

Brug af e-post og internet på arbejdspladsen

Inspirationspapir til private virksomheder og offentlige myndigheder

E-post og internettet er blevet et dagligt og vigtigt arbejdsredskab i mange stillingsfunktioner. Medarbejderes brug af disse kommunikationsværktøjer giver nogle åbenbare fordele, men har vist sig også at give anledning til nye problemer.

Denne publikation fra IT-Sikkerhedsrådet beskriver en række af de forhold, der typisk vil være relevante, når en organisation ønsker at fastlægge retningslinjer for brug af e-post og internet i en e-post- og internetpolitik.

Publikationen henvender sig især til ledelsen, IT-ansvarlige og eventuelt andre medarbejdere med særlige IT-kvalifikationer (superbrugere), organisationens human ressource-afdeling samt øvrige medarbejdere, der er beskæftiget med indførelse af en e-post- og internetpolitik i private virksomheder eller offentlige myndigheder.

Brug af e-post og internet på arbejdspladsen

Inspirationspapir til private virksomheder og offentlige myndigheder



Brug af e-post og internet på arbejdspladsen

**Inspirationspapir til private virksomheder og
offentlige myndigheder**

Brug af e-post og internet på arbejdspladsen

*Inspirationspapir til private virksomheder og
offentlige myndigheder*

Publikationen kan købes ved
henvendelse til:
Statens Information
Postboks 1300
2300 København S
Tlf. 3337 9228
Fax 3337 9280
E-post sp@si.dk
Pris ved løssalg 50,- kroner inkl. moms

Publikationen kan også hentes på
Ministeriet for Videnskab, Teknologi og
Udviklings hjemmeside
<http://www.fsk.dk>
ISBN (Internet): 87-90890-78-7

Udgivet af:
IT-Sikkerhedsrådet
c/o Ministeriet for Videnskab, Teknologi og
Udvikling
Bredgade 43
1260 København K
Tlf. 3392 9700
Fax 3332 3501
E-post fsk@fsk.dk

Tryk: K. Larsen & Søn A/S
Oplag: 4.000
ISBN: 87-90890-77-9

Forsideillustration:
Lars Refn

FORORD

At IT-sikkerhed er mange ting fremgår blandt andet af kommissoriet for IT-Sikkerhedsrådet. Ifølge dette har rådet blandt andet til opgave at pege på de menneskelige og samfundsmæssige risici og interesser, som den moderne informationsteknologi giver anledning til, og det er i den forbindelse - blandt andet - lagt i hænderne på rådet at tage „bredere IT-sikkerhedsproblemstillinger op til drøftelse“ i det omfang rådet føler behov herfor.

Den foreliggende vejledning har rod i denne del af kommissoriet. Emnet er de retningslinier, en organisation måtte ønske at fastlægge for sin brug af e-post og internet. Vejledningen retter sig især til ledelsen i private og offentlige virksomheder, IT-ansvarlige og andre med særlige IT-kvalifikationer („superbrugere“), samt til personaleansvarlige og tillidsrepræsentanter, der i en eller anden henseende bliver inddraget i dette vigtige arbejde. Emnerne er vidtspændende: Hvornår skal arbejdsgiveren kunne opnå adgang til medarbejderes e-post og hvilke regler gælder der herfor? Hvilke typer af meddelelser egner sig overhovedet til dette medium? Og hvad skal gælde med hensyn til sprog, tone og indhold af e-post, omgang med filer, surfing på internettet og så videre?

Ved at tage disse brede problemstillinger op ønsker IT-Sikkerhedsrådet at sætte fokus på det spektrum af vanskelige problemstillinger, der opstår i forsøget på at skabe hensigtsmæssige og gennemsigtige retningslinier om denne hyppige kilde til konflikt i IT-anvendelsen. Sammenligner man denne med andre af rådets vejledninger har det ikke været ønsket at fremlægge mere færdige løsninger. På de områder, hvor grænserne for en sådan politik sættes af juraen, er dette præciseret, men i øvrigt er det hovedformålet at give de involverede mulighed for at skabe den bedste „hjælp til selvhjælp“ i forsøget på at finde en hensigtsmæssig regulering.

Praksis for brug af e-post på internet er i en stadig bevægelse. Såvel afgrænsningen af de problemstillinger, der er relevante, som anvisningerne

på, hvorledes man skal gå frem for at løse disse spørgsmål, vil derfor ofte forandre sig over tid. Uanset hvilken holdning organisationen har til de anvisninger, der lægges frem, og uanset løsningsvalg vil det derfor være nødvendigt, at organisationen løbende overvejer om den til enhver tid har den mest hensigtsmæssige politik for internet og e-post.

IT-Sikkerhedsrådet har udarbejdet denne vejledning under medvirken af Bech-Bruun Dragsted, advokatfirma.

København, januar 2002

Mads Bryde Andersen
Professor, dr.jur.
Formand for IT-Sikkerhedsrådet
mads.bryde.andersen@jur.ku.dk

INDHOLD

3	Forord
7	1. Indledning
11	2. Strategiske valg ved fastlæggelse af en e-post- og internetpolitik
11	2.1 Skal e-post og internet kunne anvendes til privat brug?
14	2.2 Skal e-post og internetbrug kunne kontrolleres?
20	2.3 Skal aftaler på vegne af organisationen kunne indgås ved brug af e-post?
22	2.4 Implementering af særlige systemer til sikkerhed for e-postmeddelelsers ægthed, fortrolighed med videre
24	2.5 I hvilket omfang skal medarbejderne inddrages i fastlæggelsen af retningslinjerne?
27	3. Indholdet af en e-post- og internetpolitik
27	3.1 Procedurer ved afsendelse af e-post
34	3.2 Procedurer ved modtagelse af e-post
39	3.3 Journalisering, arkivering og sletning af e-post
41	3.4 Aftaleindgåelse via e-post og internet
42	3.5 Begrænsninger i den private brug

44	3.6	Kontrol af e-post og internetbrug
47	3.7	E-post i forbindelse med fratræden
48	3.8	Overtrædelse af e-post- og internetpolitikken
51	4.	Information om og vedtagelse af en e-post- og internetpolitik
53		Bilag

Huskeliste til brug i forbindelse med udarbejdelse af politik for medarbejderes brug af e-post- og internet (ikke udtømmende)

1. INDLEDNING

E-post og internettet er blevet et dagligt og vigtigt arbejdsredskab i mange stillingsfunktioner. Fordelene ved disse kommunikationsværktøjer er åbenbare, men flere eksempler fra de seneste år har vist, at det også giver anledning til nye problemer, når de i organisationen beskæftigede (herefter benævnt „medarbejderne“) udstyres med adgang til e-post og internet.

Da mange af problemerne udspringer af, at der endnu ikke som ved almindelig skriftlig korrespondance er etableret udbredte opfattelser af, hvad der er god omgang og god tone ved brug af nye kommunikationsværktøjer, kan problemerne i mange tilfælde undgås, hvis der foreligger klare retningslinjer for, hvordan medarbejderne skal omgås e-post og internet.

Denne publikation fra IT-Sikkerhedsrådet beskriver en række af de forhold, der typisk vil være relevante, når en organisation ønsker at fastlægge retningslinjer for brug af e-post og internet i en e-post- og internetpolitik.

Publikationen målretter sig både mod udarbejdelse af e-post- og internetpolitik for medarbejdere i private virksomheder og offentlige myndigheder (herefter tilsammen benævnt „organisationer“). Publikationen vil også generelt kunne anvendes som inspirationsgrundlag ved fastlæggelsen af retningslinjer for andre personer knyttet til organisationen end medarbejderne, for eksempel bestyrelsesmedlemmer i private virksomheder eller kommunalpolitikere, der udstyres med en kommunal e-postadresse. Det er dog vigtigt i den forbindelse at understrege, at organisationen i forhold til denne persongruppe ikke har en generel instruktionsbeføjelse eller ledelsesret, og at retningslinjerne derfor bør være udtømmende reguleret i en aftale mellem parterne.

Publikationen henvender sig især til ledelsen, IT-ansvarlige og eventuelt andre medarbejdere med særlige IT-kvalifikationer (superbrugere),

organisationens human ressource-afdeling samt øvrige medarbejdere, der er beskæftiget med indførelse af en e-post- og internetpolitik i organisationen.

Forud for udarbejdelsen af e-post- og internetpolitikken konkrete retningslinjer må organisationen træffe nogle valg af mere strategisk karakter med hensyn til privat brug, kontrol, systemsikkerhed og inddragelse af medarbejderne. Disse valg, der er beskrevet i afsnit 2, vil være spørgsmål, som ledelsen må tage stilling til. Afsnit 2 er med andre ord primært målrettet mod ledelsen.

På baggrund af de strategiske valg kan e-post- og internetpolitikken udarbejdes. En e-post- og internetpolitik vil normalt indeholde en lang række konkrete anvisninger til, hvordan der skal handles ved den daglige håndtering af e-post og internet i organisationen. Disse spørgsmål er behandlet i publikationens afsnit 3, der omhandler det nærmere indhold af en e-post- og internetpolitik, herunder procedurer ved afsendelse, modtagelse, journalisering, arkivering og sletning af e-post samt fastlæggelse af nærmere retningslinjer for privat brug, information om kontrolforanstaltninger, behandling af fratrådte medarbejders e-post og sanktioner ved overtrædelse af retningslinjerne.

Arbejdet med udfærdigelsen af de konkrete retningslinjer vil typisk ikke forestås af ledelsen men af en projektgruppe ofte bestående af organisationens IT-ansvarlige, human ressource-personale og eventuelt medarbejderrepræsentanter. Afsnit 3 er primært målrettet mod den projektgruppe, der forestår arbejdet med udformningen og gennemførelsen af e-post- og internetpolitikken.

I afsnit 4 beskrives spørgsmål om vedtagelse af og information om den udarbejdede e-post- og internetpolitik. Dette afsnit er relevant for både ledelsen og projektgruppen.

Selvom det ofte kun vil være de i afsnit 2 beskrevne strategiske valg, og ikke de valg, der er knyttet til udarbejdelsen af de konkrete retningslinjer, der vil blive truffet på ledelsesniveau, er det væsentligt at understrege, at udformningen af en e-post- og internetpolitik i sidste ende altid vil være

et ledelsesansvar og overordnet set udgøre en del af organisationens IT-sikkerhedspolitik.

Endelig er det vigtigt at understrege, at det ikke er muligt at udarbejde en standard e-post- og internetpolitik, der passer til alle organisationer. Formålet med publikationen er at sætte fokus på generelle problemstillinger og at identificere en række mere konkrete problemstillinger. Derigennem er det IT-Sikkerhedsrådets håb, at publikationen kan tjene som et inspirationspapir forud for organisationens udarbejdelse af sin egen individuelt tilpassede e-post- og internetpolitik.

2. STRATEGISKE VALG VED FASTLÆGGELSE AF EN E-POST- OG INTERNETPOLITIK

2.1 Skal e-post og internet kunne anvendes til privat brug?

Der er i Danmark en tradition for, at medarbejdere i begrænset omfang kan ordne private ærinder over telefon i arbejdstiden, og mange steder er der også allerede etableret en organisationskultur, der accepterer en vis privat brug af e-post og internet. Medarbejdere vil derfor ofte have en *forventning* om, at privat brug af e-post og internet i et givet omfang kan foretages på arbejdspladsen i arbejdstiden. E-post er endvidere blevet en del af den kollegiale kommunikation mellem medarbejdere, herunder i kommunikationen med sikkerhedsrepræsentanter med videre.

Den private brug af e-post og internet på arbejdspladsen kan dog føre visse *ulemper* med sig. Ved organisationens vurdering af, om privat brug skal tillades, må sådanne eventuelle ulemper identificeres og afvejes.

Den første og mest åbenbare ulempe ved privat brug af e-post og internet kan være, at medarbejderne bruger mere *arbejdstid* på private gøremål. Tillader organisationen i øvrigt, at der foretages private småærinder og telefonsamtaler, vil denne ulempe næppe være afgørende. Et forbud mod privat brug af e-post vil ofte medføre, at kommunikationen i stedet foretages via telefon, hvorved der alligevel vil medgå arbejdstid.

Brug af privat e-post og internet kan for det andet øge risikoen for, at der lagres og rundsendes forskellige former for *filer* i organisationens e-post-system. Sådanne filer kan både være virusinficeret og i det hele taget belaste systemets kapacitet. Forbud mod brug af e-post kan dog ikke hindre, at filer sendes til medarbejdere men vil kunne hindre, dels at filer videregives, herunder til andre medarbejdere, dels at filer hentes fra internettet. Dette resultat kan dog også opnås som led i den almindelige IT-sikkerhedspolitik ved blot at forbyde at bestemte typer filer åbnes og videresendes i

private e-postmeddelelser og hentes fra internet, eventuelt kombineret med, at organisationens system automatisk bortfiltrerer bestemte filtyper.

En tredje ulempe ved den private brug af e-post er risikoen for, at medarbejdere sender e-postmeddelelser med et i forhold til organisationen eller visse modtagere *stødende indhold* fra den e-postadresse, organisationen har stillet til deres rådighed. Ofte vil organisationens navn fremgå af e-postadressen (medarbejder@organisation.dk), og organisationen risikerer derfor at blive associeret med en e-postmeddelelse, som ikke stemmer overens med organisationens værdigrundlag.

Den nævnte risiko kan dog imødegås ved at forbyde medarbejdere at sende e-postmeddelelser med stødende indhold, for eksempel meddelelser med seksuelt eller racistisk indhold, meddelelser der indeholder nedsættende omtale af andre medarbejdere, vittigheder om minoritetsgrupper med videre. Dette emne er reelt en del af organisationens almindelige politik, som der imidlertid kan være særlig grund til at fremhæve i forbindelse med brug af e-post, fordi e-post er så oplagt et kommunikationsmiddel til uformel kommunikation.

En anden mulighed er at tillade medarbejderne at gøre privat brug af en e-postadresse fra en af de hjemmesider, der tilbyder gratis e-postfaciliteter (som for eksempel Hotmail). Hermed vil organisationen ikke umiddelbart blive associeret med e-postmeddelelsen. Denne løsning er dog mere tidskrævende, da medarbejderen skal logge sig på den pågældende hjemmeside, hver gang en e-postmeddelelse skal sendes og i øvrigt med mellemrum skal logge sig på siden for at se, om der er kommet nye meddelelser. Herudover skal organisationen være opmærksom på, at det ikke vil være muligt at føre samme kontrol med e-post, der afsendes og modtages fra hjemmesider, som med e-post, der afsendes og modtages i organisationens eget postsystem. Det kan heller ikke udelukkes, at der vil være gråzoneområder, hvor det vil være vanskeligt at afgøre, om noget er „helt“ privat. Organisationens må i lyset af de påpegede fordele og ulemper overveje, om den vil tillade brug af sådanne e-postadresser.

Som beskrevet kan ulemperne ved privat brug af e-post og internet imødegås ved nærmere fastsatte begrænsninger i anvendelsen. Det er imidlertid *vanskeligere at kontrollere*, om medarbejderne overholder sådanne begrænsninger, end det er at kontrollere overholdelsen af et generelt forbud mod privat e-post. Regler om begrænset brug af privat e-post kan ligeledes medføre *uenighed og diskussion om, hvor grænsen går*, som kan undgås ved et totalt forbud mod privat brug.

I sidste ende må udfaldet af *afvejningen mellem fordele og ulemper* bero på kulturen i den enkelte organisation. I mange organisationer vil der utvivlsomt være en forventning om, at man i et vist omfang kan gøre privat brug af e-post, og et forbud herimod kan føre til en utilfredshed, der kan være til større gene, end de beskrevne ulemper, der undgås ved helt at forbyde privat brug af e-post.

Hvis organisationen vælger at tillade privat brug af e-post og internet, skal der som led i e-post- og internetpolitikken beskrives *retningslinjer for omfanget af brugen*. Retningslinjerne skal sikre, at den private brug af e-post i arbejdstiden ligger indenfor de af organisationen afstukne rammer, og at de forventninger, organisationen har til medarbejderens brug, gøres så synlige som muligt. Udformningen af retningslinjerne er beskrevet i afsnit 3.5.

Der er *ingen lovgivning*, der særskilt regulerer spørgsmålet om privat brug af e-post, og det er derfor organisationens frie valg, om den vil tillade privat brug eller ej.

I hvilket omfang skal e-post og internet kunne anvendes privat?

Vurdér, om der er behov for at fastlægge de nærmere grænser for privat brug i organisationens e-post- og internetpolitik, eventuelt ved at angive eksempler.

2.2 Skal e-post og internetbrug kunne kontrolleres?

Organisationen må overveje, i hvilket omfang der er behov for at foretage logning og sikkerhedskopiering af medarbejdernes e-postmeddelelser. Ligeledes må det overvejes, i hvilket omfang der skal ske gennemlæsning af e-postmeddelelserne. Tilsvarende skal det vurderes, om der skal ske logning af de hjemmesider, medarbejderen besøger.

Der er ikke en tradition i Danmark for en meget intens kontrol af medarbejders brug af kommunikationsmidler. En sådan kontrol vil kunne skabe utryghed og utilfredshed i organisationen.

Det må dog betegnes som en udbredt og generelt accepteret praksis, at organisationer foretager en vis kontrol af medarbejdernes brug af e-post og internet, dels af sikkerheds- og driftshensyn dels til sikring af, at medarbejderne overholder organisationens gældende regler for brug af e-post og internet.

Da kontrol af medarbejderens adfærd, herunder medarbejderens forskellige former for kommunikation, kan være en ganske indgribende foranstaltning, indeholder *lovgivningen* grænser for den intensitet, hvormed en sådan kontrol må foretages. Organisationen må sikre sig, at disse grænser respekteres. De væsentligste regelsæt er lov om behandling af personoplysninger (persondataloven), straffelovens regler om brevhemmelighed og arbejdsretlige regler om kontrol af arbejdstagere. Nedenfor følger en kort orientering om disse regler efterfulgt af en sammenfatning.

Persondataloven

Persondataloven regulerer, i hvilket omfang personoplysninger må registreres og bruges i øvrigt. Som personoplysning anses enhver oplysning, der kan føres tilbage til enkeltpersoner, for eksempel navn, fødselsdag og bopæl. Oplysninger om, hvilke e-postmeddelelser en person har modtaget eller sendt, tidspunktet for modtagelse eller afsendelse, hvilke hjemmesider en person har besøgt og tidspunktet herfor, vil være personoplysninger.

Loven bygger på en række grundlæggende principper, herunder at oplysninger kun må indsamles til et konkret angivet og sagligt formål. Enhver form for registrering og anden behandling af personoplysninger kræver som udgangspunkt samtykke fra den, oplysningerne vedrører. Loven angiver dog en række situationer, hvor behandlingen kan ske uden samtykke. Relevant for kontrol af medarbejderes brug af e-post og internet er, at behandling af personoplysninger kan foretages uden samtykke, hvis behandlingen er nødvendig for, at organisationen kan forfølge en berettiget interesse, og hensynet til medarbejderen ikke overstiger denne interesse; eller lidt forenklet udtrykt: Hvis det vil være til større ulempe for organisationen, at behandlingen ikke kan foretages, end det vil være for medarbejderen, at behandlingen foretages.

Datatilsynet har i en udtalelse af 19. september 2000 om overvågning af medarbejders e-post og internetbrug tilkendegivet, at hensynet til systemets drift, sikkerhed, genetablering og dokumentation samt hensynet til kontrol af, at medarbejderes brug af e-post og internet følger de afstukne rammer, er berettigede interesser. En arbejdsgiver har derfor ret til uden medarbejderens samtykke at føre en log over besøgte hjemmesider og over afsendte og modtagne e-postmeddelelser samt sikkerhedskopiere e-postmeddelelser og gennemgå dem ved mistanke om misbrug, når dette sker for at varetage et eller flere af de nævnte hensyn, forudsat at følgende betingelser er opfyldt:

- Medarbejderne skal på forhånd på en klar og utvetydig måde være informeret om logning, sikkerhedskopieringen og den eventuelle gennemgang af de enkelte medarbejderes e-post.
- Ved en gennemgang af medarbejderens e-post må organisationen ikke læse den e-post, der kan identificeres som privat (med mindre der udtrykkeligt er givet samtykke fra medarbejderen).

Datatilsynet har i en afgørelse af 30. oktober 2001 i en sag, der vedrørte spørgsmålet om, hvorvidt persondataloven finder anvendelse på behandlinger, der vedrører oplysninger lagret i en browser og i et e-postsystem, udtalt at en arbejdsgivers kontrol af de ansattes brug af e-post og internet - som følge af princippet om god databehandlingsskik - normalt forudsætter, at de ansatte på forhånd på en klar og utvetydig måde er informeret om, at kontrol kan finde sted.

I den konkrete sag kunne Datatilsynet ikke tage stilling til, om virksomheden havde opfyldt denne informationspligt. Det blev udtalt, at afgørelsen heraf henhørte under domstolene, i hvilken forbindelse Datatilsynet noterede sig, at der allerede verserede retssag mellem parterne.

Datatilsynet fandt i den konkrete sag, at virksomhedens gennemgang af medarbejderens internet-browser og e-post var nødvendig, for at virksomheden kunne undersøge mistanken om den ansattes omfattende private brug af internetadgangen. Datatilsynet fandt ligeledes, at virksomhedens gennemgang af medarbejderens e-post var nødvendig, for at virksomheden kunne få adgang til de heri indeholdte arbejdsrelaterede informationer. Virksomheden havde således efter Datatilsynets opfattelse haft en berettiget interesse i at gennemgå klagerens browser og e-post, som oversteg hensynet til klageren. Datatilsynet fandt derfor, at virksomhedens gennemgang var i overensstemmelse med persondataloven.

Dernæst udtalte Datatilsynet, at oplysninger om hvilke hjemmesider en person har besøgt på internettet betragtes som almindelige ikke-følsomme oplysninger, og at det samme gælder i relation til oplysninger i et e-post-system. Det blev i den forbindelse bemærket, at det ikke af sagen fremgik, at klagerens e-post skulle have indeholdt følsomme oplysninger.

Endelig blev det udtalt, at en arbejdsgiver ikke må læse privat e-post, og at arbejdsgiveren, hvis denne bliver opmærksom på, at der er tale om privat e-post uden relation til virksomhedens drift, ikke må læse den pågældende e-post. Datatilsynet bemærkede, at bedømmelsen af om en arbejdsgivers eventuelle læsning af den ansattes private e-post er i strid med straffelovens

regler om brevhemmelighed med videre, ikke henhører under Datatilsynets kompetence, men under anklagemyndigheden og domstolene.

I henhold til Datatilsynets udtalelse skal offentlige myndigheder foretage anmeldelse til Datatilsynet, hvis logning, sikkerhedskopiering og læsning af e-post foretages for at føre kontrol med medarbejderne. Private virksomheder er ikke underlagt et tilsvarende anmeldelseskrav.

Der henvises til Datatilsynets hjemmeside www.datatilsynet.dk

Straffelovens § 263 - brevhemmelighed

Efter straffelovens § 263 er det strafbart at åbne eller i øvrigt gøre sig bekendt med indholdet af et brev eller en anden lukket meddelelse eller at skaffe sig adgang til en andens oplysninger, der er bestemt til at bruges i et anlæg til elektronisk databehandling. En overtrædelse kan give bøde, hæfte eller fængsel op til 6 måneder.

Bestemmelsen omfatter kun private e-postmeddelelser. E-postmeddelelser, der sendes til organisationen eller til en medarbejder i sin egenskab af repræsentant for organisationen, er ikke omfattet.

Bestemmelsen ulovliggør læsning af medarbejderes private e-post forudsat, at den kan identificeres som privat. Med læsning må formentlig sidestilles anvendelse af firewalls eller lignende filtre, der kan scanne og læse indholdet af en e-postmeddelelse. Hvis et softwarefilter omvendt kun filtrerer bestemte filtyper uden at scanne og læse selve informationsindholdet, er bestemmelsen derimod næppe overtrådt. Det må antages at være lovligt efter bestemmelsen for organisationen at føre log over afsendelse og modtagelse af medarbejdernes e-post.

Forbudet mod læsning af medarbejdernes private e-post kan være vanskeligt at efterleve, da organisationen ofte først ved læsningen vil få kendskab til, at der er tale om en privat e-postmeddelelse. Da en overtrædelse af § 263 kræver forsæt, vil læsning af en privat e-postmeddelelse kun være

strafbar, hvis organisationen har viden om, at e-postmeddelelsen har et privat indhold, på det tidspunkt, hvor e-postmeddelelsen læses. Opdages det under læsningen, at indholdet er privat, må vedkommende stoppe læsningen.

Det er ikke afklaret, men må antages, at logning af de hjemmesider, en medarbejder besøger, er omfattet af § 263.

§ 263 hindrer ikke, at parterne aftaler, at organisationen må læse medarbejderens private e-post. Giver medarbejderen sit udtrykkelige samtykke til, at organisationen må foretage logning af hjemmesidebesøg og læsning af privat e-post, vil disse foranstaltninger være lovlige. Det er ikke afklaret, om det er tilstrækkeligt, at organisationen blot informerer medarbejderen om kontrolforanstaltningerne. Det vil næppe være i strid med § 263, at organisationen foretager logning af hjemmesidebesøg uden forudgående samtykke fra medarbejderen, når blot denne er informeret. Tilsvarende gælder muligvis efter omstændighederne for læsning af privat e-post, men for at undgå nogen tvivl, bør organisationen indhente medarbejderens samtykke til læsning af privat e-post, hvis organisationen vurderer, at der kan opstå et sagligt begrundet behov herfor.

Arbejdsretlige regler

Det følger af § 5 i bekendtgørelse om arbejde ved skærmterminaler (bkg. nr. 1108 af 15. december 1992), der henviser til et tilhørende bilag, at der ikke må anvendes kvantitativ eller kvalitativ kontrol af medarbejders arbejde ved skærmarbejdspladser uden medarbejderens viden.

Dernæst følger det af arbejdsretlige grundsætninger, at en organisation har ret til at indføre kontrolforanstaltninger, hvortil hører kontrol af medarbejders e-post og internetbrug, såfremt kontrolforanstaltningerne hverken er krænkende eller diskriminerende, ikke påfører medarbejderen tab eller andre nævneværdige ulemper og i øvrigt er begrundet i organisationens driftsmæssige forhold. Sagligt begrundede regler om kontrol af medarbejders e-post og internetbrug, vil overholde disse betingelser.

Ved en aftale mellem DA og LO af 24. april 2001, der fungerer som et tillæg til Hovedaftalen, er det fastsat, at organisationen skal underrette lønmodtageren om nye kontrolforanstaltninger senest 2 uger inden de iværksættes. Aftalen gælder kun organiserede virksomheder, og virksomheder der har indgået tilsvarende lokalaftaler.

Herudover kan de overenskomster, som arbejdsgiveren er forpligtet af, indeholde regler om kontrol. Ved fastlæggelsen af regler om kontrol af e-post og internet må organisationen sikre, at eventuelle bestemmelser i relevante overenskomster overholdes.

Sammenfatning

Regelgennemgangen viser, at det generelt er lovligt at kontrollere medarbejdernes brug af e-post og internet, forudsat at

- Kontrollen har et sagligt formål, og organisationen en berettiget interesse i kontrolforanstaltningen.
- Medarbejderne forud er informeret herom.

Der bør indhentes samtykke fra medarbejderne til læsning af privat e-post, hvis organisationen finder behov herfor under nærmere angivne omstændigheder.

Organisationens e-post- og internetpolitik bør indeholde en *beskrivelse af det nærmere omfang af de anvendte kontrolforanstaltninger*. Regelsættet bør endvidere udformes således, at det også sikrer medarbejderne grundig information om kontrollens karakter, både med henblik på at synliggøre og dermed afmystificere kontrollen og med henblik på at sikre overholdelse af reglerne i lov om behandling af personoplysninger. I afsnit 3.6 er givet en beskrivelse af, hvilke informationer e-post- og internetpolitikken bør indeholde.

Det er vigtigt at understrege, at *kontrol ikke er et alternativ til god ledelse*. Hvis organisationen er belastet af, at der bruges for meget arbejdstid på privat surfing på internettet, vil det reelle problem sjældent være teknologien men en manglende motivation til at udføre det egentlige arbejde. Det er andre ledelsesværktøjer end kontrol, der skal opfange og imødegå sådan demotivation.

Hvis organisationen ønsker at kunne gennemføre kontrol af medarbejderens e-post og internetbrug, kræves et sagligt formål med foranstaltningerne og en berettiget interesse.

Medarbejderne skal informeres på forhånd om organisationens kontrol med deres brug af e-post og internet.

Det må anbefales at indhente medarbejdernes samtykke, hvis organisationen under nærmere angivne omstændigheder finder det nødvendigt at kunne få adgang til lovligt at læse privat e-post.

Kontrol erstatter ikke god ledelse.

2.3 Skal aftaler på vegne af organisationen kunne indgås ved brug af e-post?

E-postens *fordele* gør sig ikke kun gældende ved uformel kommunikation. Også forpligtende tilbud om køb og større aftaledokumenter kan hurtigt og enkelt fremsendes til samhandelspartnere. Det kan endvidere være muligt at købe til en lavere pris, når der handles elektronisk, både fordi køberen har en mere effektiv mulighed for at sammenligne priser, hvilket skærper konkurrencen, og fordi den elektroniske aftaleindgåelse kan være omkostningsbesparende for sælgeren.

Aftaleindgåelse via e-post og navnlig internettet rummer imidlertid også visse *risici*. Det digitale mediums hurtighed kan gøre det nærliggende at anvende mere uformelle aftaleindgåelsesprocedurer, end dem som

organisationen ellers benytter og ønsker benyttet. Man kan lettere komme til at sende et tilbud uden først at have fået godkendelse fra en overordnet. Mediets hurtighed kan også bevirke, at der er en større risiko for, at man får afgivet et tilbud, der ikke var tilsigtet eller ikke var tilstrækkeligt overvejet. Forbrugeraftaleloven yder forbrugere en vis beskyttelse mod denne type risici i form af en 14-dages fortrydelsesfrist. Lovgivningen giver ikke erhvervsdrivende og offentlige myndigheder en tilsvarende beskyttelse. Endelig er der risiko for, at den, man kommunikerer med, udgiver sig for at være en anden. Denne risiko er navnlig aktuell ved kommunikation via e-post (medarbejderen modtager e-post, der er udfærdiget af en anden end den angivne afsender) men består også ved medarbejderens kommunikation med en hjemmeside. Der er eksempler på, at hackere har kopieret en banks hjemmeside og placeret den under en www-adresse, der er forvekslelig med bankens www-adresse.

En række af disse risici kan imødegås ved brug af *digital signatur*.

I sin *afvejning* af fordele og ulemper kan organisationen vælge at sondre mellem forskellige aftaletyper og forskellige sikkerhedsniveauer. Det vil sjældent være forbundet med større risici at indgå mindre vigtige aftaler via e-post uden særlige sikkerhedsforanstaltninger, hvorimod organisationen bør overveje, hvorvidt større aftaler med videregående forpligtelser bør indgås elektronisk, uden at særlige sikkerhedssystemer, såsom digitale signaturer, anvendes.

Det kan ofte med fordel klart *angives i organisationens e-post- og internetpolitik*, om aftaler kan indgås via e-post og internet eventuelt med en nærmere specifikation af, hvilke typer aftaler, der kan indgås og hvilke procedurer, der skal følges. Når en organisation anvender digitale signaturer, bør den udarbejde en digital signaturinstruks, der supplerer e-post- og internetpolitikken. Der henvises herom til IT-Sikkerhedsrådets vejledning om **Praktisk brug af kryptering og digital signatur** (2000).

Vurderingen af, om der skal kunne indgås aftaler via e-post og internet beror på en konkret afvejning af fordelene og de særlige risici, der gør sig gældende.

Ved risikoafvejningen kan der sondres mellem forskellige typer aftaler og forskellige sikkerhedsniveauer.

2.4 Implementering af særlige systemer til sikkerhed for e-postmeddelelsers ægthed, fortrolighed med videre

Ved fremsendelse af meddelelser, der indeholder *vigtig information*, herunder retlige forpligtelser, vil det ofte være afgørende for de kommunikerende parter at opnå en høj grad af sikkerhed for, at meddelelsen stammer fra den angivne afsender (sikkerhed for meddelelsens autenticitet), at meddelelsen ikke er blevet ændret under forsendelsen (sikkerhed for integritet), at det efterfølgende kan bevises, at meddelelsen hidrører fra afsenderen (sikkerhed for uafviselighed), at tredjemand ikke kan tilegne sig informationen (sikkerhed for fortrolighed) samt eventuelt sikkerhed for, hvornår meddelelsen er afsendt henholdsvis modtaget (sikkerhed for modtagelses- og afsendelsestidspunkt).

Der eksisterer en række *løsninger*, der har til formål at skabe sikkerhed for disse forskellige aspekter i digitale kommunikationssystemer som for eksempel e-postsystemer. Digitale signaturer kan skabe en høj grad af sikkerhed for et dokumentets autenticitet, integritet og uafviselighed. Kryptering kan skabe sikkerhed for dokumentets fortrolighed. Uafhængige tidsstemplingstjenester kan skabe sikkerhed for afsendelses- og modtagelsestidspunkt.

Behovet for at implementere disse forskellige sikkerhedsløsninger afhænger af karakteren af de meddelelser, organisationen vil udveksle i sit digitale kommunikationssystem.

Digitale signaturer bør anvendes i situationer, hvor der foretages væsentlige dispositioner i tillid til e-postafsenderens identitet, hvis ikke identiteten sikres på anden måde, for eksempel ved efterfølgende papirkorrespondance.

Kryptering bør anvendes, hvis e-post anvendes til udveksling af følsomme oplysninger, som i forkerte hænder kan påføre organisationen eller tredjemand gener. Sådanne oplysninger kan for eksempel være forretningshemmeligheder eller personoplysninger.

Det følger af persondatalovens § 41 stk. 3, at den der behandler personoplysninger skal træffe de nødvendige tekniske sikkerhedsforanstaltninger mod at personoplysninger kommer til uvedkommendes kendskab. For offentlige myndigheder er kravene hertil specificeret i bkg. nr. 528 af 15. juni 2000. Kravene er ikke nærmere specificeret for private virksomheder, men det må som udgangspunkt antages, at kravene til behandlingssikkerheden finder tilsvarende anvendelse. Datatilsynet har udsendt en publikation, der beskriver, hvornår Datatilsynet anser kravene efter sikkerhedsbekendtgørelsen for opfyldt (publikation nr. 37 af 2. april 2001). Det følger af publikationen, at e-postmeddelelser, der indeholder fortrolige personoplysninger, såsom personnumre eller oplysninger om økonomiske forhold, skal krypteres, når de sendes via internettet eller andre åbne net. Indeholder e-postmeddelelsen følsomme personoplysninger, skal der anvendes stærk kryptering baseret på anerkendte algoritmer. Med følsomme personoplysninger forstås oplysninger om etnisk baggrund, politisk, religiøs eller filosofisk overbevisning, fagforeningsmæssige tilhørsforhold, helbredsmæssige og seksuelle forhold, samt oplysninger om strafbare forhold, væsentlige sociale problemer eller andre rent private forhold. Datatilsynet har tilkendegivet, at disse krav ikke kun skal efterleves af offentlige myndigheder men også af private virksomheder med de nødvendige tilpasninger.

IT-Sikkerhedsrådets vejledning om **Praktisk brug af kryptering og digital signatur** (2000) og IT-Sikkerhedsrådets introduktion og vejledning om **Digital dokumenters bevisværdi** (1998) giver råd om, hvornår og hvordan de her nævnte type sikkerhedsløsninger, særligt digital signatur og kryptering, bør implementeres.

Vejledningen om **Praktisk brug af kryptering og digital signatur** (2000) inddeler *meddelelser i tre forskellige niveauer, afhængigt af behovet for at opnå sikkerhed for meddelelsens autenticitet og fortrolighed*. I relation til spørgsmålet om sikkerhed for meddelelsens autenticitet sondres mellem 1) kritiske meddelelser (meddelelser der indebærer retsvirkninger eller har økonomiske konsekvenser), 2) andre meddelelser, hvor meddelelsesautenticitet må anses for ønskelig (for eksempel sikring af at medarbejdere i den offentlige forvaltning ikke udleverer personoplysninger til uvedkommende personer) og 3) ukritiske meddelelser. I relation til spørgsmålet om sikkerhed for meddelelsens fortrolighed sondres mellem 1) fortrolige meddelelser (for eksempel særligt følsomme personoplysninger), 2) andre meddelelser, som ønskes holdt fortrolige (for eksempel andre personoplysninger) og 3) meddelelser, som ikke kræver fortrolighed. Ved organisationens overvejelser om implementering af særlige sikkerhedsløsninger, kan der tages udgangspunkt i denne niveauopdeling.

Vælger organisationen *ikke at implementere særlige sikkerhedsløsninger*, vil organisationen i stedet i sin e-post- og internetpolitik kunne begrænse de typer information, der må sendes via e-post, i overensstemmelse hermed.

Behovet for at sende vigtig information med e-post skal sammenholdes med organisationens sikkerhedsløsninger.

2.5 I hvilket omfang skal medarbejderne inddrages i fast læggelsen af retningslinjerne?

Er organisationens e-post- og internetpolitik baseret på retningslinjer, som medarbejderne finder urimelige og uforståelige, er der en væsentlig risiko for, at medarbejderne ikke fuldt ud vil følge retningslinjerne i deres daglige arbejde. Dette kan til en vis grad imødegås ved kontrolforanstaltninger og sanktioner men *fuldt udbytte af en e-post- og internetpolitik må antages at kræve en grundlæggende accept i organisationen*.

Inden e-post- og internetpolitikken udarbejdes, kan organisationen eventuelt forsøge at *identificere den eksisterende uformelle e-post og internetkultur*. I hvilket omfang anvendes e-post og internet privat? Hvilke former for vittigheder sendes rundt? Er der nogle i organisationen, som stødes af indholdet? Anvendes en anden sprog tone ved udfærdigelse af ekstern e-post end ved udfærdigelse af breve? Undersøgelsen kan foretages på forskellige måder for eksempel (med en stigende grad af åbenhed) ved kontrol, anonyme spørgeskemaundersøgelser, interviewundersøgelser og fællesmøder.

Generelt vil det gælde, at *jo større forskel der er på den eksisterende kultur og de retningslinjer, som skal gælde efter e-post- og internetpolitikken, jo vigtigere vil det være at informere medarbejderne om politikken og ikke mindst om formålet med de angivne retningslinjer*.

Det mere præcise omfang af medarbejderinddragelse beror på kulturen i den enkelte organisation. Det er *ledelsens ret at fastlægge indholdet af e-post- og internetpolitikken*. Ledelsen vil som udgangspunkt ikke have nogen pligt til at forhandle med medarbejderne, medmindre der er tale om overenskomstdækkede organisationer eller organisationer, hvor der er indgået lokalaftaler med samme indhold som samarbejdsaftalen mellem LO og DA. Det vil dog generelt være en god ide at inddrage medarbejderne for at forankre politikken bredt i organisationen. Som beskrevet i afsnit 4 gælder derimod en pligt til at informere medarbejderen om retningslinjerne, inden de træder i kraft.

Forud for udarbejdelsen af retningslinjerne kan den eksisterende uformelle e-post- og internetkultur eventuelt identificeres.

Store forskelle i den uformelle kultur og de udarbejdede retningslinjer vil øge informationsbehovet.

3. INDHOLDET AF EN E-POST- OG INTERNETPOLITIK

En central del af en e-postpolitik består i en beskrivelse af, hvordan medarbejderen skal håndtere e-post i forskellige arbejdssituationer. Disse spørgsmål er behandlet i afsnit 3.1-3.3.

I afsnit 3.4-3.8 er behandlet nogle mere generelle spørgsmål om begrænsninger i privat brug, kontrol og sanktioner, som har relevans for brug af både e-post og internet.

3.1 Procedurer ved afsendelse af e-post

A. Hvornår er e-post anvendelig?

E-postens fordele som kommunikationsmiddel sammenlignet med kommunikation via papir og telefon er åbenbare. Netop den omstændighed at fordelene er så markante, formentlig sammenholdt med en generel fascination af den nye teknologi, har bevirket, at e-post hyppigt anvendes i situationer, hvor andre kommunikationsmidler er mere velegnede og derfor med fordel kan anvendes.

I de fleste situationer vil e-post være et praktisk og effektivt kommunikationsmiddel og dermed anvendeligt. En e-postpolitik kan derfor med fordel skitsere de *situationer, hvor e-post ikke skal anvendes*.

Den omstændighed, at en person er udstyret med en e-postadresse er ikke nødvendigvis ensbetydende med, at den pågældende ønsker at kommunikere på denne måde eller i øvrigt er fortrolig med teknikken. En e-postpolitik kan derfor fastslå, at e-post som udgangspunkt ikke skal anvendes, hvis modtageren *ikke har tilkendegivet*, at vedkommende ønsker at kommunikere via e-post. Dette gælder navnlig fremsendelse af e-post til private e-postadresser, hvor der ikke er nogen sikkerhed for, at modtageren regelmæssigt kontrollerer, om der er kommet nye e-postmeddelelser men kan også gælde i andre tilfælde. Med tiden må det forventes, at brugen af e-post

bliver så udbredt, at e-post som udgangspunkt kan anvendes som indledende kommunikationsmiddel.

Når en *ubehagelig meddelelse* skal overbringes, for eksempel en meddelelse til en medarbejder om opsigelse, vil hverken brev eller telefon og derfor heller ikke e-post være egnet. Det kan måske være fristende at bruge denne kommunikationsform, herunder e-post, for at undgå at skulle stå ansigt til ansigt med modtageren af meddelelsen, men brug af e-post i sådanne situationer vil give modtageren et indtryk af distance og manglende medfølelse og troværdighed hos afsenderen. De signaler der kan sendes med sprogets betoning, kropssprog og ansigtsudtryk, går tabt ved kommunikation via e-post og breve.

Meddelelser, der er båret af store følelser, navnlig *vrede*, bør ikke kommunikeres i e-post, heller ikke internt i organisationen. E-postens hurtighed medfører i disse situationer en oplagt risiko for, at afsenderen får nævnt ting, som efterfølgende fortrydes. Endvidere kan der være en risiko for, at budskabet opfattes alvorligere, end det reelt er ment.

I mange tilfælde vil *information hurtigere kunne udveksles via telefon* end via e-post. Dette gælder navnlig, hvis afsenderen skal skrive meget tekst i e-postmeddelelsen. Herudover er det sjældent hensigtsmæssigt, hvis e-postkommunikation får karakter af et samtaleforløb med afsendelse af en stor mængde e-postmeddelelser umiddelbart efter hinanden. I begge disse situationer, vil der ofte kunne spares tid ved at bruge telefonen.

Skal e-post sendes til en meget *stor kreds af personer, internt* i en organisation, bør det overvejes, om informationen med fordel kan kommunikeres ud på anden vis. Modtagelse af e-post vil ofte medføre et afbræk i det arbejde, medarbejderen er i gang med, med en spildtid til følge, der ligger udover den tid, det tager at læse meddelelsen. Hvis hver medarbejder på denne måde påføres to minutters spildtid om dagen, svarer det i en organisation med 500 medarbejdere til 16,5 time pr. dage. Massemeddelelser kan i stedet opslås i kantinen alle andre steder, hvor det forventes, at alle medarbejdere ser dem.

En anden mulighed er at oprette en elektronisk opslagstavle, hvor massemeddelelser lægges ind. Anvendes e-post kan massemeddelelser med fordel sendes udenfor normal arbejdstid, således at de ikke skaber unødvendige afbræk i arbejdsdagen. Organisationen kan overveje at blokere for muligheden for at sende en e-postmeddelelse til alle i organisationen, eventuelt således, at sådanne meddelelser sendes til en central kommunikationsansvarlig, der vurderer, hvordan den pågældende information bedst kommunikeres ud.

Information, som det er vigtigt, at modtageren får kendskab til inden et givent tidspunkt, bør ikke sendes via e-post, hvis ikke afsenderen er sikker på, at modtageren læser e-postmeddelelsen inden det pågældende tidspunkt. Herved kan undgås, at personer møder op til møder, der er blevet aflyst via en e-postmeddelelse, som de pågældende ikke har læst, eller at svarfrister overskrides og lignende.

Det kan være forbundet med stor risiko, at sende *fortrolig information* via e-post, medmindre der anvendes kryptering. Ved tvivl om, hvorvidt informationen har en sådan karakter af fortrolighed, at den ikke bør sendes via e-post, må det vurderes, hvad konsekvensen i værste fald vil være, hvis informationen kom i forkerte hænder. Hvis denne konsekvens er problematisk for organisationen, modtageren eller andre, som organisationen er forpligtet overfor, er informationen ikke egnet til at blive sendt med e-post. Som nævnt i afsnit 2.4 gælder særlige regler for afsendelse af visse personoplysninger via e-post.

E-postpolitikken kan indeholde en beskrivelse af de situationer, hvor e-post ikke er velegnet og derfor ikke bør anvendes som kommunikationsform.

B. Hvem skal e-post sendes til?

En e-postmeddelelse kan uden problemer og omkostninger sendes til et stort antal modtagere. Dette fører ofte til, at e-post sendes til en række modtagere, for hvem indholdet ikke er relevant, og som derfor bruger

unødigt tid på at læse indholdet. Det store antal af e-postmeddelelser, der sendes, kan nemt føre til, at det samlede tidsspild ved modtagelse af irrelevant e-post bliver markant for organisationen. Hertil kommer, at rundsendelse af irrelevant e-post er en unødvendig belastning af e-post-systemet.

Det kan derfor indgå i organisationens e-postpolitik, at *e-post kun sendes* til relevante personer og ikke til en række yderligere personer „for en god ordens skyld“. Medarbejderne kan for eksempel opfordres til at overveje, om de ville have informeret alle de påtænkte modtagere telefonisk og hvis ikke, om de pågældende da behøver informationen via e-post.

Ved *besvarelse af en e-postmeddelelse* vil det generelt være god tone at besvare alle hovedmodtagere af den oprindelige e-postmeddelelse, medmindre denne lægger op til, at der kun svares til afsenderen. Generelt vil gælde, at jo flere meddelelsen er sendt til, jo mere nærliggende vil det være kun at besvare afsenderen, der så selv kan vurdere om videre-sendelse skal ske. Om besvarelsen bør sendes til personer, der er anført i cc-modtagerfeltet, vil bero på den enkelte situation.

Anvendes e-post til *kommunikation mellem en meget stor gruppe*, vil det ofte være u hensigtsmæssigt, at alle deltagere anvender „svar alle“-funktionen. Specielt hvis der er tale om mødeindkaldelse, vil det typisk være mest hensigtsmæssigt kun at svare tilbage til afsenderen, der på basis af alle indløbne svar herefter kan fastlægge den endelige dato. Hvis en større del af en meget stor gruppe alle sender deres svar på den oprindelige e-post-meddelelse til alle gruppens deltagere, vil det være en voldsom belastning af e-postsystemets kapacitet, der kan bevirke, at systemet blokeres eller lægges ned i længere tid. Kan der ikke findes bedre alternativer til masse-kommunikationen end e-post, kan der eksempelvis fastlægges en procedure, der sikrer, at svar kun sendes til den oprindelige afsender, der herefter kan klippe alle svar sammen i en enkelt e-postmeddelelse, der udsendes til alle. Som nævnt kan organisationen også overveje at udpege en kommunikations-ansvarlig, som e-postmeddelelser til et meget stort antal interne modtagere skal sendes til med henblik på en vurdering af, om den pågældende information bedre kan kommunikeres ud på anden vis.

Der flourer et stort antal *falske virusadvarsler* („hoaxes“), der ofte videregives i de bedste hensigter. Disse advarsler er som regel i sig selv uskadelige, men rundsending heraf i organisationen kan være både tidskrævende og belaste systemets kapacitet. Virusadvarsler skal kun sendes til organisationens IT-ansvarlige, der vurderer, hvilke reaktioner advarslen giver anledning til.

For at undgå tidsspild og unødigt belastning af e-postsystemets kapacitet kan e-postpolitikken fastslå, at e-post kun må sendes til relevante modtagere.

Der kan fastsættes særlige procedurer for at undgå unødvendige „send til alle“-meddelelser.

C. Sprog, tone og indhold

E-post lægger op til en mere uformel omgangstone end breve og anden skriftlig kommunikation. Det kan overvejes, om en sådan uformel omgangstone vil være i strid med de krav og forventninger, som organisationen har til den eksterne kommunikation. Ved disse overvejelser må det erindres, at udbredt brug af en mere uformel omgangstone ved udfærdigelse af en e-postmeddelelse afspejles af en tilsvarende udbredt accept af, at modtagne e-postmeddelelser er holdt i en mere uformel tone end breve. Hvis en uformel omgangstone er i strid med organisationens kommunikationspolitik, kan e-postpolitikken indeholde retningslinjer for, hvilken omgangstone der skal anvendes ved e-post. Det nærmere omfang af sådanne retningslinjer beror helt på kulturen i den enkelte organisation, men det er under alle omstændigheder væsentligt, at de forventninger, organisationen har på dette område, synliggøres i e-postpolitikken.

Retningslinjerne kan tage udgangspunkt i de krav, der stilles til udformning af almindelige breve, og eventuelt fastslå, at omgangstone i e-postmeddelelser skal svare til omgangstone i almindelige breve. Dette krav må normalt altid stilles til offentlige myndigheders korrespondance med borgerne.

Organisationen må endvidere forholde sig til, om der skal ske præcisering af kravene til retskrivning, grammatik, opstilling med videre. Anvendelse af udtryk som „hej“, „kære“ og lignende kan der også tages stilling til i politikken. Det bør angives, hvordan e-postmeddelelser skal underskrives, herunder om der skal anvendes autosignatur, om der skal underskrives i en andens navn (fuldmagtsregler), anvendes fuldt navn, eller om man i visse situationer kan nøjes med fornavn, om forkortelser som „mvh“ kan anvendes.

Ved udarbejdelsen af retningslinjerne må det tages i betragtning, at der ofte skal besvares e-postmeddelelser, der er holdt i en uformel tone. At besvare en uformel e-postmeddelelse i et meget formelt sprog kan virke distancerende for modtageren af svaret og måske direkte uhøfligt. Det er med andre ord vigtigt, at retningslinjerne ikke blive for stive, men at der overlades den enkelte medarbejder et konkret skøn afpasset efter stillingsindhold.

E-post lægger ikke kun op til en mere uformel omgangstone men også til udveksling af billeder, vittigheder, kommentarer og bemærkninger til oplevelser/begivenheder med videre af en karakter, som ikke ville blive rundsendt som almindelige post. Der er adskillige eksempler på, at denne type e-postmeddelelser kan virke *stødende* på nogle modtagere både internt i organisationen og eksternt. Konsekvenserne heraf kan være skadelig omtale af organisationen og splid internt i organisationen. En e-post-politik vil derfor med fordel kunne fastslå, hvorvidt e-postmeddelelser må indeholde vittigheder, billeder eller andet materiale, der har en karakter, der kan virke stødende på andre. Dette gælder ligeledes links til hjemmesider med et sådant indhold. Risikoen er særlig stor, når e-post udveksles over landegrænser, for eksempel mellem forskellige nationale afdelinger af samme organisation, på grund af de kulturelle forskelle, der ofte gør sig gældende. Risikoen øges endvidere, når meddelelsen sendes til et stort antal modtagere, som afsenderen *ikke* har *personligt* kendskab til. Det må derfor anbefales, at e-postmeddelelser indholdende vittigheder og lignende, hvis det overhovedet tillades, altid kun sendes til en afgrænset personkreds, som afsenderen har et konkret kendskab til.

Modtagelsen af et stort antal e-postmeddelelser i løbet af en arbejdsdag bevirker, at meddelelserne som regel læses hurtigt og ofte kun én gang. Dette øger risikoen for, at e-postmeddelelsen *ikke tilstrækkelig effektivt får formidlet den indeholdte information* til modtageren. Enkelte retningslinjer kan øge informationseffektiviteten af en e-postmeddelelse. Emnefeltet bør give præcis information om, hvad e-postmeddelelsen vedrører, så modtageren allerede er bekendt hermed, når vedkommende starter med at læse selve teksten. Længere tekster kan med fordel vedhæftes som en selvstændig tekstfil, der mere naturligt lægger op til udskrivning frem for læsning på skærmen. Ofte falder koncentrationen som læsningen skrider frem og den vigtigste information (eventuelt en konklusion) placeres derfor bedst i starten af e-postmeddelelsen. Information om aflysning et møde bør eksempelvis ikke placeres sidst i meddelelsen, hvis denne er af en vis længde.

E-postpolitikken kan indeholde retningslinjer for, hvornår e-post skal skrives i samme tone som almindelige breve.

En e-postpolitik vil som regel forholde sig til, hvilke typer information der ikke må rundsendes i organisationen og/eller eksternt.

D. Vedhæftning af filer

Vedhæftning af filer i e-post er en effektiv og hurtig måde at videreformidle større informationsmængder på. Filerne kan imidlertid både indeholde virus og have et omfang, der belaster e-postsystemets kapacitet voldsomt. Rundsendelse af billeder fra firmajulefrokosten kan lægge e-postsystemet ned. En e-postpolitik vil derfor med fordel kunne indeholde *retningslinjer for, hvilke filer, der må vedhæftes e-post*. Begrænsninger kan både vedrøre filformatet (for eksempel mp3-filer og exe-filer) og filstørrelsen. Sker der automatisk filtrering af bestemte filformater, vil det være hensigtsmæssigt, at retningslinjerne informerer herom.

Navnlig ved kommunikation via e-post internt i organisationen kan det overvejes, hvornår den i filen indeholdte information (for eksempel billederne fra firmajulefrokosten) med fordel skal kommunikeres ud på anden vis, for eksempel ved brug af elektroniske opslagstavler. Tilsvarende gælder medarbejdernes interne kommunikation i organisationen af mere privat karakter, for eksempel køb og salg af brugte barnevogne med mere, indkaldelse til sociale arrangementer og lignende.

E-postsystemet bør indstilles således, at vedhæftede filer ikke tilbage-sendes ved besvarelse af en e-postmeddelelse, da dette vil være en unødigt belastning af systemet, navnlig hvis e-post rundsendes mellem mange personer.

Sikkerhedsrisikoen ved brug af vedhæftede filer er beskrevet i IT-Sikkerhedsrådet vejledning **Sikkerhed ved e-post og internet** (2001).

Vurdér, om e-postpolitikken skal indeholde retningslinjer for, hvilke filer der ikke må vedhæftes e-post.

3.2 Procedurer ved modtagelse af e-post

A. Kvittering for modtagelse af e-post

Den *accepterede reaktionstid* på en e-postmeddelelse vil typisk være *kortere* end tilfældet er for almindelige breve, og afsenderen af en e-postmeddelelse vil ofte forvente et meget hurtigt svar fra modtageren. Det er imidlertid ikke altid, at modtageren er i stand til at levere et hurtigt svar, fordi en forespørgsel er rejst via e-post.

Oftest vil det imidlertid være tilstrækkeligt, at modtageren kvitterer for modtagelsen og informerer om tidsrammen for en nærmere besvarelse. Organisationens e-postpolitik kan indeholde faste retningslinjer for, *hvornår der senest skal være kvitteret for modtagelse* af en e-postmeddelelse.

Hvis organisationen har en *central e-postadresse* (organisation@organisation.dk eller underorganisation@organisation.dk), vil det være hensigtsmæssigt, at tidsfristen for kvittering også gælder for denne adresse. Det må i så fald anbefales, at e-postpolitikken klarlægger, hvem der har ansvaret for læsning og besvarelse eller intern videresendelse af e-post til den centrale e-postadresse. I tilfælde af videresendelse skal den ansvarlige sikre sig, at den medarbejder, der videresendes til, ikke er fraværende.

Skal der i e-postpolitikken fastsættes en tidsfrist inden for hvilken, modtagne e-postmeddelelser skal være besvaret?

Skal tidsfristen også gælde for e-post, der sendes til organisationen centrale e-postadresse?

B. Medarbejderens fravær

Fravær kan hindre medarbejderen i at besvare modtagne e-postmeddelelser indenfor den accepterede tidsramme. Endvidere kan en modtagen e-postmeddelelse i nogle tilfælde udløse retsvirkninger, uanset om medarbejderen ikke læser den. Er der eksempelvis knyttet en tidsfrist (for eksempel en acceptfrist, opsigelsesfrist eller klagefrist) til besvarelse af en e-postmeddelelse, vil fristen ofte begynde at løbe fra modtagelsen af e-postmeddelelsen. Det vil derfor være en fordel at lade e-postpolitikken indeholde *retningslinjer, der beskriver hvilke procedurer, der skal iagttages ved en medarbejders fravær.*

Besvarelse af e-postmeddelelser indenfor den fastlagte tidsramme kan sikres ved brug af den *auto-svarfunktion*, som de mest udbredte e-postprogrammer alle er udstyret med. Auto-svarmeddelelsen kan indeholde oplysninger om, hvornår medarbejderen er tilbage igen (alternativt at medarbejderen eksempelvis er sygemeldt på ubestemt tid), og hvilken person der kan kontaktes i perioden.

Auto-svarfunktionen sikrer ikke i sig selv mod, at en modtagen e-postmeddelelse udløser retsvirkninger. *E-postmeddelelser, der kræver reaktion for*

at undgå u hensigtsmæssige retsvirkninger, må læses og behandles af en tilstedeværende medarbejder. Dette kan enten gøres ved at indstille e-post-programmet til automatisk at videresende den fraværende medarbejders e-post til en anden medarbejder, eller ved at en anden medarbejder får adgang til den fraværende medarbejders e-post. Det sidste vil typisk kræve, at den fraværende medarbejders log-on adgangskode udleveres til den medarbejder, der skal læse e-posten. Denne fremgangsmåde kan indebære en sikkerhedsrisiko, hvis for eksempel den private nøgle til medarbejderens digitale signatur er lagret på computerens harddisk. Den fraværende medarbejder må under alle omstændigheder ændre adgangskode, når vedkommende kommer tilbage.

Da læsning og behandling af den fraværende medarbejders e-post både vil være tidskrævende og kunne virke kompromitterende for medarbejderen, hvis der fremsendes e-post med privat indhold i fravær-perioden, er denne løsning primært relevant, hvis organisationen vurderer, at brug af auto-svarfunktionen ikke i tilstrækkelig grad sikrer organisationens interesser. Ved denne vurdering må der lægges vægt på sandsynligheden for, at medarbejderen vil modtage e-post, der kræver hurtig reaktion for at undgå retstab, samt på længden af medarbejderens fravær. Der henvises til afsnit 3.3, 3.4 og 3.5 i IT-Sikkerhedsrådets vejledning om **Praktisk brug af kryptering og digital signatur** (2000).

Der kan imidlertid altid opstå situationer, hvor organisationen har brug for at få adgang til medarbejderens e-post, herunder for at undgå retstab og erstatningsansvar for tredjemand (for eksempel for at opfylde en aftale, fordi en e-postmeddelelse skal videresendes til en tredjepart, fordi afsenderen har mistet en vedhæftet fil og anmoder organisationen om at tilbagesende en kopi, eller fordi afsenderen (ved en fejl) har mærket e-postmeddelelsen „personlig“, „privat“ eller „fortrolig“). Det er ikke muligt for en organisation objektivt set at sikre sig, at al e-post, der er mærket „privat“ eller „fortrolig“, ikke vedrører organisationen. Dette gælder i særlig grad indgående e-post. *Det bør derfor vurderes, om der er behov for i retningslinjerne at angive, at organisationen altid har ret til at skaffe sig adgang til medarbejderens e-post og gøre sig bekendt med indholdet i tilfælde af fravær.*

En e-postpolitik kan med fordel indeholde en beskrivelse af proceduren for behandling af e-post, der sendes til en fraværende medarbejder.

Vurdér, om der er behov for, at e-postpolitikken fastlægger retningslinjer for behandling af e-post til fraværende medarbejdere, og hvorvidt organisationen skal have ret til om nødvendigt at læse den modtagne e-post.

C. Åbning af modtagne filer

Som allerede nævnt er der en risiko for, at filer vedhæftet en e-post-meddelelse indeholder virus, der aktiveres ved åbning af filen. Virus kan have alvorlige konsekvenser for organisationen og i værste fald bevirke, at store mængder af vigtige data slettes og/eller kompromitteres.

En e-postpolitik kan derfor med fordel indeholde *retningslinjer for omgang med modtagne filer*. Hvis afsenderen er ukendt for medarbejderen, og overskriften har en usædvanlig formulering eller et usædvanligt indhold, bør medarbejderen ikke åbne vedhæftede filer men i stedet kontakte organisationens IT-ansvarlige.

Nogle vira spredes ved, at en e-postmeddelelse indeholdende virus automatisk videregives til alle personer i modtagerens elektroniske adressekartotek. Selvom afsenderen er kendt for modtageren, kan e-postmeddelelsen derfor godt være en virusinficeret meddelelse sendt uden afsenderens viden. Hvis modtageren kender afsenderen af en mistænkelig e-postmeddelelse, bør han kontakte denne og høre, hvad meddelelsen indeholder og efter omstændighederne kontakte den IT-ansvarlige. Det må som udgangspunkt anbefales at indstille e-postprogrammet således, at der ikke sker automatisk åbning af modtagne e-postmeddelelser.

Sikkerhedsrisikoen ved brug af vedhæftede filer er beskrevet i IT-Sikkerhedsrådets vejledning **Sikkerhed ved e-post og internet** (2001).

En e-postpolitik bør indeholde retningslinjer for, hvornår vedhæftede filer ikke uden videre må åbnes.

D. Sikring af e-postmeddelelsens autenticitet

I langt de fleste situationer, vil en e-postmeddelelse stamme fra den angivne afsender, hvilket kan få modtageren til at antage, at dette altid vil være tilfældet. Teknisk set er det dog ganske nemt at producere en e-postmeddelelse med en falsk afsenderadresse, når der ikke gøres brug af digital signatur eller tilsvarende sikkerhedsforanstaltninger. Der er derfor en risiko for, at modtageren af den falske e-postmeddelelse indleder korrespondance med en ukendt tredjemand. Risikoen herved er navnlig, at modtageren (medarbejderen) får afgivet fortrolig information til tredjemanden.

Som beskrevet i afsnit 2.4 må organisationen overveje, om den elektroniske kommunikation skal understøttes af digitale signaturer eller lignende. Selvom dette vælges, kan medarbejderne imidlertid fortsat modtage e-postmeddelelser, der ikke er digitalt signeret. Det vil derfor være nyttigt under alle omstændigheder at fastsætte *retningslinjer for, hvornår medarbejderne skal sikre sig, at modtagne e-postmeddelelser er ægte.*

Retningslinjerne må afhænge af indholdet af korrespondancen. Hvis en besvarelse af den modtagne e-postmeddelelse bevirker, at der afgives personoplysninger eller andre fortrolige informationer, vil det være anbefalelsesværdigt at kontrollere meddelelsens ægthed. Dette gælder tilsvarende, hvis modtageren i tillid til meddelelsens ægthed foretager dispositioner, som kan påføre organisationen tab eller andre væsentlige ulemper, såfremt det efterfølgende viser sig, at e-postmeddelelsen er falsk. Det vil eksempelvis være forbundet med en vis risiko at effektuere en ordre afgivet via e-post, før e-postmeddelelsens ægthed er kontrolleret. Almindelige sagskorrespondance og mere uformel korrespondance, der ikke indeholder fortrolige oplysninger, vil normalt ikke kræve kontrol.

Hvis ikke den modtagne e-post er påført en digital signatur, må *autenticiteten sikres* ved at rette henvendelse til afsenderen og eventuelt få en underskrevet papirbekræftelse.

IT-Sikkerhedsrådets vejledning om **Praktisk brug af kryptering og digital signatur** (2000) indeholder nærmere beskrivelser af, hvordan en meddelelses autenticitet kan sikres.

Vurdér, om der er behov for i e-postpolitikken at give retningslinjer for, i hvilke situationer det skal sikres, at modtagne e-postmeddelelser er ægte, og hvad der i givet fald skal gøres.

E-postpolitikken kan ved fastlæggelse af retningslinjerne baseres på en risikoafvejning, der tager udgangspunkt i karakteren af den information, der indeholdes i e-postkommunikationen.

3.3 Journalisering, arkivering og sletning af e-post

E-post skal *journaliseres og arkiveres* i samme omfang som papirdokumenter. Der må i e-postpolitikken tages stilling til, om journalisering og arkivering skal ske efter de samme regler som gælder for papirdokumenter.

Er organisationens journalisering og arkivering baseret på papirdokumenter, vil udgangspunktet typisk være, at alle e-postmeddelelser og vedhæftede filer skal udskrives og lægges på sagen. Har organisationen digitaliseret sin sagsgang, og anvender organisationen som følge heraf elektroniske journaler og arkiver, kan der udarbejdes særlige retningslinjer for den elektroniske journalisering og arkivering. Der henvises for offentlige myndigheder til cirkulære nr. 5 af 6. november 2000 om offentlige myndigheders arkivering.

Hvis e-post udskrives på papir og journaliseres og arkiveres som papirdokumenter, kan e-postmeddelelsen normalt *slettes* efter udskrivning, hvis

medarbejderen skønner, at der ikke er behov for yderligere behandling (besvarelse eller videresendelse) af e-postmeddelelsen.

Anvender organisationen elektroniske journaler og arkiver, kan sletning af overflødige eksemplarer af e-postmeddelelsen normalt først ske, når medarbejderen har kontrolleret, at e-postmeddelelsen er lagret i overensstemmelse med retningslinjerne. Skal der eksempelvis ske elektronisk journalisering på en central enhed, må medarbejderen først slette eksemplaret i sit eget e-postsystem, når han har kontrolleret, at meddelelsen er lagret på den centrale journaliseringsenhed. Tilsvarende kontrol skal udføres ved overflytning fra journal til arkiv.

Det følger af persondataloven, at e-post, der indeholder personoplysninger, skal slettes, når de har opfyldt deres formål. Opbevaringstidens længde og sagligheden heraf vil i henhold til persondatalovens § 6, stk. 1, nr. 3, bero på indholdet af den pågældende e-post, herunder om det kan have saglige bevismæssige formål at opbevare e-post i en længere periode, for dermed at sikre muligheden for senere at føre bevis for, hvad der eksempelvis er sket i forbindelse med en sådan korrespondance. Der henvises endvidere til IT-Sikkerhedsrådets introduktion og vejledning med bilag om **Digitale dokumenters bevisværdi** (1998), side 113-129.

Det må anbefales, at der foretages en løbende sletning af e-post både af ordenshensyn og for at undgå unødigt belastning af e-postsystemet.

Reglerne om aktindsigt i offentlighedsloven og forvaltningsloven og reglerne om pligtaflevering til offentlige arkiver fastsætter særlige krav til *offentlige myndigheders* journalisering og arkivering. Folketingets Ombudsmand har i sin årsberetning for 1997 (s. 198 ff.), tilkendegivet, at reglerne i offentlighedsloven, forvaltningsloven og grundlæggende dokumentationskrav i forvaltningssager kræver, at en myndighed enten har en kopi af dokumenter, som myndigheden har udfærdiget, eller med sikkerhed med meget kort varsel fra et edb-anlæg vil kunne frembringe en fuldstændig nøjagtig udskrift (svarende til en kopi) af dokumentet. Ombudsmanden tilkendegav endvidere, at en myndigheds valg af elektronisk medium, i

stedet for papir, ikke berettiger en kassation af et dokument på et tidligere tidspunkt, end hvis det havde foreligget i papirform.

Offentlighedslovens § 6 (om notatpligt) fastslår blot, at mundtlige oplysninger af betydning for afgørelsen af en sag skal nedfældes i et notat. Det forekommer naturligt at antage, at notatpligten kan opfyldes elektronisk. I offentlighedslovens § 6, stk. 2, er angivet, at justitsministeren kan fastsætte nærmere regler om elektroniske dokumenter. Denne bemyndigelse er dog for tiden ikke udnyttet.

IT-Sikkerhedsrådet vejledning om **Digitale dokumenters bevisværdi** (1998) indeholder en beskrivelse af nogle centrale spørgsmål ved omlægning fra papirarkivering til digital arkivering, herunder særligt hvordan organisationen sikrer, at digitaliserede dokumenter har tilstrækkelig bevisværdi i en eventuel retssag.

Vurdér, om e-postpolitikken skal fastslå, at der skal ske journalisering og arkivering efter samme retningslinjer som gælder for papirdokumenter.

Har organisationen indført elektroniske journaler og arkiver, vil e-postpolitikken skulle afstemmes med de eksisterende procedurer for elektronisk journalisering og arkivering.

3.4 Aftaleindgåelse via e-post og internet

E-post- og internetpolitikken kan angive, om der må indgås aftaler på organisationens vegne via e-post og internet. Er dette tilfældet, kan retningslinjerne fastslå, at medarbejderen kan indgå aftaler elektronisk i samme omfang som medarbejderen i øvrigt kan indgå aftaler.

Retningslinjerne kan også fastlægge *særlige begrænsninger* i mulighederne for at indgå elektroniske aftaler, navnlig under hensyntagen til de risici,

som kan være forbundet med elektronisk aftaleindgåelse, jævnfør nærmere afsnit 2.3.

Begrænsningerne kan eksempelvis fastslå, at kun udvalgte medarbejdere må indgå aftaler elektronisk, at aftaler kun må indgås op til bestemte beløbsgrænser, at aftaler kun må indgås med parter, som organisationen har et jævnlige samhandelsforhold med, at aftaler kun må indgås via e-post men ikke via hjemmesider med videre.

I det omfang det er muligt, bør *eksterne parter informeres* om organisationens retningslinjer for elektronisk aftaleindgåelse.

Skal en e-post- og internetpolitik indeholde retningslinjer for, i hvilket omfang medarbejderne kan indgå aftaler elektronisk på vegne af organisationen?

3.5 Begrænsninger i den private brug

E-post- og internetpolitikken bør klart angive, hvorvidt der må gøres privat brug af e-post og internet. Er privat brug tilladt, må det anbefales, at det tilladte omfang nærmere præciseres.

Brugen kan for det første begrænses *kvantitativt*, således at privat brug er tilladt „i begrænset omfang“, „i rimeligt omfang“ eller lignende.

Det kan eventuelt angives, hvordan post, som har rent privat karakter, skal markeres, for eksempel ved i „emnefeltet“ at angive „privat“ som den første tekst, jævnfør dog bemærkningerne i afsnit 3.2 B, sidste afsnit.

Dernæst kan brugen begrænses i relation til *anvendelsesmåder*. For *e-post* vil det navnlig være relevant at knytte begrænsninger til indholdet af meddelelsen og anvendelse af vedhæftede filer. De retningslinjer, der

generelt gælder om forbud mod e-post med stødende indhold og håndtering af vedhæftede filer for arbejdsrelateret e-post, jævnfør ovenfor, vil normalt kunne finde tilsvarende anvendelse ved medarbejderens private brug af e-post.

Det er ikke et ukendt fænomen, at e-post kan bruges til at sprede ulovligt kopierede billeder, musikstykker og andet materiale, der er ophavsretligt beskyttet. I yderste konsekvens risikerer organisationen at blive pålagt et retligt ansvar for medarbejdernes ulovlige omgang med beskyttet musik med videre. Sådanne aktiviteter kan også komme i konflikt med organisationens etiske profil. Det vil derfor være en god idé klart at angive i e-post- og internetpolitikken, at der naturligvis ikke må ske nogen form for kopiering, videresendelse eller brug i øvrigt af piratkopieret materiale.

Privat brug kan forbydes i relation til bestemte typer af *hjemmesider*, for eksempel hjemmesider med pornografisk, racistisk eller andet indhold, der i forhold til organisationens værdisæt kan virke stødende, hjemmesider med ulovligt indhold, herunder ulovlige musikfiler samt hjemmesider, der kan udløse en betalingsforpligtelse med videre. Herudover kan det være forbudt at hente filer fra internettet, enten generelt eller i relation til bestemte filtyper. Yderligere kan begrænsninger relatere sig til bestemte former for tjenester, for eksempel homebanking, e-handel og deltagelse i chatrooms eller newsgroups.

Hvis medarbejderne er udstyret med *hjemmearbejdsplads*, bør det overvejes, om der skal gælde særlige regler for privat e-post herfra. Da e-post stadig afsendes via medarbejderens e-postadresse i organisationen, vil det være nærliggende at lade de samme regler gælde for brug af e-post fra en hjemmearbejdsplads som fra en kontorarbejdsplads. Dog gælder det selvsagt, at medarbejderens private brug af internet og e-post fra en hjemmearbejdsplads i fritiden ikke står i modsætning til en effektiv udnyttelse af arbejdstiden. Ofte vil det derfor være acceptabelt, at medarbejderen har ret til uindskrænket privat brug af e-post og internet fra hjemmearbejdspladsen, når dette sker i fritiden og under overholdelse af de øvrige begrænsninger, der gælder. Hvis organisationen betaler medarbejderens opkobling til organisationens centrale server, og betalingen opgøres efter

forbrug, kan organisationen dog af omkostningsgrunde vælge at begrænse den private brug af en hjemmearbejdsplads. Det kan fremgå af retningslinjerne, hvem der afholder udgifter til opkobling fra hjemmearbejdspladsen.

Der henvises endvidere til § 7, stk. 2, om sikkerhed ved hjemmearbejdspladser i Datatilsynets bekendtgørelse nr. 528 af 15. juni 2000 som ændret ved bekendtgørelse nr. 201 af 22. marts 2001 om sikkerhed til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning.

De nærmere grænser for medarbejderens private brug bør fremgå af e-post- og internetpolitikken.

Privat brug fra en hjemmearbejdsplads vil i de fleste henseender kunne sidestilles med privat brug fra en kontorarbejdsplads.

3.6 Kontrol af e-post og internetbrug

E-post- og internetpolitikken skal *informere medarbejderne* om formålet med og omfanget af en kontrol af medarbejdernes brug af e-post og internet. Formålet skal som tidligere nævnt i afsnit 2.2 være sagligt begrundet og skal ske for at varetage en berettiget interesse, der ikke overstiger medarbejderens berettigede interesse.

Formålet med kontrollen skal ikke mindst angives for at informere medarbejderne om, hvad formålet med kontrollen *ikke* er. Manglende information og klarhed i politikken er egnet til at skabe utryghed og rygtedannelser. Det er vigtigt, at medarbejderne klart og entydigt oplyses om formålet. Som nævnt anser Datatilsynet det for et legitimt formål at foretage kontrol med henblik på sikring af, at medarbejdernes brug af e-post og internet ligger inden for den af organisationen definerede ramme og/eller sker af drifts- eller sikkerhedsmæssige hensyn.

Normalt vil arbejdsgiveren ikke have nogen interesse i at læse medarbejderens *private e-post*. Alligevel kan det i mange situationer være vigtigt for arbejdsgiveren at kunne få adgang også til privat e-post, for eksempel i tilfælde af en medarbejders fravær eller ved mistanke om uregelmæssigheder, misbrug eller lignende. Har organisationen selv mulighed for at skaffe sig adgang til en e-postmeddelelse, som medarbejderen hævder er privat, risikerer organisationen at ifalde ansvar, hvis meddelelsen alligevel læses, og det viser sig, at den er af privat karakter. Organisationens kan undgå at skulle tage denne standpunktsrisiko, hvis den med sikkerhed er berettiget til at læse medarbejderens private e-postmeddelelser. Dette vil organisationen være, hvis den har indhentet medarbejderens samtykke til, at privat e-post må læses. Det kan i e-postpolitikken være angivet, at al e-post er organisationens ejendom, hvorved det understreges, at organisationen har fuld dispositionsret over alle e-postmeddelelser, også selvom de har privat karakter. Det kan også angives, at alle e-postmeddelelser anses for arbejdsrelateret kommunikation, og at der følgelig ikke eksisterer „privat“ e-post. Uanset hvilken løsning der vælges, er det vigtigt, at medarbejderen klart informeres om og giver sit samtykke til, at organisationen er berettiget til at læse al e-post, og dermed også e-post, der har et indhold af privat karakter.

Ved vurderingen af hvorvidt en organisation har behov for at kunne læse også medarbejdernes private e-post, bør det indgå, at der ikke findes objektive kriterier, der kan sikre, at e-post, der for eksempel er mærket „privat“ eller „fortrolig“, ikke er virksomhedsrelateret, blandt andet fordi det er afsenderen, der ud fra egne kriterier træffer valget om at anføre for eksempel „fortrolig“.

Det bør fremgå af e-post- og internetpolitikken, at formålet med at indhente samtykke ikke er kontrol for kontrollens skyld, men derimod at kunne gribe ind ved mistanke om, at afstukne retningslinjer ikke overholdes samt ud fra drifts- og sikkerhedsmæssige hensyn. Hvis det til formålet er tilstrækkeligt at anvende data om bestemte medarbejdere, som allerede er indsamlet af drifts- og sikkerhedsmæssige hensyn, som for eksempel en log og backup, bør sådanne data primært anvendes.

I forlængelse af formålet bør angives, *hvordan kontrollen foretages*, herunder om der sker logning samt sikkerhedskopiering og læsning af e-post. Det bør også for den ikke-teknikkyndige medarbejder klart fremstå, hvilke informationer kontrollen udstyrer organisationen med. Frem for at angive at al e-postkommunikation logges, kan det eksempelvis angives, at oplysninger om afsendelsestidspunkt, modtagelsestidspunkt, modtager og afsender gemmes i organisationens system, hvis det er det, der reelt sker.

Ofte vil det være muligt at *genskabe en slettet e-postmeddelelse*, og retningslinjerne kan derfor præcisere, at kontrolforanstaltningerne også indbefatter en ret til at genskabe slettede e-postmeddelelser.

Den del af kontrollen, der består i selve logningen og sikkerhedskopiering af e-postmeddelelser, vil typisk ikke være den, medarbejderen oplever som mest intens. Det vil derimod være den del af kontrollen, hvor andre personer i organisationen gør sig bekendt med den registrerede information, for eksempel undersøger hvilke hjemmesider medarbejderen har besøgt, hvem medarbejderen har sendt e-post til eller læser indholdet af en e-postmeddelelse.

Medarbejderen bør informeres om, *hvordan* organisationen gør sig bekendt med den registrerede information, herunder om der sker manuel og/eller automatisk stikprøvekontrol. Det vil sjældent være relevant at gennemlæse samtlige medarbejders e-postmeddelelser, og medarbejderne bør informeres om, at der *ikke sker systematisk daglig gennemgang* af den enkelte medarbejders e-post og internetbrug, men at der kan foretages systematisk gennemgang ved konkret mistanke om misbrug. Medarbejderen bør orienteres efter en sådan systematisk gennemgang er foretaget. Denne *oplysningspligt* følger af persondatalovens §§ 28 og 29.

Regelsættet bør endvidere indeholde information om, *hvem* der læser logfiler og e-postmeddelelser. De pågældende bør være underlagt tavshedspligt.

Medarbejderne bør informeres om *opbevaringstiden af logfiler og e-postmeddelelser*. Det følger af persondataloven, at informationerne ikke må opbevares længere end krævet for at opfylde deres formål.

Medarbejderne bør informeres om, at de har ret til *indsigt* i, hvilke konkrete informationer virksomheden har registreret om den enkelte medarbejders e-post og internetbrug. Denne ret følger af persondatalovens § 31.

Endelig kan det overvejes at fastsætte særlige *procedureregler*, herunder eventuelt om inddragelse af samarbejdsudvalg, tillidsrepræsentanter eller lignende.

En e-postpolitik bør informere om formålet med kontrolforanstaltninger og det nærmere indhold af kontrollen.

3.7 E-post i forbindelse med fratræden

Ved fratræden vil e-postpolitikken ofte give medarbejderen *mulighed* for at medtage privat e-post (og private filer, adressekartoteker med videre), enten ved kopiering eller videresendelse til en anden e-postadresse og efterfølgende slette e-postmeddelelserne.

Det kan overvejes at præcisere, at de almindelige regler og kontrolforanstaltninger også gælder i opsigelsesperioden, og at medtagelse/videresendelse af fortrolig information efter omstændighederne kan medføre erstatnings- og strafansvar. Baggrunden herfor er, at det fra visse sider hævdes, at risikoen for, at medarbejderne i opsigelsessituationen (måske i frustration) kan være særligt fristet til at misbruge besiddelsen af fortroligt materialet, er steget ved anvendelse af e-post, der hurtigt, diskret og ubesværet muliggør distribution af al slags information.

Det kan angives i e-postpolitikken, at organisationen beslutter, *hvornår medarbejderens e-postkonto skal lukkes*. Hvis lukning ikke sker samtidig med medarbejderens fratræden, kan auto-svarfunktionen bruges til at oplyse, at medarbejderen er fratrådt.

Det må anbefales, at det tydeligt angives, hvis al e-post til medarbejderen, *der modtages efter fratrædelsestidspunktet*, vil blive åbnet af organisationen.

Det kan overvejes, hvad der skal ske med privat e-post, der modtages efter fratrædelsestidspunktet. Organisationen kan vælge at slette al privat e-post eller i et rimeligt omfang at videresende private meddelelser til en e-postadresse opgivet af medarbejderen. Videresendelse af privat e-post kan blive tidskrævende, og organisationen må tage stilling til, om den vil påtage sig denne opgave.

De retningslinjer, der gælder for fratrædende medarbejdere, vil ofte også kunne anvendes i tilfælde af en medarbejders dødsfald.

E-postpolitikken vil ofte give en fratrædende medarbejder mulighed for at medtage og fjerne privat e-post med videre.

E-postpolitikken kan informere medarbejderen om, at al e-post, der sendes til medarbejderen efter fratrædelsestidspunktet, vil blive læst og privat e-post slettet.

3.8 Overtrædelse af e-post- og internetpolitikken

Der kan være en risiko for, at de sanktioner organisationen vælger at tage i anvendelse ved overtrædelse af retningslinjerne *opleves som urimelige af medarbejderne*, dels fordi mange af de spørgsmål, organisationen tager stilling til i sin e-post- og internetpolitik, beror på en vanskelig afbalancering af tungtvejende modsatrettede hensyn, dels fordi der for mange af spørgsmålene ikke eksisterer en fælles opfattelse af, hvad der er acceptabelt.

Mange af de problemer, der ellers kan opstå, hvis organisationen sanktionerer en medarbejders uhensigtsmæssige brug af e-post eller internettet, kan imidlertid afværges, hvis medarbejderne tydeligt er gjort opmærksomme på, hvilke regler der gælder for brug af e-post og internettet, og hvilke

sanktioner en manglende overholdelse af disse regler kan medføre. Det er derfor vigtigt, at medarbejderne meget *klart er informeret om, hvilke konsekvenser en manglende overholdelse af politikken kan få for medarbejderen.*

Indholdet af sanktionerne kan spænde fra advarsel over opsigelse til bortvisning og bør altid stå i et proportionalt forhold til medarbejderens handlinger.

Det vil være normalt at fastslå, at grove og gentagne overtrædelser fører til bortvisning af medarbejderen.

Der kan eventuelt yderligere knyttes konsekvenser direkte til politikkens centrale bestemmelser, eksempelvis således at en overtrædelse af et forbud mod at rundsende e-post med racistisk eller seksuelt indhold kan medføre bortvisning selv i enkeltstående grove tilfælde, mens videresendelse af organisationens fortrolige materiale altid medfører bortvisning.

Uanset om konsekvenserne alene beskrives generelt eller også i forhold til konkrete bestemmelser, vil det være en fordel, at alle e-post- og internetpolitikens regler om konsekvenser af overtrædelse anføres i et *samlet sanktionsafsnit*, så konsekvenserne fremstår klartest muligt for medarbejderen.

Det er domstolene, der i sidste ende afgør, om en konkret handling i relation til e-post og internet har berettiget en opsigelse eller bortvisning.

Sanktioner forbundet med overtrædelse af retningslinjerne skal fremgå tydeligt og samlet.

4. INFORMATION OM OG VEDTAGELSE AF EN E-POST- OG INTERNETPOLITIK

Det er ledelsens ret at fastlægge indholdet af politikken. Er organisationen underlagt reglerne om etablering af samarbejdsudvalg, skal politikken forelægges samarbejdsudvalget. Ved en aftale mellem DA og LO af 24. april 2001, der fungerer som et tillæg til Hovedaftalen, er det fastsat, at arbejdsgiveren skal underrette lønmodtageren om nye kontrolforanstaltninger senest 2 uger inden de iværksættes. Aftalen gælder kun organiserede organisationer, og organisationer der har indgået tilsvarende lokalaftaler.

De nævnte regler pålægger alene organisationen en *informationspligt*, og der gælder således generelt ikke noget krav om, at medarbejderne skal tiltræde politikken. Det vil bero på kulturen i den enkelte organisationen, i hvilket omfang det skønnes hensigtsmæssigt at inddrage medarbejderne i udformningen af reglerne, jævnfør nærmere afsnit 2.5. Åbenhed må under alle omstændigheder anses for et nøgleord, hvis indførelsen af en e-post- og internetpolitik skal blive en succes.

Mens der ikke gælder et generelt krav om, at medarbejderne tiltræder den fastlagte politik, er det uafklaret, hvorvidt straffelovens regler om brevhemmelighed kræver hver enkelt medarbejders *samtykke til, at den pågældendes private e-post må læses af organisationen*.

Det må derfor anbefales, at organisationen sikrer sig medarbejderens dokumenterede samtykke, for eksempel ved at medarbejderen underskriver en erklæring om at være bekendt med organisationens e-post- og internetpolitik og at være indforstået med at følge denne, og med underskriften giver sit samtykke til, at organisationen, såfremt organisationen finder det nødvendigt, kan få adgang til at læse medarbejderens e-post, herunder privat e-post, uanset om e-posten angives at være „privat“, „fortrolig“ eller på anden måde angives at have et privat indhold. Som nævnt kan e-postpolitikken anføre, at al e-post er organisationens ejendom, forstået på den måde at alle ind- og udgående e-postmeddelelser anses for arbejdsrelateret kommunikation.

Uanset at eksisterende medarbejdere gøres bekendt med politikken ved dens ikrafttræden og nye medarbejdere ved deres ansættelse, er dette ikke i sig selv tilstrækkeligt til at sikre, at politikken får den betydning for medarbejdernes daglige omgang med e-post og internettet, som er det primære sigte med en sådan politik. Den fulde effekt kræver, at *e-post- og internetpolitikken er en synlig del af medarbejdernes hverdag.*

Dette opnås ikke, hvis e-post- og internetpolitikken alene har sin plads i en mappe eller skuffe sammen med medarbejderens ansættelseskontrakt eller personalehåndbog. Eksemplarer af den vedtagne politik kan med fordel placeres, hvor medarbejderne dagligt vil blive gjort opmærksom på den, for eksempel en opslagstavle på medarbejderens kontor. Til brug herfor kan der eventuelt udarbejdes en kortfattet stikordsudgave af politikken. Politikken kan endvidere være umiddelbart tilgængelig i en elektronisk udgave, for eksempel være placeret under eget ikon på „skrivebordet“ på hver enkelt medarbejders computer.

Det er ledelsens ret at fastlægge indholdet af en e-post- og internetpolitik, og medarbejderne skal informeres klart og entydigt.

Jo vigtigere det er for organisationen, at e-post- og internetpolitikken følges, jo vigtigere er det, at politikken synliggøres for medarbejderne og opleves som rimelig.

BILAG

Huskeliste til brug i forbindelse med udarbejdelse af politik for medarbejderes brug af e-post- og internet (ikke udtømmende)

I. Privat brug af e-post og internet på arbejdspladsen?

1. Må medarbejderne gøre privat brug af e-post og internet?
2. Hvis JA, i hvilket omfang?
3. Hvilke grænser for brugen skal gælde, herunder i forbindelse med hjemmearbejds-pladser?
4. Vurdér virksomhedens behov for kontrol med medarbejdernes brug af e-post og internet.
5. Hvis det vurderes, at der er behov for at føre kontrol¹, skal kontrollen da omfatte brug, der fremstår som privat brug?
6. Informér medarbejderne om, at der foretages kontrol af medarbejderens brug af e-post og internet, herunder formål og omfang, og hvordan kontrollen gennemføres.
7. Indhent forhåndssamtykke, hvis kontrollen skal kunne omfatte læsning af privat e-post.
8. Andet

¹ Omfanget af kontrollen skal altid være sagligt begrundet og forfølge en berettiget interesse, for eksempel drifts- og eller sikkerhedsmæssige hensyn eller for at kontrollere, at retningslinjer for anvendelse af e-post og internet overholdes.

II. Håndtering af organisationens anvendelse af e-post og internet i øvrigt

1. I hvilket omfang skal fortrolige informationer kunne sendes via e-post?
2. Skal medarbejderen kunne indgå aftaler på vegne af organisationen via e-post og internet?
3. Hvornår bør identiteten af afsenderen af modtagne e-post meddelelser sikres?
4. Fastsæt eventuelle retningslinjer for
 - sprog, tone og indhold af e-postmeddelelser,
 - hvem e-post bør sendes til,
 - hvornår e-post ikke bør anvendes,
 - signaturregler,
 - anvendelse af autosvar,
 - omgang med filer for at mindske risikoen for virus,
 - tidsfrist for besvarelse af modtaget e-post, herunder e-post til organisationens centrale e-postadresse.
5. Udarbejd eventuel procedure for behandling af e-post, der sendes til fraværende medarbejdere, herunder med angivelse af om e-posten må åbnes og læses af organisationen.
6. Udarbejd eventuel procedure for journalisering, arkivering og sletning af e-postmeddelelser.
7. Udarbejd procedure for behandling af e-postmeddelelser ved en medarbejders fratræden og død, herunder med retningslinjer for den fratrædende medarbejders ret til at slette og medtage e-postmeddelelser.
8. Beskriv organisationens syn på overtrædelse af e-post- og internetpolitikken og forventelige sanktioner.
9. Andet.

