i forbindelse med ferie, sygdom mv.
- Hvilken kommunikation må ske pr. e-mail?
- Hvornår skal der anvendes digital signatur?
- Retningslinier for godkendelse af sprog og indhold af e-mail.
- Udformning af autosignaturer, herunder ansvarsfraskrivelser mv.
- Journalisering og opbevaring af indgående og udgående e-mail.
- Retningslinier for rapportering om uregelmæssigheder i EDB anlægget.
- Retningslinier for kvittering ved modtagelse af e-mail.
- Holdning til hjemmearbejde eller anden håndtering af virksomhedens materiale uden for virksomhedens lokaler.

- Principper for brug af gratis Internettjenester (f.eks. oplysningen).

4.3. Sikkerhedskopiering, registrering, logning og overvågning

- Hvad er formålet med overvågningen, logningen mv.?
- Hvad overvåges (automatisk eller manuel overvågning)?
- Hvor længe og hvordan opbevares oplysninger?
- Hvem har adgang til oplysningerne?
- Hvor tit tages der sikkerhedskopier, og hvad lagres?
- I hvilke situationer gennemgås den lagrede information?
- Fremgangsmåde ved gennemgangen.
- Præcisere, at privat e-mail mv. ikke må læses.