



Övervakning i arbetslivet
**Kontroll av de anställdas Internet-
och e-postanvändning m.m.**

Datainspektionens rapport 2005:3

Innehållsförteckning

1. Inledning	3
2. Sammanfattning	4
3. Personuppgiftslagen (PuL)	7
Allmänt	7
Några grundläggande begrepp	8
4. Internet och e-post	9
4.1. Enkät svar	9
<i>Internetanvändning</i>	9
<i>E-postanvändning</i>	10
4.2. Inspektioner	11
<i>Internetanvändning</i>	11
<i>E-postanvändning</i>	13
4.3. Datainspektionens synpunkter	14
<i>Allmänt</i>	14
<i>Angående avsaknad av regler och kontroll</i>	16
<i>Hur man motverkar oetisk surfning</i>	16
<i>Information</i>	16
<i>Gallring</i>	18
5. Biometriska uppgifter	20
5.1. Enkät svar	20
5.2. Inspektioner	20
5.3. Datainspektionens synpunkter	20
<i>Allmänt</i>	20
<i>Grundläggande krav</i>	21
<i>Tillåten behandling</i>	21
6. Kameraövervakning	23
6.1. Enkät svar	23
6.2. Inspektioner	23
6.3. Datainspektionens synpunkter	24
<i>Allmänt</i>	24
<i>Grundläggande krav</i>	24
<i>Tillåten behandling</i>	24
<i>Information</i>	25

7. Jämförelser med erfarenheter från det tidigare projektet	26
<i>Arbetsgivarnas riktlinjer</i>	<i>26</i>
<i>Samtycke</i>	<i>27</i>
<i>Information</i>	<i>27</i>
<i>Gallring</i>	<i>27</i>
Checklista	29
Tillåten användning av Internet och e-post	29
Begränsningar av Internet- och e-postanvändande	29
Kontroll av Internet- och e-postanvändning	30
Kontroll av innehållet i privata e-postmeddelanden	31
Överträdelse av reglerna	31
Bevarande och gallring	32
Bilaga 1. Tillsynsobjekt (enkätinspektioner)	
Bilaga 2. Enkät	
Bilaga 3. Tillsynsobjekt (fältinspektioner)	

1. Inledning

Datainspektionen har tidigare granskat hur personuppgifter behandlas i arbetslivet för att kontrollera och övervaka anställda. Datainspektionens slutsatser från denna granskning finns redovisade i Datainspektionens rapport 2003:3 ”Behandling av personuppgifter för kontroll av anställda”.

För att följa utvecklingen på området har Datainspektionen under 2005 utökat denna granskning genom att kontrollera fler arbetsgivares behandling av personuppgifter. I det nya projektet har Datainspektionen undersökt arbetsgivarnas kontroll av de anställdas Internet- och e-postanvändning och i vilken omfattning anställda övervakas med hjälp av behandling av biometriska uppgifter och övervakningskameror. Tillsynen omfattar andra företag och myndigheter än i det föregående projektet.

Tillsynen inleddes genom att 103 slumpvis utvalda företag och myndigheter (bilaga 1) skriftligen i en enkät (bilaga 2) fick besvara ett antal frågor om anställdas Internet- och e-postanvändning och den övervakning som sker med hjälp av behandling av biometriska uppgifter och övervakningskameror.

Sedan enkätsvaren sammanställts inspekterades 15 av dessa företag och myndigheter på plats (bilaga 3). Datainspektionen valde i första hand ut företag och myndigheter som utarbetat riktlinjer för övervakning av de anställdas Internetanvändning respektive påbörjat behandling av biometriska uppgifter. I två fall utfördes IT-säkerhetsinspektioner.

Här lämnas en sammanfattning av resultatet av tillsynsprojektet. Därefter redovisas utfallet i enkätinspektionerna och platsinspektionerna. Datainspektionen ger också råd i en checklista om vad en arbetsgivare bör tänka på när riktlinjer för kontroll av de anställdas Internet- och e-postanvändning utformas.

Stockholm i december 2005

2. Sammanfattning

De flesta arbetsgivare har regler för hur Internet och e-post får användas

De flesta arbetsgivare hade någon form av dokumenterad IT-policy som mer eller mindre reglerade de anställdas rätt att använda Internet och e-post. På de allra flesta arbetsplatser hade de anställda rätt att med vissa begränsningar utnyttja Internet och e-post för privat bruk.

Hälften av arbetsgivarna kontrollerar de anställdas Internetanvändning – men inte för att övervaka vad de anställda gör på sin arbetstid

Ungefär hälften av arbetsgivarna uppgav att de utövar någon form av kontroll över de anställdas Internetanvändning. Som syfte med kontrollerna angavs ofta säkerhetsmässiga och tekniska skäl och för att utreda misstanke om brott. Det var däremot mycket ovanligt att arbetsgivare kontrollerade Internetanvändningen för att övervaka vad den anställde gjorde på sin arbetstid. Ett allt vanligare syfte med kontrollerna var i stället att försöka motverka surfning på oetiska webbplatser. Inspektionerna utvisade dock att många av dessa arbetsgivare saknade en klar uppfattning om vad som var att betrakta som oetiskt i dessa sammanhang.

Få arbetsgivare kontrollerar e-posten

Endast ett fåtal av arbetsgivarna uppgav att de kontrollerade de anställdas e-postanvändning. Vid den rutinmässiga kontrollen gick arbetsgivarna i första hand igenom loggfiler. Det förekom inte i något fall rutinmässig genomgång av innehållet i e-postmeddelanden. I princip riskerade den enskilde att kontrolleras endast om något e-postmeddelande förorsakat virusattacker eller överbelastning på systemet samt om misstanke om brott uppstått.

Bristande information – vad är tillåtet och hur utförs kontrollen?

Datainspektionen har inom ramen för projektet tittat närmare på den skriftliga information som arbetsgivarna lämnade till de anställda om den övervakning av Internet- och e-postanvändning som förekom på arbetsplatsen. I ca hälften av de granskade fallen höll arbetsgivarnas informationsmaterial god standard. Drygt tio procent av de arbetsgivare som omfattades av undersökningen saknade riktlinjer helt och hållet.

En vanligt förekommande brist i informationen var att det inte klart framgick vilka begränsningar som gällde för den anställdes Internetanvändning. Av informationen framgick endast att den anställde inte fick utnyttja Internet och e-posten i ”tvivelaktiga och oseriösa sammanhang” eller i enlighet med ”underförstådda etiska regler”.

Vidare saknade nära hälften av de arbetsgivare som utförde någon form av kontroll av arbetstagarnas Internetanvändning regler för hur denna kontroll skulle ske. Motsvarande siffra vid kontroll av e-post var 20 procent. Var fjärde arbetsgivare som utförde kontroller lämnade över huvud taget inte någon information om kontrollen till de anställda.

Även om det blivit vanligare att samtycke inhämtades till de kontroller som utfördes skedde detta fortfarande bara i en minoritet av fallen. I en dryg tredjedel av fallen omfattades kontrollerna av någon form av facklig överenskommelse.

Gallring – få har rutiner

Enkätsvaren och erfarenheter från inspektionerna visade att det fortfarande är vanligt att arbetsgivare inte utarbetat några gallringsrutiner med beaktande av bestämmelserna i personuppgiftslagen (PuL). Datainspektionen anser att uppgifter som ligger till grund för arbetsgivarens övervakning av den anställdes Internet- och e-postanvändning i normala fall bör gallras senast efter tre månader.

Datainspektionen har kunnat konstatera att det förekommer att arbetsgivare använder sig av särskilda spärprogram som förhindrar surfning på oetiska webbplatser. Genom spärprogrammet uppnår man i denna del syftet utan en närgången och omfattande övervakning av de anställda.

Ytterst sällsynt att biometri används

Vad gäller behandling av den anställdes biometriska uppgifter var detta än så länge mycket ovanligt. Endast en av de granskade arbetsgivarna använde de anställdas biometriska personuppgifter för autentisering/verifiering eller identifiering. Ett fåtal arbetsgivare uppgav att det fanns planer på att i framtiden påbörja hantering av de anställdas biometriska uppgifter. Datainspektionen pekar i rapporten på vissa frågor som en arbetsgivare måste beakta om man överväger att påbörja en sådan behandling.

Kameraövervakning är ovanligt och används inte för prestationsmätning

Även kameraövervakning av de anställda på arbetsplats dit allmänheten inte har tillträde var relativt ovanlig. Åtta arbetsgivare uppgav att sådan övervakning skedde på ett sätt att det omfattas av PuL. Den övervakning som skedde utfördes av säkerhetsmässiga och tekniska skäl samt för att motverka och utreda brott. Inte i något fall skedde kontroll för att övervaka den anställdes arbetsprestation. De områden som kamerorna var riktade mot var sådana den anställda kunde tänkas passera förbi, men inte typiskt sett utför sitt arbete på.

Vad gäller den kameraövervakning som förekom såg Datainspektionen i huvudsak två brister:

- I flera fall förekom långa, eller inga, gallringstider av inspelningarna. Med hänsyn till de ändamål för övervakning som uppgavs i enkätsvaren anser Datainspektionen att daglig eller veckovis gallring i normalfallet bör vara ett riktmärke.
- Den information som lämnas till arbetstagarna är bristfällig. Enligt Datainspektionens mening sträcker sig PuL:s krav på information längre än kravet på upplysning om kameraövervakning i lagen om allmän kameraövervakning. I de fall kameraövervakningen omfattas av PuL räcker det därför inte med att sätta upp skyltar i de utrymmen där kameraövervakning bedrivs, vilket var fallet hos några av arbetsgivarna i denna studie.

Sammanfattningsvis kan sägas att projektet har utvisat att många arbetsgivare har tekniska möjligheter att utöva en omfattande kontroll av de anställdas Internet- och e-postanvändning, men att få arbetsgivare utnyttjar dessa möjligheter i dagsläget. Det finns påtagliga brister beträffande informationen till de anställda om den begränsade kontroll som utövas i dag. Många arbetsgivare behöver också förbättra informationen angående hur IT-verktygen får användas.

3. Personuppgiftslagen (PuL)

Allmänt

Syftet med PuL är att skydda människor mot att deras personliga integritet kränks genom behandling av personuppgifter.

PuL tillämpas på all behandling av personuppgifter som utförs helt eller delvis med hjälp av datorer. PuL gäller inte om det skulle strida mot tryck- eller yttrandefriheten. Om det i en annan lag eller förordning finns bestämmelser som avviker från PuL gäller de bestämmelserna i stället för PuL.

PuL innehåller regler om grundläggande krav som gäller för all behandling av personuppgifter. Personuppgifter får t.ex. endast samlas in för särskilda, uttryckligt angivna och berättigade ändamål. Uppgifter som samlas in för ett visst ändamål får sedan inte behandlas för något ändamål som är oförenligt med det ursprungliga. Fler uppgifter än vad som är nödvändigt med hänsyn till ändamålen får inte behandlas. Personuppgifterna som behandlas ska även vara riktiga och – om nödvändigt – aktuella, samt får inte bevaras under längre tid än vad som är nödvändigt med hänsyn till ändamålen med behandlingen.

PuL innehåller regler för när behandling av personuppgifter är tillåten. Personuppgifter får behandlas om den registrerade har lämnat sitt samtycke till behandlingen. Eftersom ett samtycke enligt PuL måste vara frivilligt är behandling av personuppgifter i arbetslivet med stöd av samtycke begränsat till sådana situationer där arbetstagaren har ett verkligt fritt val och senare kan ta tillbaka sitt samtycke utan att det medför några nackdelar för honom eller henne. Utan samtycke får uppgifterna bara behandlas när behandlingen är nödvändig för vissa i lagen angivna syften. Det kan t.ex. vara tillåtet för arbetsgivaren att kontrollera arbetstagaren efter en intresseavvägning. Kontrollen ska vara nödvändig för att ett ändamål som rör ett berättigat intresse ska kunna tillgodoses – om detta intresse väger tyngre än den registrerades intresse av skydd mot kränkning av den personliga integriteten.

I PuL finns också restriktioner när det gäller behandling av känsliga personuppgifter, uppgifter om lagöverträdelse m.m. och uppgift om personnummer. Det finns också bestämmelser om bl.a. information till de registrerade, om rättelser av uppgifter och om IT-säkerhet.

Den personuppgiftsansvarige är skyldig att anmäla sin behandling av personuppgifter till Datainspektionen. Huvudregeln är att varje enskild behandling av personuppgifter ska anmälas till Datainspektionen. Från denna bestämmelse finns dock undantag. Anmälan kan i vissa fall ersättas av en egen förteckning som den personuppgiftsansvarige själv upprättar och för. Detta gäller bl.a.

om det finns en anknytning mellan den registrerade och den personuppgiftsansvarige genom t.ex. anställning när behandlingen inte omfattar känsliga personuppgifter.

PuL innehåller bestämmelser om straff, böter eller fängelse i högst sex månader för den som bryter mot vissa bestämmelser i lagen. Är brottet grovt är straffet fängelse i högst två år. I ringa fall döms inte till straff. En personuppgiftsansvarig som behandlar personuppgifter i strid med PuL kan bli skadeståndsskyldig gentemot den registrerade och dömas att ersätta denne för skada och kränkning av den personliga integriteten som den olagliga behandlingen har orsakat.

Några grundläggande begrepp

Personuppgifter – all slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet.

Behandling av personuppgifter – varje åtgärd eller serie av åtgärder som vidtas i fråga om personuppgifter, vare sig det sker på automatisk väg eller inte, t.ex. insamling, registrering, organisering, lagring, bearbetning eller ändring, återvinning, inhämtande, användning, utlämnande genom översändande, spridning eller annat tillhandahållande av uppgifter, sammanställning eller samkörning, blockering, utplåning eller förstöring.

Personuppgiftsansvarig – den som ensam eller tillsammans med andra bestämmer ändamålen, dvs. syftet med och medlen för behandlingen av personuppgifter.

Den registrerade – den som en personuppgift avser.

Personuppgiftsbiträde – den som behandlar personuppgifter för den personuppgiftsansvariges räkning.

Samtycke – varje slag av frivillig, särskild och otvetydig viljeyttring genom vilken den registrerade, efter att ha fått information, godtar behandling av personuppgifter som rör honom eller henne.

4. Internet och e-post

4.1. Enkät svar

Internetanvändning

Av de 103 arbetsgivarna uppgav 91 att de hade regler för den anställdes Internetanvändning. I 84 fall fanns dessa regler dokumenterade. I de flesta fall fanns information om reglerna utlagd på arbetsgivarens intranät. I två fall uppgav arbetsgivaren att regler visserligen fanns, men att ingen information om reglerna lämnades.

Sju av arbetsgivarna tillät inte att den anställda utnyttjade Internet för privat bruk över huvud taget. Sex av dessa tillhörde det privata näringslivet.

Av enkät svaren framgick att 44 av arbetsgivarna utförde någon form av kontroll av arbetstagarnas Internetanvändning. I knappt hälften (19) av dessa fall saknades regler/riktlinjer för hur denna kontroll skulle ske. 57 arbetsgivare svarade att ingen sådan kontroll förekom.

Kontroll skedde ofta av säkerhetsmässiga och tekniska skäl. I 30 av fallen skedde kontrollen även för att motverka surfning på s.k. oetiska webbplatser. Det var däremot bara två arbetsgivare som uppgav att kontroll skedde för att övervaka vad den anställda gjorde på sin arbetstid.

Vad gäller kontrollernas omfattning utfördes dessa i de flesta fallen antingen slumpmässigt eller på förekommen anledning, exempelvis vid misstanke om brott. Stickprovskontroll förekom i tretton fall. Stickprovskontrollerna skedde till övervägande del mer sällan än en gång i månaden. I nio av fallen uppgav arbetsgivaren att all Internetanvändning kontrollerades.

När kontroller genomfördes skedde detta i 35 av de 44 fallen genom en genomgång av loggfiler. I de flesta fallen kunde loggen knytas till en enskild individ genom IP-adress/användar-ID. Endast i två fall användes information i cookies för att följa upp den anställdes surfande. I några fall användes automatisk blockering för att förhindra att oetiska webbplatser besöktes.

Information om den kontroll som sker lämnades i ca tre fjärdedelar av fallen. I övrigt lämnades ingen information alls.

I en majoritet av fallen, 23 stycken, skedde kontrollen utan den anställdes samtycke.

I 16 av fallen fanns det någon form av facklig överenskommelse angående kontrollerna.

De rutiner som arbetsgivarna tillämpade för gallring av de loggade uppgifter som låg till grund för kontrollen av de anställdas Internetanvändning uppvisade stora olikheter. I vissa fall förekom gallring varje vecka, i fyra fall skedde ingen gallring över huvud taget.

E-postanvändning

Av de 103 arbetsgivarna uppgav 85 att de hade regler för den anställdes e-postanvändning. I 78 fall fanns dessa dokumenterade. I de flesta fall fanns information om reglerna utlagd på arbetsgivarens intranät. I samtliga fall lämnades någon form av information.

Åtta av arbetsgivarna tillät inte att den anställda utnyttjade e-post för privat bruk över huvud taget. Sex av dessa tillhörde det privata näringslivet.

Av enkätsvaren framgick att 15 av arbetsgivarna utförde någon form av kontroll av arbetstagarnas e-postanvändning. I tre av dessa fall saknades regler/riktlinjer för hur denna kontroll skulle ske. 86 arbetsgivare svarade att ingen sådan kontroll förekom.

Kontroll skedde av säkerhetsmässiga och tekniska skäl samt för att utreda misstanke om brott. Inte i något fall skedde kontroll för att övervaka vad den anställda gjorde på sin arbetstid. I ett fall saknades dokumenterat syfte för kontrollen.

Vad gäller kontrollens omfattning utfördes kontrollerna hos två arbetsgivare vid misstanke om brott. Stickprovskontroll förekom i tre fall. I två av de 15 fallen kontrollerades all e-postanvändning.

När kontroller genomfördes skedde detta i nio av de 15 fallen genom en genomgång av loggfiler. I sex av fallen genomgicks enskilda e-postmeddelanden.

De flesta arbetsgivare lämnade skriftlig eller muntlig information om den kontroll som sker. I tre av fallen lämnades dock ingen information alls.

I sju av fallen uppgav arbetsgivaren att den anställda lämnade samtycke till kontrollen. I två av fallen uppgavs kontrollen ske utan den anställdes samtycke.

I sex av fallen fanns det någon form av facklig överenskommelse angående kontrollerna.

Det rådde mycket stora olikheter i arbetsgivarnas gallringsrutiner. Gallringen kunde vara systemstyrd eller ske efter varje utredning. Där regelbunden gallring förekom skedde denna årsvis. I tre fall skedde ingen gallring över huvud taget.

4.2. Inspektioner

Datainspektionen inspekterade 15 av arbetsgivarna på plats. Genom dessa inspektioner kunde enkätsvaren i vissa delar korrigeras och nyanseras. Inspektionerna utvisade att enkätsvaren generellt sett var korrekta men i vissa enstaka fall ofullständiga och i något fall missvisande. Datainspektionen bedömer dock att de generella slutsatser som kan dras av enkätsvar och av vad som framkommit vid inspektioner är tillförlitliga.

Vid inspektionerna framkom bl.a. följande omständigheter som Datainspektionen sedermera tagit hänsyn till när enkätsvaren tolkats.

Internetanvändning

En av de arbetsgivare som i enkäten uppgivit att de anställda inte fick utnyttja Internet för privat bruk över huvud taget inspekterades på plats. Inspektionen utvisade att arbetsgivaren i praktiken tillät viss användning av Internet för privata ändamål på lunch- och kafferaster. Det formella förbudet berodde på att företaget ville undvika att det skapades en privat sfär på datorn, något som kunde leda till problem exempelvis i samband med säkerhetskopiering.

Enligt enkätsvaren utövade tolv av de utvalda arbetsgivarna någon form av kontroll av de anställdas Internetanvändningen, medan tre uppgav att de inte gjorde det.

Enligt enkätsvaren kontrollerade fyra av de inspekterade arbetsgivarna all Internetanvändning. Vid inspektionerna framkom att det i tre av dessa fall i första hand handlade om löpande driftskontroll. Endast i ett av fallen förekom kontroll och uppföljning av de anställdas surfvanor. Inspektionerna utvisade att fler än dessa fyra arbetsgivare kontrollerade all Internetanvändning i den meningen att de löpande övervakade nätverksdriften.

Vid inspektionerna framkom att de arbetsgivare som inte uppgivit att kontroll kunde ske för att kunna utreda misstanke om brott, i praktiken kunde tänka sig att genomföra kontroll för detta ändamål. Det gällde även arbetsgivare som påstått att ingen kontroll skedde över huvud taget.

Enligt enkätsvaren kontrollerade fem av de inspekterade arbetsgivarna Internetanvändningen för att motverka surfning på oetiska webbplatser. Inspektionerna utvisade att arbetsgivarna försökte nå detta mål på olika sätt.

Den förste arbetsgivaren gjorde ingen kontroll på individnivå. Undersökningarna hade endast till syfte att se var arbetstagarkollektivet surfar.

Den andre arbetsgivaren kontrollerade en gång per månad om oetiska webbplatser besökts. I samband därmed togs en lista fram med uppgift om vilka webbplatser som de anställda besökt. Om en anställd besökt oetiska webbplatser togs en diskussion upp med den enskilde.

Den tredje arbetsgivaren anlätade ett externt bolag som kontrollerade hot mot driften. I samband därmed kunde det externa bolaget rapportera surfning som kunde innefatta brott.

Den fjärde arbetsgivaren tog en gång i månaden fram en lista som visade hur många timmar personalen surfat på Internet. Av denna lista framgick inte enskilda individers surfning. Kontroll av enskild arbetstagares surfning beslutades av personalchef. En sådan kontroll initierades efter påpekande från linjechef.

Den femte arbetsgivaren hade en teknisk blockering (outsourcad) som skulle hindra de flesta försök att surfa på oetiska webbplatser. Misstänkt missbruk utreddes av arbetsgivarens säkerhetsavdelning.

Utöver dessa fem arbetsgivare som uppgivit att kontroll skedde, utvisade inspektionerna att det fanns ytterligare en arbetsgivare som i praktiken vidtog åtgärder för att motverka surfning på oetiska webbplatser. Denne arbetsgivare tog i samband med övervakning av nätverkstrafiken ut en lista över s.k. "larm". Ett larm uppkom när vissa ord, i praktiken engelska ord som kan förekomma på pornografiska webbplatser, förekom. Uppgifterna om larm hade dock ännu inte använts i något enskilt fall.

Vid inspektionerna framkom att fyra arbetsgivare hade särskilda programvaror som förhindrade surfning på oetiska webbplatser.

Enligt enkätsvaren kontrollerade en av de inspekterade arbetsgivarna Internetanvändningen för att se vad den anställde gör på sin arbetstid. Arbetsgivaren tog en gång i månaden fram en lista som visade hur många timmar personalen surfat på Internet. Av denna lista framgick inte enskilda individers surfning.

Av de femton arbetsgivare som inspekterades hade tre uppgett att de inte kontrollerade Internetanvändningen över huvud taget. Inspektionerna utvisade att dessa tre arbetsgivare i praktiken utövade, eller i framtiden kunde tänkas utöva, en viss sådan kontroll. En av arbetsgivarna kunde följa upp loggar vid misstanke om brott. Denne arbetsgivare använde dessutom Telias spärrtjänst för att motverka att den anställde surfar på förbjudna webbplatser. Den andre arbetsgivaren kunde komma att installera surfningsfilter på enskilda förvaltningar om behov skulle uppstå. Det hade förekommit misstanke om, och i

något fall bekräftats, att anställda surfat på pornografiska webbplatser. Detta upptäcktes dock inte med hjälp av behandling av personuppgifter utan av kollegor. Hos den tredje arbetsgivaren hade en anställd påkommit med att surfa på pornografiska webbplatser. Även i detta fall gjordes upptäckten av kollegor.

Vid inspektionerna framkom att det rådde viss osäkerhet om vad som var att betrakta som en oetisk webbplats. Alla arbetsgivare ansåg att pornografiska och rasistiska webbplatser hörde till denna grupp. Därutöver avgjorde arbetsgivare från fall till fall vad som kunde anses vara oetiskt. Arbetsgivare som utrett saken närmare kunde anse att även spelsidor, sidor med terroristanknytning, sidor för fildelning, sidor som bryter mot upphovsrättslagen och sidor som rent allmänt ”strider mot svensk lagstiftning” var att betrakta som oetiska.

Nio arbetsgivare uppgav att utredning av enskilda arbetstagares Internet-surfning förekommit.

E-postanvändning

En av arbetsgivarna som inspekterades på plats hade uppgivit att de anställda inte fick utnyttja e-posten för privat bruk över huvud taget. Inspektionen utvisade dock att arbetsgivaren i praktiken tillät viss användning av e-post för privata ändamål. E-posten fick utnyttjas för enklare privata ärenden på samma sätt som en tjänstetelefon.

Enligt enkätsvaren kontrollerade sju av de utvalda inspektionsobjekten e-postanvändningen medan åtta inte gjorde det.

Vid den rutinmässiga kontrollen gick arbetsgivarna i första hand igenom logg-filer. Det förekom inte i något fall rutinmässig genomgång av innehållet i e-postmeddelanden. Genomgång av innehållet i enskilda e-postmeddelanden kunde bli aktuell om den anställdes anställning upphört, vid långtidsfrånvaro eller i samband med misstanke om brott.

Inspektionerna utvisade att enkätsvaren inte varit uttömmande. Flera av de arbetsgivare som sade sig kontrollera e-postanvändningen övervakade endast trafiken av tekniska och säkerhetsmässiga skäl. Kontroll av enskilda anställda genomfördes endast vid misstanke om brott, vilket var mycket sällsynt. Det visade sig även att de arbetsgivare som uppgivit att ingen kontroll skedde, i praktiken kunde tänka sig att genomföra kontroll i samband med misstanke om brott.

Av undersökningen framgick att många arbetsgivare hade möjlighet att kontrollera de anställdas e-postanvändning. Ingen av de inspekterade arbetsgivarna genomförde dock några rutinmässiga kontroller av den anställdes e-postanvändning. I princip riskerade den enskilde att kontrolleras endast i

de fall dennes e-posttrafik förorsakat virusattacker eller överbelastning på systemet samt om misstanke om brott uppstått. Fyra av arbetsgivarna uppgav att de vid något tillfälle kontrollerat innehållet i enskilda anställdas e-post.

4.3. Datainspektionens synpunkter

Allmänt

Arbetsgivaren är ansvarig för den behandling av personuppgifter som utförs i arbetet. Enligt de grundläggande kraven i PuL får personuppgifter bara samlas in för särskilda, uttryckligt angivna och berättigade ändamål. Ändamålen med behandlingen bestämmer sedan hur arbetsgivaren får använda de redan insamlade uppgifterna.

En arbetsgivare som samlar in uppgifter om sina anställda genom IT-verktygen, t.ex. genom loggning, ska vid insamlingen klart och tydligt ha bestämt för vilka ändamål som uppgifterna ska användas. Det är inte tillåtet att använda logguppgifter för ändamål eller syften som är oförenliga med de ursprungligen bestämda. Det är inte tillräckligt att som ändamål bestämma att uppgifterna kan komma att användas för kontroller. Syftet med kontrollen måste framgå, t.ex. om Internettrafiken övervakas av tekniska och säkerhetsmässiga skäl, eller för att följa upp att de interna reglerna följs.

När uppgifterna samlas in ska de registrerade dessutom ha fått information om ändamålen med behandlingen. Den anställdes intresse av att få information kan förväntas vara särskilt starkt när det gäller vilka kontroller som han eller hon kan komma att utsättas för med hjälp av de insamlade uppgifterna.

Ändamålen med behandlingen avgör dessutom hur länge personuppgifterna får sparas.

I PuL finns det en uttömmande uppräkningslista för i vilka fall behandling av personuppgifter är tillåten. Arbetsgivarens behandling av personuppgifter i samband med kontroll av arbetstagaren kan bl.a. vara tillåten med stöd av arbetstagarens samtycke, ett avtal mellan arbetsgivaren och arbetstagaren eller för att kunna fullgöra en rättslig skyldighet. Behandlingen kan också vara tillåten efter en intresseavvägning. Om behandlingen inte kan hänföras till någon situation som PuL tillåter är behandlingen och därmed kontrollen olaglig. Arbetsgivaren bör alltid ha gjort klart för sig med vilket lagligt stöd i PuL som arbetstagarens personuppgifter behandlas.

Inledningsvis bör arbetsgivaren ta ställning till om syftet med behandlingen motiverar att den utförs på individnivå. Det strider nämligen mot PuL att behandla personuppgifter om det inte är nödvändigt. Det kan ibland vara

tillräckligt att utföra kontroller på så sätt att enskilda inte kan identifieras, t.ex. på gruppnivå.

För att ett samtycke ska vara giltigt enligt PuL måste arbetstagaren ha fått sådan information att han eller hon förstår vad samtycket innebär. Ett samtycke enligt PuL ska vara individuellt, frivilligt, särskilt, otvetydigt och informerat. Det är inte tillräckligt att samtycka till att kontroller kan utföras enligt PuL. Det är inte heller tillräckligt att endast ha fått information om att loggning sker. En arbetstagarorganisation kan inte heller samtycka för medlemmarnas räkning.

Behandling av personuppgifter för individuell kontroll av arbetstagarens Internet- och e-postanvändning kan vara tillåten i den mån det är nödvändigt för att kunna fullgöra en rättslig skyldighet. Ett exempel kan vara att en offentlig arbetsgivare behöver ta del av de uppgifter som finns i ett e-postmeddelande för att kunna uppfylla myndighetens skyldigheter om allmänna handlingars offentlighet. De krav som offentlighetsprincipen ställer på en arbetsgivare kan dock inte medföra en rätt för arbetsgivaren att ta del av vad som tydligt framgår är arbetstagarens privata e-post. Arbetsgivaren ska omedelbart avbryta läsningen av ett e-postmeddelande som han eller hon inser är privat.

PuL tillåter behandling av personuppgifter efter en intresseavvägning. En arbetsgivare som för sin kontroll vill behandla personuppgifter om arbetstagaren kan således överväga att tillämpa intresseavvägningen som lagligt stöd för sin behandling.

I vilka fall som en arbetsgivares intresse väger över de registrerades intresse att få ha sina personuppgifter i fred får avgöras efter en bedömning av omständigheterna i det enskilda fallet. Vid denna bedömning kan man bl.a. ta hänsyn till om arbetsgivaren följer reglerna i PuL t.ex. när det gäller kraven på information, väl avvägda gallringsrutiner samt skydd mot obehörig åtkomst. De grundläggande kraven i PuL måste också alltid beaktas och gör sig inte minst gällande vid tillämpningen av intresseavvägningen.

Fackliga överenskommelser som rör behandling av personuppgifter i kontrollsyfte kan väga tungt vid en intresseavvägning.

Om arbetstagaren uttryckligen har motsatt sig personuppgiftsbehandlingen, krävs det starka skäl för att med stöd av en intresseavvägning få utföra kontrollen.

Angående ansaknad av regler och kontroll

Av enkätsvaren framgick att tio arbetsgivare saknade regler för såväl Internet- som e-postanvändningen. Dessa arbetsgivare utövade inte någon kontroll över denna användning. Enligt Datainspektionens erfarenhet kan dock de flesta arbetsgivare antas ha olika värderingar och ideal, oavsett om dessa uttalas eller inte. Datainspektionen anser att samtliga arbetsgivare som utnyttjar Internet och e-post i sin verksamhet bör ha en Internet-policy som innehåller riktlinjer för Internet- och e-postanvändning. För det fall arbetsgivaren inte anser att några begränsningar av de anställdas Internet- och e-postanvändning behövs bör även denna ståndpunkt formuleras som en riktlinje.

Hur man motverkar oetisk surfning

Datainspektionen konstaterar att arbetsgivare som vill motverka att anställda surfar på oetiska webbplatser på Internet kan gå till väga på åtminstone två sätt. Antingen kontrollerar arbetsgivaren den surfning som förekommer och förbehåller sig rätten att i efterhand gå in och vidta åtgärder mot dem som missbrukar Internet. Ett annat alternativ är att arbetsgivaren redan från början försöker omöjliggöra sådan surfning genom särskilda spärprogram.

Genom ett spärprogram kan tillgång till vissa webbplatser blockeras. Spärprogrammet kan också, utan att blockera webbplatsen, vid påloggning tala om för användaren att den eftersökta webbplatsen kan vara av tvivelaktig karaktär.

Datainspektionen anser att arbetsgivare som vill begränsa de anställdas rätt att surfa på oetiska webbplatser bör överväga om det är lämpligt att införskaffa sådana spärprogram. På vissa arbetsplatser behöver de anställda tillgång till allehanda webbplatser i sin tjänsteutövning, men i många fall skulle ett sådant spärprogram medföra att risken för att de anställda medvetet eller omedvetet utnyttjar Internet i strid med givna riktlinjer minskar betydligt. Därmed kan behovet av närgångna kontroller av de anställdas Internetanvändande antas bli mindre. Dessutom minskar risken för att arbetsgivaren ska behöva genomföra en för alla parter påfrestande utredning av misstänkta oegentligheter.

Information

Av PuL framgår att den personuppgiftsansvarige vid behandling av personuppgifter ska lämna den registrerade information som omfattar:

- uppgift om vem som är personuppgiftsansvarig
- uppgift om ändamålen med behandlingen

- all övrig information som behövs för att den registrerade ska kunna ta till vara sina rättigheter i samband med behandlingen, såsom information om mottagarna av uppgifterna, skyldighet att lämna uppgifter och rätten att ansöka om information och få rättelse.

Arbetsgivaren är således skyldig att informera sina anställda om den personuppgiftsbehandling som sker i samband med övervakning av den anställdes Internet- och e-postanvändning. Skyldigheten att informera innebär att det ska framgå av arbetsgivarens riktlinjer vilken kontroll som kan komma att ske. Det finns däremot inget krav på att den anställda informeras vid varje enskilt kontrolltillfälle. Som tidigare nämnts framgick det av enkätsvaren att det fanns ett flertal arbetsgivare som inte informerade de anställda om vilka kontroller av Internet- och e-postanvändningen som genomfördes. I ett par fall lämnade arbetsgivaren över huvud taget inte någon information om vilka regler som gällde på arbetsplatsen. De flesta arbetsgivare lämnade dock någon form av information om vilka regler som gällde och vilka kontroller av Internet- och e-postanvändningen som genomfördes.

I de fall information faktiskt lämnas måste denna stå i överensstämmelse med bestämmelserna i PuL. För att kunna bedöma informationens kvalitet inhämtade Datainspektionen den skriftliga information som arbetsgivarna lämnade till de anställda.

Av de drygt 80 arbetsgivare som uppgav att det fanns dokumenterad information bifogade 79 arbetsgivare informationen med enkäten. Med anledning av det inhämtade materialet lämnar Datainspektionen följande kommentarer.

Den information som lämnades om arbetsgivarens regler för Internet- och e-postanvändning kan sägas leva upp till god standard i drygt hälften av fallen. I övriga fall hade information brister. I ca 15 fall var informationen klart otillräcklig. Att informationen i vissa fall var otillräcklig kunde naturligtvis bero på att de regler som informationen refererade till var bristfälliga.

De anställda hade i de allra flesta fall rätt att med vissa begränsningar utnyttja Internet och e-post för privat bruk. I de flesta fall som informationen var bristfällig hörde detta samman med att det inte klart framgick vilka begränsningar som gällde för den anställdes Internetanvändning. Informationen var ofta alltför allmänt hållen. Det är exempelvis inte lämpligt att enbart hänvisa de anställda till att inte utnyttja Internet i ”tveklaktiga och oseriösa sammanhang” eller i enlighet med ”underförstådda etiska regler”.

Det var vanligt förekommande att informationsmaterialet inte innehöll någon hänvisning till bestämmelserna i PuL. Datainspektionen anser att det är lämpligt att en sådan hänvisning görs för att den anställda ska kunna tillvarata sina rättigheter.

Ett annat förekommande fel var att informationen angav att den anställde inte fick utnyttja Internet eller e-post för privat bruk över huvud taget trots att viss sådan användning i praktiken var tillåten. För det fall en arbetsgivare tillåter viss privat användning av Internet- och e-post bör inte informationen ge något annat vid handen.

En allvarlig brist som Datainspektionen noterade var att ett stort antal arbetsgivare, ca 25 stycken, lämnade ingen eller otillräcklig information om den kontroll av den anställdes Internetanvändning som kunde bli aktuell. Av informationen kunde exempelvis framgå att ”Internettrafiken loggas” och att det genomfördes ”kontroll av loggarna vid misstanke om missbruk”. Enligt PuL är det aldrig tillåtet för en arbetsgivare att behandla personuppgifter om arbetstagaren i smyg. Det är inte tillräckligt att den anställde har fått information om att kontroller eller loggning kan förekomma. Syftet med behandlingen måste alltid framgå. Den anställde ska ha fått informationen senast i samband med att de uppgifter som ligger till grund för kontrollen samlades in. Det finns inget krav på att informera den anställde inför varje enskild kontroll.

Det förekom även att arbetsgivare lämnade ingen eller otillräcklig information om den kontroll av den anställdes e-postanvändning som kunde bli aktuell.

Sammanfattningsvis kan sägas att Datainspektionens utredning visar att många arbetsgivare bör komplettera eller omarbete sina riktlinjer för användning av Internet och e-post. Det ankommer på den enskilde arbetsgivaren att själv utforma sina riktlinjer. Någon form av ”standardriktlinjer” som passar alla arbetsgivare finns dessvärre inte. I vilken omfattning de anställda får använda Internet och e-post för privat bruk och vilken kontroll av denna användning som befinner sig nödvändig är en fråga som måste avgöras på den enskilda arbetsplatsen. För att underlätta för arbetsgivare att utforma riktlinjer som uppfyller PuL:s krav på information har Datainspektionen sammanställt en ”checklista”, se sidan 29. I checklisten tar Datainspektionen upp de punkter som bör finnas med i arbetsgivarens riktlinjer om de anställda har tillgång till Internet och e-post.

Gallring

Personuppgifter får inte bevaras under längre tid än vad som är nödvändigt med hänsyn till ändamålet med behandlingen. Det innebär att det är ändamålet, dvs. anledningen till att personuppgifterna behandlas, som avgör hur länge uppgifterna får bevaras i identifierbart skick.

När ändamålet med behandlingen av personuppgifter är övervakning av de anställdas Internet- och e-postanvändning ska uppgifterna som ligger till grund för kontrollen av den anställdes Internet- och e-postanvändning avidentifieras eller förstöras så snart de inte längre har någon betydelse för denna övervakning. Frågan om bevarande och gallring blir därmed beroende av vilka kontrollrutiner som arbetsgivaren slagit fast i sina interna riktlinjer.

Om arbetsgivaren kontrollerar de anställdas Internetanvändning genom att exempelvis genomföra regelbundna kontroller, eller stickprovskontroller, en gång i månaden kan en rimlig period att bevara uppgifterna vara tre månader, så länge inte uppgifterna måste bevaras för andra ändamål. Om arbetsgivaren genomför kontroller med något längre mellanrum kan det finnas anledning att i motsvarande mån bevara uppgifterna en något längre tid. För det fall arbetsgivarens kontroll leder till att en utredning av den anställdes Internetanvändning påbörjas får arbetsgivaren bevara de aktuella uppgifterna så länge utredningen pågår.

Om arbetsgivaren inte övervakar de anställdas Internet- och e-postanvändning över huvud taget kan det vara rimligt att uppgifterna gallras inom en månad.

5. Biometriska uppgifter

5.1. Enkät svar

Av de 103 arbetsgivarna uppgav tre stycken att de registrerade biometriska uppgifter. Dessa tre arbetsgivare inspekterades på plats.

Endast tre av de övriga 100 arbetsgivarna uppgav att det fanns planer på att i framtiden påbörja hantering av biometriska uppgifter.

5.2. Inspektioner

Datainspektionens avsikt med enkätfrågorna om biometriska personuppgifter var i första hand att granska de fall där de anställdas biometriska personuppgifter användes för autentisering/verifiering eller identifiering. En av inspektionerna visade att någon behandling av biometriska uppgifter i denna mening inte skedde.

En annan av inspektionerna utvisade att det inte förkom någon registrering av biometriska uppgifter som låg inom den arbetsgivarens personuppgiftsansvar. Vid inspektionen framkom dock att det, inom ramen för den aktuella arbetsgivarens personuppgiftsansvar, förekommit tester med registrering av fingeravtryck på personer som varit intresserade av att pröva att använda fingeravtryck vid påloggning på ADB-systemet. Arbetsgivaren har dock inte gått vidare med denna teknik.

Den tredje arbetsgivaren som inspekterades på plats tillverkar medicinska preparat. Tillverkningsprocessen är ur hygienisk synvinkel mycket känslig och om fel uppkommit är det av stor vikt att preparatet kan spåras tillbaka till källan. Arbetsgivaren använde därför ett system för iriskontroll av anställda vid inloggning och signering till fyllningsrobotar i fyllningslokalerna. Uppgift om den anställdes iriskod lagrades i ett behörighetssystem och kopplades till ett användarkonto som innehöll bl.a. fullständigt namn. Iriskoden användes sedan för att säkerställa verifiering av användare vid signering av händelser samt att endast behörig personal har tillgång till robotar. Att just iris användes beror på att miljön i fyllningslokalerna inte tillät tangentbord eller fingeravtrycksläsare.

5.3. Datainspektionens synpunkter

Allmänt

Kännetecknande för biometriska uppgifter är att de går att härleda till den mänskliga kroppen genom att dessa uppgifter finns hos varje person. De är också utmärkande för varje person och är antingen permanenta, det vill säga de förändras inte över tiden, eller åtminstone stabila över en viss tidsperiod.

Exempel på biometriska uppgifter är fingeravtryck, ansiktsegenskaper, irismönster och handgeometri. Användningen av biometriska uppgifter i arbetslivet är en relativt ny företeelse. Utöver de i detta projekt aktuella ärendena har Datainspektionen ännu inte behandlat frågan inom ramen för något tillsynsärende. Datainspektionen har således än så länge ingen praxis att tala om i frågan. Nedan berörs några av de frågor som bör beaktas vid behandling av biometriska uppgifter i arbetslivet.

Grundläggande krav

I 9 § PuL finns grundläggande krav som alltid måste vara uppfyllda för att det ska vara tillåtet att behandla personuppgifter. Dessa krav kan till exempel innebära att en arbetsgivares behandling av personuppgifter i syfte att utföra kontroller inte får genomföras på ett sätt som innebär en mycket närgången och omfattande övervakning av den anställde. Biometriska uppgifter möjliggör en unik och livslång identifiering av en person vilket gör uppgifterna särskilt integritetskänsliga. Användningen av biometriska uppgifter ger även upphov till integritetsrisker som kan vara svåra att överblicka i dagsläget. Att behandla biometriska uppgifter om den anställde kan mot den bakgrunden anses förenligt med de grundläggande kraven på behandling av personuppgifter i 9 § PuL endast när vikten av en säker identifiering är stor. Det kan exempelvis i normalfallet inte anses förenligt med de grundläggande kraven i PuL att behandla biometriska uppgifter om den anställde i syfte att kontrollera arbetstid och närvaro på arbetsplatsen. Däremot kan behandling av biometriska uppgifter vara förenlig med de grundläggande kraven om den sker i syfte att starta datorer eller annan teknisk utrustning, logga in på nätverk eller signera dokument eller i samband med tillträde till låsta utrymmen. Exempelvis anser Datainspektionen att den på föregående sida refererade användningen av iriskontroll för inloggning och signering av fyllnadsrobotar är förenlig med 9 § PuL. I situationer där det tidigare inte ansetts nödvändigt med identifiering över huvud taget kan vikten av en säker identifiering inte anses stor. Arbetsgivaren måste alltid ställa sig frågan om det aktuella syftet kan tillgodoses på ett för den anställde mindre integritetskränkande sätt.

Tillåten behandling

Behandlingen måste, utöver att leva upp till de grundläggande kraven, dessutom vara tillåten. I 10 § PuL anges de fall när behandling av personuppgifter är tillåten. I normalfallet kan två grunder bli aktuella vid användandet av biometriska uppgifter i arbetslivet; antingen med stöd av en intresseavvägning eller om den anställde lämnat sitt samtycke till behandlingen.

En arbetsgivare får behandla biometriska uppgifter om det är nödvändigt för att ett berättigat intresse hos arbetsgivaren ska kunna tillgodoses, om det intresset väger tyngre än den registrerades intresse av skydd mot kränkning av den personliga integriteten. Vid en intresseavvägning väger åtgärder som betingas av säkerhetsskäl i allmänhet tyngre än åtgärder som betingas av till exempel företagsekonomiska effektivitetsskäl. En samlad bedömning av omständigheterna i varje enskilt fall måste dock göras.

Vid en intresseavvägning kan bland annat följande frågor vara nödvändiga att beakta: ändamålet med registreringen, vilken slags verksamhet som bedrivs, vilken typ av biometriska uppgifter som ska registreras och hur omfattande registreringen är, hur länge uppgifterna sparas, om det är möjligt att återskapa exempelvis ett fingeravtryck utifrån de uppgifter som registreras, om det finns risk för att uppgifterna på något sätt skulle kunna missbrukas eller användas för andra ändamål än det avsedda, om uppgifterna ska lagras lokalt eller centralt, vilka tekniska och organisatoriska åtgärder som omgärdar de uppgifter som behandlas samt att arbetsledningsrätten inte utövas på ett sätt som strider mot god sed. I samband med bedömning enligt den sista punkten kan eventuella ställningstaganden från fackföreningar vara relevanta. Vid en intresseavvägning bör även uppmärksammas att en fara i samband med biometrisk databehandling är att en ökad användning av biometriska uppgifter kan medföra att människor blir mindre uppmärksamma på hur behandlingen av dessa uppgifter kan påverka deras vardag.

För att ett samtycke skall vara giltigt krävs att det utgör en frivillig, särskild och otvetydig viljeyttring. Den anställde ska vidare ha fått tillräcklig information om behandlingen för att kunna ta ställning till ett eventuellt samtycke. Behandling av biometriska uppgifter i arbetslivet med stöd av samtycke begränsas till sådana situationer där den anställde har ett verkligt fritt val och senare kan ta tillbaka sitt samtycke utan att det medför några nackdelar för honom eller henne. Det innebär bland annat att den anställde måste erbjudas en alternativ metod till den biometriska behandlingen – exempelvis möjlighet att logga in genom användarnamn och lösenord istället – samt att han eller hon inte utsätts för någon direkt eller indirekt påtryckning till att välja det alternativ som innebär behandling av biometriska uppgifter. Innan en person blivit anställd är beroendeställningen till arbetsgivaren inte lika stor. Ett samtycke till behandling av biometriska uppgifter som lämnas vid anställningstillfället kan därför i normalfallet anses frivilligt.

6. Kameraövervakning

6.1. Enkät svar

Av de 103 arbetsgivarna uppgav 14 att de övervakade den anställde med hjälp av kameror. I åtta fall skedde inspelningen med digital teknik.

I dessa åtta fall uppgavs det i enkät svaren att kamerorna bevakade entréer, garage, stängsel, gods, parkeringsplatser, ytterområden och inpassering till datorhallar. De bevakningsområden som exemplifierades i enkät svaren var således områden som den anställde kan tänkas passera förbi, men inte typiskt sett utför sitt arbete på.

I samtliga fall utom ett lämnades någon form av information till den anställde. I fem av fallen hade den anställde lämnat sitt samtycke till övervakningen. I lika många fall fanns det någon form av facklig överenskommelse om kameraövervakning.

Kontroll skedde av säkerhetsmässiga och tekniska skäl samt för att motverka och utreda brott. Inte i något fall skedde kontroll för att övervaka den anställdes arbetsprestation.

Det rådde mycket stora olikheter i arbetsgivarnas gallringsrutiner. Gallring förekom såväl veckovis som årsvis. I vissa fall skedde en kontinuerlig överskrivning av tidigare inspelningar. Sådan överskrivning kan, beroende på med vilken intervall den sker, innebära långa gallringstider.

6.2. Inspektioner

Fem av de arbetsgivare som inspekterades uppgav i enkät svaren att den anställde övervakades på arbetsplatsen med hjälp av kameror. I samtliga fall utom ett skedde inspelningen med digital teknik. Inspektionerna bekräftade i huvudsak vad som uppgetts i enkät svaren, dock gjordes vissa förtydliganden angående syftet med övervakningen i ett par av fallen. Genom inspektionerna gavs även tydligare svar beträffande vilken information som lämnats till arbetstagarna. Inspektionerna bekräftade att det inte förkom någon kontroll av de anställdas arbetsprestationer med hjälp av kameraövervakning. En arbetsgivare uppgav dock att om det skulle uppkomma kassabrist som inte upphör kan bolaget, som sista utväg, besluta om dold kameraövervakning av kassorna. När ett sådant beslut fattas kommer bolaget att informera berörd personal om att kameraövervakning kommer att ske.

6.3. Datainspektionens synpunkter

Allmänt

Enligt lagen (1998:150) om allmän kameraövervakning krävs tillstånd till allmän kameraövervakning för att en övervakningskamera ska få vara uppsatt så att den kan riktas mot en plats dit allmänheten har tillträde. När det däremot gäller platser dit allmänheten inte har tillträde behövs inget tillstånd. De flesta av bestämmelserna i lagen om allmän kameraövervakning gäller bara övervakning av platser dit allmänheten har tillträde. Om det rör sig om övervakning av en plats dit allmänheten inte har tillträde genom en automatiserad behandling av personuppgifter, dvs. med digital teknik, är PuL:s regler tillämpliga.

Grundläggande krav

Enligt de grundläggande kraven i 9 § PuL ska personuppgifter alltid behandlas på ett korrekt sätt och i enlighet med god sed. Uppgifterna får bara samlas in för särskilda, uttryckligt angivna och berättigade ändamål och får inte behandlas för något ändamål som är oförenligt med det för vilket uppgifterna samlades in. Vidare får uppgifterna inte bevaras under en längre tid än vad som är nödvändigt med hänsyn till det ändamål som har bestämts. Eftersom gallringstiden måste bestämmas med hänsyn till ändamålet går det inte att fastslå någon allmänt giltig tid. Med hänsyn till de ändamål för övervakning som uppgavs i enkätsvaren kan dock sägas att daglig eller veckovis gallring i normalfallet bör vara ett riktmärke. Ett par arbetsgivare uppgav att uppgifterna endast gallrades årsvis eller på längre obestämda perioder genom överskrivning av tidigare inspelningar. Så långa gallringstider kan, mot bakgrund av de uppgivna ändamålen, normalt inte anses förenliga med PuL.

Tillåten behandling

Behandlingen måste även ha stöd i 10 § PuL för att vara tillåten. Huvudregeln är att personuppgifter bara får behandlas med samtycke från den enskilde. Arbetstagare befinner sig ofta i en beroendeställning till arbetsgivaren. Behandling av personuppgifter i arbetslivet med stöd av samtycke ska begränsas till sådana situationer där den anställde har ett verkligt fritt val och senare kan ta tillbaka sitt samtycke utan att det medför några nackdelar för honom eller henne. Ett samtycke ska dessutom vara uttryckligt. Det är inte tillräckligt att informera om en tilltänkt behandling och ge de berörda en viss frist att motsätta sig behandlingen. Om någon av de anställda, även om det bara är en enda person, motsätter sig behandlingen kan kameraövervakningen inte genomföras enbart med stöd av samtycke. Datainspektionen anser därför att det är tveksamt om kameraövervakning är möjlig att genomföra på större arbetsplatser med stöd av samtycke.

En arbetsgivare kan även utan samtycke få behandla personuppgifter efter en intresseavvägning om det är nödvändigt för att kunna tillgodose ett berättigat intresse och intresset av att behandla uppgifterna är större än den anställdes intresse av att uppgifterna inte behandlas. Utfallet av intresseavvägningen måste avgöras efter en helhetsbedömning i det enskilda fallet. Vid bedömningen kan man bland annat ta hänsyn till för vilket ändamål behandlingen ska utföras, vilken verksamhet som bedrivs, eventuella överenskommelser som finns i kollektivavtal och vilken information arbetstagarna har fått enligt PuL. Det har självfallet även mycket stor betydelse vilket område kameran bevakar.

Kameraövervakning av arbetet kan av många upplevas som särskilt obehaglig. För att sådan övervakning ska vara tillåten krävs därför mycket starka skäl. När ändamålet är de anställdas säkerhet krävs att det är fråga om en arbetsplats med hög riskfaktor för att kameraövervakningen ska vara tillåten. Exempelvis arbetsplatser som ofta utsätts för rån eller där riskfylld produktion pågår. Även i sådana fall kan dock de angivna ändamålen ofta tillgodoses på andra, mindre ingripande sätt, än genom kameraövervakning.

Information

I lagen om allmän kameraövervakning finns en bestämmelse om att upplysning om allmän kameraövervakning ska lämnas genom tydlig skyltning eller på något annat verksamt sätt. Enligt Datainspektionens mening sträcker sig PuL:s krav på information längre än kravet på upplysning om kameraövervakning i lagen om allmän kameraövervakning. Det räcker därför inte att endast sätta upp skyltar i de utrymmen där kameraövervakning bedrivs, vilket var fallet hos några av arbetsgivarna i denna studie. Arbetsgivaren måste dessutom på lämpligt sätt informera de anställda enligt 23-25 §§ PuL. Informations-skyldigheten innebär i detta fall bl.a. att upplysning om ändamålet med övervakningen och hur länge uppgifterna bevaras måste lämnas. Sådan information kan exempelvis lämnas i samband med nyanställning eller när kamerorna sätts upp. Informationen bör även finnas i personalpärmen och/eller på intranätet.

7. Jämförelser med erfarenheter från det tidigare projektet

Vid Datainspektionens granskning 2002 undersöktes inte användningen av biometriska uppgifter och kameraövervakning. Några jämförelser i dessa delar är därför inte möjliga att göra. De jämförelser som görs nedan avser därför enbart Internet- och e-postanvändning.

I det föregående projektet uppgav ca hälften av arbetsgivarna att det förekom någon form av kontroller av de anställdas Internet och e-postanvändning.

Av svaren i den nya enkätundersökningen att döma förekom det någon form av kontroll av anställdas Internetanvändning hos drygt 40 procent av arbetsgivarna och kontroll av e-postanvändning hos ca 15 procent av arbetsgivarna. Vid en jämförelse med svaren i det tidigare projektet finns det ingenting som tyder på att arbetsgivarnas övervakning av de anställdas Internet- och e-postanvändning skulle ha ökat.

Liksom tidigare skedde kontrollen ofta av säkerhetsmässiga och tekniska skäl och, på förekommen anledning, för att utreda misstanke om brott. Att motverka surfning på oetiska webbplatser angavs numera betydligt oftare som kontrolländamål. I den tidigare undersökningen uppgav inte någon arbetsgivare att de kontrollerade Internetanvändningen för att övervaka vad den anställda gjorde på sin arbetstid. Detta ändamål angavs nu i två av fallen.

Kontrollen skedde liksom tidigare i första hand genom kontroll av loggfiler. Loggen kunde i de flesta fall knytas till enskild individ genom IP-adress/användar-ID. Det var ovanligt att information i cookies användes för att följa upp surfande.

Undersökningen utvisade att arbetsgivarna fortfarande inte använde någon särskild programvara för att kontrollera de anställdas e-post- och Internetanvändning, annat än s.k. standardverktyg för logganalys samt antivirusprogram.

Arbetsgivarnas riktlinjer

De flesta arbetsgivare som utförde kontroller hade utarbetat riktlinjer för de anställdas Internet- och e-postanvändning. Av enkätsvaren framgick att nästan hälften av de arbetsgivare som utförde någon form av kontroll av arbetstagarnas Internetanvändning saknade riktlinjer för hur denna kontroll skulle ske. I e-postfallet saknades sådana regler i 20 procent av fallen.

När det uppstod misstanke om missbruk vid Internet- och e-postanvändning togs problemet i första hand med ansvarig chef. Det ankom sedan på denna chef att kontakta den enskilde anställde för att komma till rätta med problemet.

Detta överensstämmer i stort med de iakttagelser som Datainspektionen gjorde i den tidigare undersökningen.

Samtycke

Vid Datainspektionens tidigare undersökning konstaterades att arbetsgivarna mycket sällan inhämtade den anställdes samtycke till de kontroller som utfördes. Av enkätsvaren i den nya undersökningen framgick att inhämtande av samtycke blivit vanligare, även om det fortfarande bara skedde i en minoritet av fallen. Vid övervakning av Internetanvändningen skedde kontrollen med den anställdes samtycke i 15 av 44 fall. I 16 av fallen omfattades kontrollerna av någon form av facklig överenskommelse.

Utfallet av enkäten blev i princip detsamma i e-postfallet. I sex av 15 fall inhämtades den anställdes samtycke. Här omfattades dock kontrollerna i hälften av fallen av någon form av facklig överenskommelse.

Samtycke kunde liksom tidigare inhämtas på flera olika sätt. Ofta inhämtades samtycket vid anställningen, genom underskrifter av regler eller vid ansökan om tillgång till Internet.

Information

I den förra undersökningen kunde Datainspektionen konstatera att de allra flesta arbetsgivare hade dokumenterade regler för Internet- och e-postanvändning och i de flesta fall fanns information om reglerna utlagd på arbetsgivarens intranät. Detta förhållande bekräftades av den nya enkätundersökningen.

Av enkätsvaren framgick även att det fortfarande var vanligt att de arbetsgivare som kontrollerade de anställdas Internetanvändning saknade dokumenterade regler för hur själva kontrollen skulle gå till. Var fjärde arbetsgivare som utförde kontroller lämnade dessutom inte någon information om kontrollen till de anställda.

Gallring

Undersökningen som gjordes 2002 visade att mer än hälften av arbetsgivarna saknade regler för gallring av de uppgifter som ligger till grund för kontrollen av den anställdes Internet- och e-postanvändning. Enkätsvaren och erfarenheter från inspektionerna i den nya undersökningen visade att det fortfarande

var vanligt att arbetsgivare inte utarbetat några gallringsrutiner med beaktande av bestämmelserna i PuL.

Sammanfattning

De iakttagelser som gjorts i detta projekt stämmer i huvudsak överens med de iakttagelser som gjordes i det tidigare projektet. Några förändringar har dock noterats. Det har exempelvis blivit vanligare att arbetsgivare kontrollerar den anställdes Internetanvändning för att motverka surfning på oetiska webbplatser.

Checklista

Arbetsgivaren bör ha riktlinjer för användning av Internet och e-post. Hur pass omfattande och detaljerade dessa riktlinjer bör vara beror i viss mån på den verksamhet som arbetsgivaren bedriver. En arbetsgivare med tusentals anställda kanske har större behov av detaljerade regler än ett småföretag där alla känner alla. En myndighet måste ta med i beräkningen att personuppgifterna kan omfattas av offentlighetsprincipen. En arbetsgivare kan således anse sig ha behov av fler regler än de som framgår av Datainspektionens exempel nedan. Datainspektionen har i denna checklista i korta ordalag tagit upp de regler som är så pass viktiga att de alltid bör ingå i arbetsgivarens riktlinjer för användning av Internet och e-post. Varje punkt följs av ett exempel och en kommentar där Datainspektionen klargör vad en arbetsgivare bör tänka på när de egna riktlinjerna utformas.

Exempel

Tillåten användning av Internet och e-post

Det bör klart framgå av arbetsgivarens regler i vilken omfattning den anställda har rätt att använda Internet och e-post för privat bruk.

Exempel: Internet är ett arbetsverktyg och får för privat bruk användas bara i sådan omfattning att det inte inkräktar på arbetet eller medför onödiga kostnader för arbetsgivaren.

Kommentar: Det har inom ramen för detta projekt framgått att de flesta arbetsgivare tillåter att de anställda surfar på harmlösa webbplatser för privata ändamål exempelvis på lunch- och kafferaster. De anställda får i princip alltid skicka enkla e-postmeddelanden för privat bruk så länge detta inte inkräktar på arbetet. Det bör i detta sammanhang framhållas att arbetsgivarens riktlinjer måste vara allvarligt menade. Arbetsgivaren ska inte i sitt regelverk förbjuda all privat Internet- och e-postanvändning samtidigt som den anställda i praktiken ges sådan rätt.

Begränsningar av Internet- och e-postanvändande

Om en arbetsgivare vill begränsa den anställdes möjligheter att utnyttja Internet och e-post bör detta klart framgå av riktlinjer och information.

Exempel: Det är inte tillåtet att för privata syften besöka webbplatser med extrempolitiskt eller pornografiskt innehåll. Det är heller inte tillåtet att delta i chat-sidor eller ladda ner filer från Internet.

Det är inte tillåtet att skicka kedjebrev. För anmälan till mejlinglistor gäller att anmälan endast får ske till listor där informationen behövs i tjänsten.

Kommentar: Begränsningarna ska i möjligaste mån uttryckas klart och tydligt. Det räcker inte att hänvisa till ”underförstådda etiska regler” eller förbjuda tillgång till ”information som kan uppfattas som olämplig ur moralisk synvinkel” etc. Begränsningarna kan gälla vilka webbplatser som får besökas eller vilken information den anställda får sprida på egen hand. Det är heller inte ovanligt med begränsningar av säkerhetsskäl för att undvika exempelvis virusangrepp eller onödig belastning av nätet.

Av de regler Datainspektionen tagit del av framgår att många arbetsgivare vill hindra besök på webbplatser som ger uttryck för extrempolitiska åsikter, såsom rasism eller terrorism, eller innehåller pornografiskt material. Begränsningarna kan även gälla nedladdning av musik eller rörliga bilder, handla/betala på Internet, hämta e-post från privat brevlåda, delta i chat-sidor osv. Hur pass omfattande dessa begränsningar bör vara är en fråga som bör avgöras på den enskilda arbetsplatsen.

Kontroll av Internet- och e-postanvändning

Om arbetsgivaren utövar någon form av kontroll över de anställdas Internet- och e-postanvändning bör detta klart framgå av regler och information. Det bör även framgå hur kontrollen går till.

Exempel: All användning av Internet registreras i en logg. Loggningen omfattar uppgifter om användarnamn och namnet på den webbplats som besökts.

Det förs även en logg över all e-post som innefattar uppgifter om avsändare, mottagare, ärendemening, tidpunkt och storlek på meddelandet samt namnet på bifogade filer.

Med hjälp av loggen tar IT-avdelningen en gång i månaden fram en lista som visar hur många timmar som personalen surfat på Internet totalt. Vid denna månatliga kontroll sker ingen kontroll av enskilda individers surfning. De åtkomna webbplatserna är indelade i olika kategorier såsom sport, nyheter, pornografi osv.

Om det av kontrollistan framgår att det förekommer surfning på webbplatser som enligt riktlinjerna inte får besökas, eller om surfning förekommer

i onormalt stor omfattning på vissa tillåtna kategorier webbplatser kan personalchef besluta om kontroll av enskilda individers surfning.

Arbetsgivaren utövar ingen kontroll över de anställdas e-postmeddelanden. Arbetsgivaren kan dock i enskilda fall komma att kontrollera e-postmeddelanden om det är nödvändigt vid fara för informationssäkerhet, t.ex. vid virusangrepp, eller för att utreda misstanke om brott. Beslut om kontroll fattas av IT-säkerhetsansvarig.

Kommentar: Kontroll av Internet kan ske regelbundet (såsom i exemplet), genom stickprov eller på förekommen anledning. Om kontroll sker på förekommen anledning, eller om en generell övervakning under vissa omständigheter övergår till kontroll av en enskild individ, är det viktigt att det klart framgår vad det är som föranleder arbetsgivaren att inleda kontrollen av den anställde. Kontroll kan inledas om loggen indikerar exempelvis att det förekommit onormalt hög andel icke arbetsrelaterad surfning eller surfning på vissa otillåtna webbplatser. Det ska även framgå vem eller vilka som beslutar om att kontroll ska ske, exempelvis personalchefen (såsom i exemplet) eller IT-chefen eller en viss grupp befattningshavare.

Kontroll av innehållet i privata e-postmeddelanden

Om arbetsgivaren kan komma att gå igenom innehållet i den anställdes privata e-post bör detta klart framgå av regler och information.

Exempel: Arbetsgivaren kan komma att ta del av de uppgifter som finns i ett e-postmeddelande om det är nödvändigt för att uppfylla myndighetens skyldigheter om allmänna handlingars offentlighet.

Arbetsgivaren kan även komma att ta del av de uppgifter som finns i ett e-postmeddelande om det är nödvändigt vid fara för informationssäkerhet, t.ex. vid virus- och hackerangrepp, eller för att utreda och förhindra brott.

Kommentar: Det är ovanligt att arbetsgivare kontrollerar innehållet i de anställdas e-postmeddelanden. Det förekommer dock i samband med brottsutredningar eller av säkerhetsskäl. Detta ska då framgå av informationen. Det kan även vara lämpligt att ange vad som händer med den anställdes e-postmeddelanden vid en uppsägning eller efter en längre tids sjukdom.

Överträdelse av reglerna

Det bör av riktlinjerna framgå vilka åtgärder som arbetsgivaren kommer att vidta om den anställde bryter mot Internet-policyn.

Exempel: Om det av kontrollerna framgår att riktlinjerna överträtts kan ärendet komma att utredas av personalchef. Arbetsgivaren kommer att i första

hand försöka åstadkomma rättelse genom påpekanden eller liknande förfaranden. Vid allvarigare missbruk kan disciplinära åtgärder komma att vidtas.

Kommentar: Det bör av riktlinjerna framgå vem eller vilka som ska genomföra en eventuell utredning. Det bör även framgå vilka åtgärder som arbetsgivaren kan komma att vidta mot den anställde vid en överträdelse av riktlinjerna.

Bevarande och gallring

Det bör av riktlinjerna framgå hur länge arbetsgivaren bevarar de uppgifter som ligger till grund för kontrollen av den anställdes Internet- och e-postanvändning.

Exempel: Uppgifterna som ligger till grund för kontrollen av den anställdes Internet- och e-postanvändning gallras efter tre månader. Om en utredning påbörjas kommer uppgifterna att bevaras så länge utredningen pågår.

Kommentar: En arbetsgivare är skyldig att se till att personuppgifter inte bevaras under längre tid än som är nödvändigt med hänsyn till ändamålet med behandlingen. I det aktuella exemplet tar arbetsgivaren fram en lista med statistik över de anställdas Internetsurfning en gång i månaden. Denna lista ska sedan gås igenom av IT-avdelningen och vid misstanke om otillåtet surfande överlämnas till personalchef för vidare åtgärder. Om kontrollen sker på detta sätt torde det inte vara nödvändigt att bevara uppgifterna längre än högst tre månader. För det fall en utredning av den enskildes surfande faktiskt påbörjas kan det vara nödvändigt att bevara uppgifterna så länge utredningen pågår, även om utredningen tar längre tid än tre månader.

För det fall arbetsgivaren övervakar de anställdas e-postanvändning bör en liknande gallringsregel finnas beträffande gallring av de uppgifter som ligger till grund för kontrollen av e-postanvändningen.

Bilaga 1 – Tillsynsobjekt (enkätinspektioner)

Akzo Nobel Industrial Coatings AB

Apoteket Aktiebolag

Arbets- och socialnämnden i Landskrona kommun

AstraZeneca AB

Atlas Copco Aktiebolag

Barn- och utbildningsutskottet i Aneby kommun

Bollnäsbestäder

Boverket

Chalmers Tekniska Högskola

Direktmedia Bonnier DM AB

Egmont AB

Familjebostäder i Göteborg AB

Ferruform AB

Fiskeriverket

Försvarets Materielverk

Glesbygdsverket

Gothia Financial Group AB

Gävle Energi AB, Gävle

Göteborgs universitet

Härnösand Energi & Miljö AB

Högskolan i Gävle

Jordbruksverket

Kalix Tele24 AB

Karolinska Institutet

Kirunabostäder AB

Kommunstyrelsen i Aneby kommun

Kommunstyrelsen i Borgholms kommun

Kommunstyrelsen i Borås stad

Kommunstyrelsen i Jönköpings kommun

Kommunstyrelsen i Halmstads kommun

Kommunstyrelsen i Kalmars kommun

Kommunstyrelsen i Karlskrona kommun

Kommunstyrelsen i Landskrona kommun

Kommunstyrelsen i Linköpings kommun

Kommunstyrelsen i Lunds kommun

Kommunstyrelsen i Nacka kommun

Kommunstyrelsen i Stockholms kommun

Kommunstyrelsen i Uppsala kommun

Kommunstyrelsen i Vaxholms kommun

Kommunstyrelsen i Växjö kommun

Kommunstyrelsen i Åmåls kommun

Kommunstyrelsen, Östersunds kommun

Korsnäs AB

KPMG Bohlins Aktiebolag

Krambo Bostads AB

Kriminalvårdsstyrelsen

Kultur- och fritidsnämnden, Gävle kommun

Kungliga Tekniska Högskolan

Landstinget Blekinge

Landstinget Sörmland

Lernia Aktiebolag

Lindebergs Grant Thornton AB

LKAB

Lulebo AB

Luleå Energi AB

Luleå Industrimontage AB

Luleå tekniska universitet

Läkemedelsverket

Länsförsäkringar Västernorrland

Länsstyrelsen i Stockholms län

Länsstyrelsen i Södermanlands län

Länsstyrelsen i Uppsala län

Malmö Högskola

Manpower Solutions AB

Migrationsverket

Mittuniversitetet

Mölnlycke Health Care AB

NCC Construction Sverige AB

Norrlands miljövård AB

Patent och registreringsverket

Polismyndigheten i Gävleborgs län

Polismyndigheten i Norrbotten
Polismyndigheten i Västerbottens län
Radiotjänst i Kiruna AB
Schenker AB
Skandiabanken AB
AB SKF
Skogsvårdsstyrelsen Norrbotten
Skärholmens stadsdelsnämnd
Socialnämnden i Borgholms kommun
Socialnämnden i Halmstads kommun
Socialnämnden i Jönköpings kommun
Socialnämnden i Karlskrona kommun
Socialnämnden i Kalmars kommun
Socialnämnden i Linköpings kommun
Socialnämnden i Lunds kommun
Socialnämnden i Nacka kommun
Socialnämnden i Vaxholms kommun
Socialnämnden i Växjö kommun
Socialnämnden, Östersunds kommun
Statistiska Centralbyrån
Sveaskog AB
Svenska kommunalarbetsförbundet
Svenska Rymd AB
Sydkraft AB

Tekniska nämnden, Gävle kommun

Umeå universitet

Unisys Aktiebolag

Uppsala kommun, Produktionsnämnden för teknik och service

Vattenfall Aktiebolag

Vattenfall Service Nord AB

Volvo Business Services AB

Örebro läns landsting

Regler för Internetanvändning

1. a) Finns det regler för den anställdes Internetanvändning?

1 Ja

Om ja:

2 Nej

→ Gå till fråga 4

b) Finns reglerna dokumenterade?

1 Ja

→ Bifoga reglerna med denna enkät!

2 Nej

2. Får den anställda information om reglerna?
Flera svar kan markeras.

1 Skriftlig information

→ Bifoga informationen

1 Muntlig information

1 Finns på det interna nätet

2 Ingen information lämnas

3. Får den anställda i viss omfattning använda Internet för privat bruk?

1 Ja

2 Nej, all privat användning är förbjuden

Kontroll av Internetanvändning

4. a) Sker det någon kontroll av den anställdes Internetanvändning?

1 Ja

2 Nej

→ Gå till fråga 13

T.ex. genom uppföljning av loggar.

Om ja:

b) Finns det regler/riktlinjer för hur kontrollen av den anställdes Internetanvändning ska ske?

1 Ja

→ Bifoga reglerna med denna enkät!

2 Nej

5. I vilket syfte görs dessa kontroller?

Flera svar kan markeras.

1 Kontroll av vad den anställda gör på sin arbetstid

1 Motverka surfning på "oetiska" webbplatser

1 Kunna utreda misstanke om brott

1 Övervakning av tekniska skäl

1 Säkerhetsmässiga skäl

1 Annat, nämligen

2 Dokumenterat syfte saknas

6. a) I vilken omfattning genomförs kontrollerna?

1 I princip all Internetanvändning

2 Stickprovskontroller

3 Annat, nämligen

Om stickprovskontroll:

b) Hur ofta?

1 Varje vecka

2 Minst varje månad

3 Mera sällan

<p>7. a) Används genomgång av loggfiler som kontroll?</p> <p>Om ja:</p> <p>b) Kan loggen knytas till enskild individ genom IP-nummer/användar-ID?</p> <p>Om nej:</p> <p>c) Vad kan loggen knytas till?</p> <p>d) Vad är det som loggas?</p> <p>e) Används information i cookies för att följa upp den anställdes surfande?</p> <p>f) Sker kontroll genom annan metod?</p>	<p>1 <input type="checkbox"/> Ja 2 <input type="checkbox"/> Nej → Gå till fråga 7e)</p> <p>1 <input type="checkbox"/> Ja → Gå till fråga 7 d) 2 <input type="checkbox"/> Nej</p> <p>.....</p> <p>1 <input type="checkbox"/> IP-nummer/användar-ID 1 <input type="checkbox"/> Destinationsadress (www-adressen) 1 <input type="checkbox"/> Tidpunkt 1 <input type="checkbox"/> Annat, nämligen</p> <p>.....</p> <p>1 <input type="checkbox"/> Ja 2 <input type="checkbox"/> Nej</p> <p>1 <input type="checkbox"/> Ja → Vilken? 2 <input type="checkbox"/> Nej</p>
<p>8. a) Får den anställde information om den kontroll som sker?</p> <p>Om ja:</p> <p>b) Anges syftet med kontrollen i informationen?</p>	<p>1 <input type="checkbox"/> Ja, skriftligt → Bifoga informationen 1 <input type="checkbox"/> Ja, muntlig 1 <input type="checkbox"/> Nej</p> <p>1 <input type="checkbox"/> Ja 2 <input type="checkbox"/> Nej</p>
<p>9. a) Har den anställde lämnat samtycke till kontrollen?</p> <p>Om ja:</p> <p>b) På vilket sätt inhämtas samtycke?</p>	<p>1 <input type="checkbox"/> Ja, till all kontroll som kan ske 2 <input type="checkbox"/> Ja, till viss kontroll 3 <input type="checkbox"/> Nej 4 <input type="checkbox"/> Annat, nämligen</p> <p>.....</p> <p>.....</p>
<p>10. Finns det någon facklig överenskommelse om kontroll av den anställdes Internet-användning?</p>	<p>1 <input type="checkbox"/> Ja 2 <input type="checkbox"/> Nej</p>
<p>11. Hur ofta gallras de uppgifter som ligger till grund för kontrollen av den anställdes Internetanvändning?</p>	<p>1 <input type="checkbox"/> Aldrig 2 <input type="checkbox"/> Veckovis 3 <input type="checkbox"/> Månadsvis 4 <input type="checkbox"/> Årsvis 5 <input type="checkbox"/> Annat dvs.</p>
<p>12. På vilket sätt sker gallringen?</p>	<p>1 <input type="checkbox"/> Automatiskt 2 <input type="checkbox"/> Manuellt 3 <input type="checkbox"/> Både automatiskt och manuellt</p>

Regler för privat e-postanvändning

13. a) Finns det regler för den anställdes e-postanvändning?

1 Ja

2 Nej

→ Gå till fråga 16

Om ja:

b) Finns reglerna dokumenterade?

1 Ja

→ Bifoga reglerna med denna enkät!

2 Nej

14. Får den anställda information om reglerna?

Flera svar kan markeras.

1 Skriftlig information

→ Bifoga informationen

1 Muntlig information

1 Finns på det interna nätet

2 Ingen information lämnas

15. a) Får den anställda i viss omfattning använda e-post för privat bruk?

1 Ja

2 Nej, all privat användning är förbjuden

Om ja:

b) Ska den anställda hålla privata e-postmeddelanden åtskilda från de som har anknytning till arbetet?

1 Ja

2 Nej

Kontroll av privat e-postanvändning

16. a) Sker det någon kontroll av den anställdes privata e-postanvändning?

1 Ja

2 Nej

→ Gå till fråga 25

Om ja:

b) Finns det regler/riktlinjer för hur kontrollen av den anställdes privata e-postanvändning ska ske?

1 Ja

→ Bifoga reglerna med denna enkät!

2 Nej

17. I vilket syfte görs dessa kontroller?

Flera svar kan markeras.

1 Kontroll av vad den anställda gör på sin arbetstid

1 Kunna utreda misstanke om brott

1 Övervakning av tekniska skäl

1 Säkerhetsmässiga skäl

1 Annat, nämligen

.....

2 Dokumenterat syfte saknas

<p>18. I vilken omfattning genomförs kontrollerna?</p> <p><i>Om stickprovskontroll</i></p> <p>Hur ofta?</p>	<p>1 <input type="checkbox"/> I princip all e-postanvändning</p> <p>2 <input type="checkbox"/> Stickprovskontroller</p> <p>3 <input type="checkbox"/> Annat, nämligen</p> <p>.....</p> <p>1 <input type="checkbox"/> Varje vecka</p> <p>2 <input type="checkbox"/> Minst varje månad</p> <p>3 <input type="checkbox"/> Mera sällan</p>
<p>19. Vilka kontrollmetoder tillämpas?</p> <p><i>Flera svar kan markeras</i></p>	<p>1 <input type="checkbox"/> Genomgång av loggfiler</p> <p>1 <input type="checkbox"/> Nyckelordssökning</p> <p>1 <input type="checkbox"/> Genomgång av enskilda e-postmeddelanden</p> <p>1 <input type="checkbox"/> Annat, nämligen</p>
<p>20. a) Får den anställda information om den kontroll som sker?</p> <p><i>Om ja:</i></p> <p>b) Anges syftet med kontrollen i informationen?</p>	<p>1 <input type="checkbox"/> Ja, skriftligt → <i>Bifoga informationen</i></p> <p>1 <input type="checkbox"/> Ja, muntligt</p> <p>1 <input type="checkbox"/> Nej</p> <p>1 <input type="checkbox"/> Ja</p> <p>2 <input type="checkbox"/> Nej</p>
<p>21. Har den anställda lämnat samtycke till kontrollen?</p> <p><i>Om ja:</i></p> <p>b) På vilket sätt inhämtas samtycke?</p>	<p>1 <input type="checkbox"/> Ja, till all kontroll som kan ske</p> <p>2 <input type="checkbox"/> Ja, till viss kontroll</p> <p>3 <input type="checkbox"/> Nej</p> <p>4 <input type="checkbox"/> Annat, nämligen</p> <p>.....</p> <p>.....</p>
<p>22. Finns det någon facklig överenskommelse om kontroll av den anställdes privata e-postanvändning?</p>	<p>1 <input type="checkbox"/> Ja</p> <p>2 <input type="checkbox"/> Nej</p>
<p>23. Hur ofta gallras de uppgifter som ligger till grund för kontrollen av den anställdes privata e-postanvändning?</p>	<p>1 <input type="checkbox"/> Aldrig</p> <p>2 <input type="checkbox"/> Veckovis</p> <p>3 <input type="checkbox"/> Månadsvis</p> <p>4 <input type="checkbox"/> Årsvis</p> <p>5 <input type="checkbox"/> Annat dvs.</p>
<p>24. På vilket sätt sker gallringen?</p>	<p>1 <input type="checkbox"/> Automatiskt</p> <p>2 <input type="checkbox"/> Manuellt</p> <p>3 <input type="checkbox"/> Både automatiskt och manuellt</p>

Biometriska personuppgifter

25. a) Registreras biometriska uppgifter om den anställda? 1 Ja
2 Nej → Gå till fråga 33
- Om ja:
b) Vilka biometriska uppgifter samlas in? 1 Fingeravtryck
1 Fingergeometri
1 Irisigenkänning
1 Analys av näthinnan
1 Ansiktsigenkänning
1 Handgeometri
1 Annat dvs.
26. För vilka ändamål samlas uppgifterna in? 1 Identifiering vid in- och utpassering i säkerhets- och behörighetssyfte
2 Identifiering vid in- och utpassering i tidredovisningssyfte
3 Annat dvs.
27. På vilket sätt får den anställda information om den biometriska personuppgiftsbehandlingen? 1 Skriftlig information → *Bifoga informationen*
1 Muntlig information
1 Finns på det interna nätet
2 Ingen information lämnas
Flera svar kan markeras.
28. Har den anställda lämnat samtycke till den biometriska personuppgiftsbehandlingen?
1 Ja
2 Nej
Om ja:
På vilket sätt inhämtas samtycke?
29. Erbjuds den anställda något alternativ till biometrisk registrering om denne motsätter sig personuppgiftsbehandlingen? 1 Ja, dvs
2 Nej
30. Finns det någon facklig överenskommelse om insamling av den anställdes biometriska uppgifter? 1 Ja
2 Nej
31. Hur ofta gallras de biometriska uppgifterna? 1 Aldrig
2 Veckovis
3 Månadsvis
4 Årsvis
5 Annat dvs.

<p>32. Finns det för närvarande några planer på att utveckla redan befintliga rutiner?</p>	<p>1 <input type="checkbox"/> Ja 2 <input type="checkbox"/> Nej</p>	<p>→ Gå till fråga 34 → Gå till fråga 35</p>
<p>33. Finns det för närvarande några planer på att i framtiden påbörja hantering av biometriska personuppgifter?</p>	<p>1 <input type="checkbox"/> Ja 2 <input type="checkbox"/> Nej</p>	<p>→ Gå till fråga 35</p>
<p>34. Om ja: Redogör kort för den planerade hanteringen av biometriska personuppgifter:</p> <p>.....</p> <p>.....</p> <p>.....</p> <p>.....</p>		
<p align="center">Kameraövervakning på arbetsplats dit allmänheten inte har tillträde</p>		
<p>35. a) Övervakas den anställda på arbetsplatsen med hjälp av kameror? <i>Gäller på arbetsplats dit allmänheten inte har tillträde.</i></p> <p><i>Om ja:</i></p> <p>b) Sker inspelningen med digital teknik?</p>	<p>1 <input type="checkbox"/> Ja 2 <input type="checkbox"/> Nej</p> <p>1 <input type="checkbox"/> Ja 2 <input type="checkbox"/> Nej</p>	<p>→ Gå till fråga 41 → Gå till fråga 41</p>
<p>36. Vad är syftet med denna övervakning?</p>	<p>1 <input type="checkbox"/> Att underlätta brottsutredningar 2 <input type="checkbox"/> Övervakning av tekniska funktioner och av säkerhetsmässiga skäl 3 <input type="checkbox"/> Att kontrollera den anställdes arbetsprestation 4 <input type="checkbox"/> Annat syfte.</p> <p>.....</p> <p>.....</p>	
<p>37. Får den anställda information om kameraövervakningen? <i>Flera svar får markeras.</i></p>	<p>1 <input type="checkbox"/> Skriftlig information → <i>Bifoga informationen</i> 1 <input type="checkbox"/> Muntlig information 1 <input type="checkbox"/> Finns på det interna nätet 2 <input type="checkbox"/> Ingen information lämnas</p>	
<p>38. Har den anställda lämnat samtycke till kameraövervakningen?</p> <p>1 <input type="checkbox"/> Ja 2 <input type="checkbox"/> Nej</p> <p><i>Om ja:</i> På vilket sätt inhämtas samtycke?</p> <p>.....</p>		

39. Finns det någon facklig överenskommelse om kameraövervakning?

Gäller på arbetsplats dit allmänheten inte har tillträde?

1 Ja

2 Nej

40. Hur ofta gallras uppgifterna som samlas in genom kameraövervakning?

1 Aldrig

2 Veckovis

3 Månadsvis

4 Årsvis

5 Annat dvs.

Övrigt

41. Har du andra synpunkter att framföra till Datainspektionen?

.....

.....

.....

.....

.....

Företag:

Antal anställda:

Kontaktperson:

Telefonnummer:

E-post:

Bilaga 3 – Tillsynsobjekt (fältinspektionen)

Apoteket Aktiebolag

AstraZeneca AB

Försvarets Materielverk

Göteborgs universitet

Kommunstyrelsen i Borås stad

Kommunstyrelsen i Stockholms kommun

Kommunstyrelsen i Vaxholms kommun

Korsnäs AB

Kungliga Tekniska Högskolan

Manpower Solutions AB

NCC Construction Sverige AB

Skandiabanken AB

AB SKF

Skärholmens stadsdelsnämnd

Vattenfall Aktiebolag