ARTIKEL 29-GRUPPEN VEDRØRENDE DATABESKYTTELSE

17/DA

WP 249

Udtalelse 2/2017 om databehandling på arbejdspladsen

Vedtaget den 8. juni 2017

Indholdsfortegnelse

1 Resumé

Denne udtalelse supplerer Artikel 29-gruppens ("WP29") tidligere publikationer, *Udtalelse 8/2001 om behandling af personoplysninger i ansættelsesforhold* (WP48)[1] og *Arbejdsdokument om overvågning af elektronisk kommunikation på arbejdspladsen* fra 2002 (WP55)[2]. Der er siden disse dokumenters offentliggørelse kommet en række nye teknologier til, som muliggør en mere systematisk behandling af de ansattes personoplysninger på arbejdspladsen, hvilket har skabt betydelige udfordringer med hensyn til beskyttelse af privatlivets fred og databeskyttelse.

I denne udtalelse foretages en fornyet vurdering af balancen mellem arbejdsgivernes legitime interesser og de ansattes berettigede forventninger om beskyttelse af privatlivets fred, idet de risici, der er forbundet med de nye teknologier, beskrives, og der foretages en proportionalitetsvurdering af en række scenarier, inden for hvilke disse teknologier kan anvendes.

Udtalelsen tager primært udgangspunkt i databeskyttelsesdirektivet, men ser også på de yderligere forpligtelser, som arbejdsgiverne pålægges ifølge den generelle forordning om databeskyttelse. Den gengiver endvidere holdningen og konklusionerne i udtalelse 8/2001 og WP55-arbejdsdokumentet, nemlig at ved behandling af de ansattes personoplysninger:

- skal arbejdsgiverne altid overholde de grundlæggende databeskyttelsesprincipper, uanset hvilken teknologi der anvendes
- er indholdet i elektronisk kommunikation, der udgår fra arbejdspladsen, omfattet af den samme beskyttelse af de grundlæggende rettigheder som indholdet i analog kommunikation
- er det højst usandsynligt, at samtykke kan anvendes som retsgrundlag for databehandling på arbejdspladsen, medmindre de ansatte kan afvise at give deres samtykke uden at lide skade
- kan opfyldelse af en kontrakt og legitime interesser nogle gange gøres gældende, under forudsætning af at behandlingen er strengt nødvendig for et legitimt formål og sker i overensstemmelse med proportionalitets- og nærhedsprincippet
- skal de ansatte underrettes effektivt om den overvågning, der finder sted
- skal det sikres, at alle internationale overførsler af oplysninger om ansatte er omfattet af et passende beskyttelsesniveau.

2. Indledning

Den hastige indførelse af nye informationsteknologier på arbejdspladsen med hensyn til infrastruktur, applikationer og intelligente enheder åbner op for nye former for systematisk og potentielt indgribende databehandling på arbejdspladsen. Et par eksempler:

---

[1] WP29, *Udtalelse 8/2001 om behandling af personoplysninger i ansættelsesforhold*, WP48, 13. september 2001, url: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2001/wp48_en.pdf.

[2] WP29, *Arbejdsdokument om overvågning af elektronisk kommunikation på arbejdspladsen*, WP55, 29. maj 2002, url: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2002/wp55_da.pdf.

- Teknologierne til databehandling på arbejdspladsen kan nu implementeres for en brøkdel af det, det kostede for nogle år siden, og disse teknologiers kapacitet til behandling af personoplysninger er steget eksponentielt.
- De nye former for databehandling, f.eks. af personoplysninger i forbindelse med anvendelsen af online tjenester og/eller lokaliseringsdata fra intelligente enheder, er langt mindre synlige for de ansatte end andre mere traditionelle metoder som f.eks. tv-overvågningskameraer. Dette rejser spørgsmålet om, i hvilket omfang de ansatte er bevidst om disse teknologier, eftersom arbejdsgiverne kan implementere databehandlingen ulovligt uden først at underrette de ansatte derom.
- Grænserne mellem hjem og arbejde er blevet mere og mere flydende. Når de ansatte fjernarbejder (f.eks. hjemmefra), eller når de er ude at rejse i forretningsøjemed, kan deres aktiviteter uden for det fysiske arbejdsmiljø overvåges, hvilket potentielt kan medføre overvågning af deres privatliv.

Derfor kan anvendelsen af sådanne teknologier være en hjælp til at detektere eller forhindre tab af virksomhedens intellektuelle og materielle ejendom, forbedre de ansattes produktivitet og beskytte de personoplysninger, som den registeransvarlige har ansvaret for, men den skaber også store udfordringer i forbindelse med beskyttelse af privatlivets fred og databeskyttelse. Der er derfor brug for en fornyet vurdering af balancen mellem arbejdsgiverens legitime interesse i at beskytte sin virksomhed og de berettigede forventninger om beskyttelse af privatlivets fred, som de registrerede, altså de ansatte, har.

I udtalelsen fokuseres der på de nye informationsteknologier ud fra ni forskellige scenarier, inden for hvilke disse teknologier kan finde anvendelse, og der ses også kort på mere traditionelle metoder til databehandling på arbejdspladsen, hvor risiciene er blevet skærpet som følge af den teknologiske udvikling.

Når ordet "ansat" anvendes i denne udtalelse, ønsker WP29 ikke at indskrænke betydningen af termen til personer med en ansættelseskontrakt, der er anerkendt som sådan i henhold til gældende arbejdslovgivning. Gennem de seneste årtier er der kommet nye forretningsmodeller til i kraft af de nye former for arbejdsforhold, navnlig beskæftigelse på freelancebasis. Denne udtalelse skal dække over alle situationer, hvor der består et ansættelsesforhold, uanset om dette forhold er baseret på en ansættelseskontrakt eller ej.

Det er vigtigt at bemærke, at de ansatte sjældent er i stand til frit at give, afvise at give eller trække et samtykke tilbage som følge af det afhængighedsforhold, der består mellem arbejdsgiver og arbejdstager. Undtagen i helt særlige tilfælde skal arbejdsgiverne gøre et andet retsgrundlag end samtykke gældende – f.eks. nødvendigheden af at behandle oplysningerne for at forfølge en legitim interesse. Dog er en legitim interesse i sig selv ikke tilstrækkelig til at tilsidesætte de ansattes rettigheder og frihedsrettigheder.

Uanset retsgrundlaget for en sådan behandling skal der foretages en proportionalitetstest forud for behandlingens indledning for at afgøre, om behandlingen er nødvendig for at nå et legitimt mål, og for at se på de foranstaltninger, der skal træffes for at sikre, at krænkelserne af retten til privatliv og kommunikationshemmelighed begrænses til et minimum. Dette kan indgå i en konsekvensanalyse vedrørende databeskyttelse (DPIA).

3. Den retlige ramme

Mens nedenstående analyse primært er foretaget ud fra den nuværende retlige ramme i direktiv 95/46/EF (databeskyttelsesdirektivet)[3], ses der i udtalelsen også på forpligtelserne i forordning 2016/679 (den generelle forordning om databeskyttelse)[4], der allerede er trådt i kraft, og som vil finde anvendelse fra den 25. maj 2018.

Med hensyn til forslaget til forordning om e-databeskyttelse[5] opfordrer arbejdsgruppen de europæiske lovgivere til at indsætte en specifik undtagelse for indblanding i forbindelse med udstyr, som de ansatte har fået udleveret[6]. Forslaget til forordning indeholder ikke nogen passende undtagelse fra det generelle forbud mod indblanding, og arbejdsgiverne kan normalt ikke forelægge et gyldigt samtykke til behandling af deres ansattes personoplysninger.

3.1 Direktiv 95/46/EF – databeskyttelsesdirektivet

I sin udtalelse 8/2001 forklarede WP29 tidligere, at arbejdsgiverne tager højde for databeskyttelsesdirektivets grundlæggende databeskyttelsesprincipper, når de behandler personoplysninger i ansættelsesforhold. Det har udviklingen af nye teknologier og nye metoder til databehandling i sådanne forhold ikke ændret på. Faktisk kan man sige, at denne udvikling har gjort det *endnu* vigtigere, at arbejdsgiverne overholder databeskyttelsesprincipperne. I denne forbindelse bør arbejdsgiverne:

- sikre, at datene behandles med et specifikt og legitimt formål for øje, som er forholdsmæssigt og nødvendigt
- tage højde for princippet om formålsbegrænsning og sikre, at dataene er egnede, relevante og ikke er for omfattende til det legitime formål
- anvende proportionalitets- og nærhedsprincippet uanset det gældende retsgrundlag
- være åbne over for de ansatte om anvendelsen af og formålet med overvågningsteknologier
- give den registrerede mulighed for at udøve sine rettigheder, herunder retten til indsigt i og eventuelt til berigtigelse, sletning eller blokering af personoplysninger
- holde dataene ajour og ikke opbevare dem længere end højst nødvendigt og
- træffe alle nødvendige foranstaltninger for at beskytte dataene mod uautoriseret adgang og sikre, at personalet er tilstrækkeligt bevidst om databeskyttelsesforpligtelserne.

Uden at gentage de tidligere afgivne råd vil WP29 gerne fremhæve tre principper, nemlig retsgrundlag, gennemsigtighed og automatiske afgørelser.

---

[3] Europa-Parlamentet og Rådets direktiv 95/46/EF af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (*EFT L 281 af 23.11.1995, s. 31-50*, url: http://eur-lex.europa.eu/legal-content/DA/TXT/?uri=celex:31995L0046).

[4] Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse), (*EUT L 119 af 4.5.2016, s. 1-88*, url: http://eur-lex.europa.eu/legal-content/DA/TXT/?uri=CELEX%3A32016R0679).

[5] Forslag til Europa-Parlamentets og Rådets forordning om respekt for privatliv og beskyttelse af personoplysninger i forbindelse med elektronisk kommunikation og om ophævelse af direktiv 2002/58/EF, 2017/3 (COD), url: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=41241.

[6] Se WP29, *Udtalelse 1/2017 om forslaget til forordning om e-databeskyttelse*, WP247, 4. april 2017, s. 29, url: http://ec.europa.eu/newsroom/document.cfm?doc_id=44103.

3.1.1 *RETSGRUNDLAG (ARTIKEL 7)*

Ved behandling af personoplysninger i ansættelsesforhold skal mindst et af kriterierne i artikel 7 være opfyldt. Hvis de behandlede personoplysninger tilhører de særlige kategorier (jf. artikel 8), er behandlingen ulovlig, medmindre der er tale om en undtagelse[7,8]. Selv om arbejdsgiveren kan gøre en af disse undtagelser gældende, kræver det fortsat et retsgrundlag fra artikel 7, for at behandlingen er lovlig.

Kort fortalt skal arbejdsgiverne altså bemærke følgende:

- I forbindelse med de fleste tilfælde af databehandling på arbejdspladsen **kan og bør retsgrundlaget ikke være de ansattes samtykke** (artikel 7, litra a)) som følge af forholdet mellem arbejdsgiver og arbejdstager.
- Behandlingen kan være nødvendig af hensyn til **opfyldelsen af en kontrakt** (artikel 7, litra b)) i tilfælde, hvor arbejdsgiveren er nødt til at behandle den ansattes personoplysninger for at opfylde en sådan forpligtelse.
- Det er ret almindeligt, at **arbejdsretten indeholder retlige forpligtelser** (artikel 7, litra c)), **som gør det nødvendigt at behandle personoplysninger.** I sådanne tilfælde skal den ansatte informeres klart og fuldt ud om behandlingen (medmindre der er tale om en undtagelse).
- Såfremt en arbejdsgiver forfølger en **legitim interesse** (artikel 7, litra f)), skal formålet med behandlingen være legitim. Den valgte metode eller specifikke teknologi skal være nødvendig, forholdsmæssig og implementeret på den mindst indgribende måde, og arbejdsgiveren skal kunne påvise, at **der er iværksat passende foranstaltninger** til sikring af balancen med de ansattes grundlæggende rettigheder og frihedsrettigheder[9].
- Behandlingen skal endvidere ske i overensstemmelse med **gennemsigtighedskravene** (artikel 10 og 11), og de ansatte skal informeres klart og fuldt ud om behandlingen af deres personoplysninger[10], herunder om eventuel overvågning.
- De **fornødne tekniske og organisatoriske foranstaltninger** skal iværksættes for at tilgodese behandlingssikkerheden (artikel 17).

De mest relevante kriterier i artikel 7 er beskrevet nedenfor.

- **Samtykke (artikel 7, litra a))**

Samtykke defineres i databeskyttelsesdirektivet som enhver frivillig, specifik og informeret viljetilkendegivelse, hvorved den registrerede indvilliger i, at personoplysninger, der vedrører

[7] Som nævnt i del 8 i udtalelse 8/2001. F.eks. fastsættes det i artikel 8, stk. 2, litra b), at behandlingen er nødvendig for overholdelsen af den registeransvarliges arbejdsretlige forpligtelser og specifikke rettigheder, for så vidt den er tilladt ifølge nationale lovbestemmelser, som fastsætter de fornødne garantier.

[8] Det skal bemærkes, at der i nogle lande er truffet særlige foranstaltninger, som arbejdsgiverne skal efterkomme, for at beskytte de ansattes privatliv. Et af disse lande er Portugal, og tilsvarende foranstaltninger kan finde anvendelse i flere andre medlemsstater. Konklusionerne i afsnit 5.6 og eksemplerne i afsnit 5.1 og 5.7.1 i denne udtalelse gælder derfor ikke Portugal.

[9] WP29, *Udtalelse 6/2014 om den registeransvarliges legitime interesser som omhandlet i artikel 7 i direktiv 95/46/EF*, WP217, vedtaget den 9. april 2014, url: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_da.pdf.

[10] I henhold til artikel 11, stk. 2, i databeskyttelsesdirektivet er den registeransvarlige fritaget fra forpligtelsen til at underrette den registrerede i tilfælde, hvor registreringen eller indsamlingen af oplysninger er udtrykkeligt fastsat ved lov.

den pågældende selv, gøres til genstand for behandling. Et samtykke er kun gyldigt, hvis det kan trækkes tilbage.

WP29 har tidligere i udtalelse 8/2001 nævnt, at det, når en arbejdsgiver skal behandle sine ansattes personoplysninger, er forkert at gå ud fra, at behandlingen er lovlig, fordi den ansatte har givet sit samtykke. I tilfælde, hvor arbejdsgiverne siger, de kræver et samtykke, og der er en reel eller potentielt relevant risiko for, at den ansatte lider skade, hvis han eller hun afviser at give sit samtykke (hvilket er yderst sandsynligt i ansættelsesforhold, navnlig når der er tale om, at arbejdsgiveren sporer den ansattes adfærd over tid), kan samtykket ikke gøres gældende, da det ikke er givet – og ikke kan gives – frivilligt. I størstedelen af de tilfælde, hvor arbejdsgiverne behandler oplysninger om de ansatte, kan og bør retsgrundlaget for den pågældende behandling ikke være de ansattes samtykke, og der skal foreligge et andet retsgrundlag.

Selv i tilfælde, hvor et samtykke kan opfattes som et gyldigt retsgrundlag for en sådan behandling (dvs. hvis der ikke hersker nogen tvivl om, at samtykket er givet frivilligt), skal der være tale om en specifik og informeret viljetilkendegivelse fra den ansattes side. Standardindstillinger på udstyr og/eller installering af software, der letter elektronisk behandling af personoplysninger, kan ikke opfattes som en ansats samtykke, da et samtykke kræver en aktiv viljetilkendegivelse. Manglende handling (f.eks. at den ansatte ikke har ændret standardindstillingerne) kan generelt ikke opfattes som et specifikt samtykke til en sådan behandling[11].

- **Opfyldelse af en kontrakt (artikel 7, litra b))**

Ansættelsesforhold er ofte baseret på en ansættelseskontrakt mellem arbejdsgiver og arbejdstager. Når arbejdsgiveren opfylder forpligtelserne i en sådan kontrakt, f.eks. ved lønudbetaling til den ansatte, er han eller hun nødt til at behandle nogle personoplysninger.

- **Retlige forpligtelser (artikel 7, litra c))**

Det sker ganske ofte, at arbejdsretten pålægger arbejdsgiveren retlige forpligtelser, som nødvendiggør behandling af personoplysninger (f.eks. ved skatteberegning og lønadministration). Det er klart, at sådanne arbejdsretlige forpligtelser i disse tilfælde udgør retsgrundlaget for databehandlingen.

- **Legitim interesse (artikel 7, litra f))**

Hvis en arbejdsgiver vil gøre retsgrundlaget i artikel 7, litra f), i databeskyttelsesdirektivet gældende, skal formålet med behandlingen være legitimt, og den valgte metode eller specifikke teknologi, der anvendes til behandlingen, skal være nødvendig for at tilgodese arbejdsgiverens legitime interesse. Behandlingen skal endvidere stå i et rimeligt forhold til virksomhedens behov, dvs. formålet med behandlingen. Databehandling på arbejdspladsen skal ske på den mindst indgribende måde og være målrettet det specifikke risikoområde. Derudover har den ansatte i henhold til artikel 14 ret til at gøre indsigelse mod behandling efter artikel 7, litra f), af vægtige legitime grunde.

[11] Se også WP29, *Udtalelse 15/2011 om definitionen af samtykke*, WP187, 13. juli 2011, url: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_da.pdf, s. 24.

For at kunne gøre artikel 7, litra f), gældende som retsgrundlag for behandlingen er det vigtigt, at der er iværksat specifikke risikobegrænsende foranstaltninger for at sikre den rette balance mellem arbejdsgiverens legitime interesser og den ansattes grundlæggende rettigheder og frihedsrettigheder[12]. Sådanne foranstaltninger bør, alt efter overvågningsmetoden, omfatte begrænsninger for overvågningen for at garantere, at den ansattes privatliv ikke krænkes. Disse begrænsninger kan f.eks. være:

- geografiske (f.eks. begrænsning af overvågningen til bestemte steder – overvågning af følsomme områder såsom religiøse opholdssteder og f.eks. toiletter og pauserum skal forbydes)
- dataorienterede (f.eks. bør personlige elektroniske filer og personlig kommunikation ikke overvåges)
- tidsrelaterede (f.eks. stikprøveovervågning i stedet for løbende overvågning).

3.1.2 *GENNEMSIGTIGHED (ARTIKEL 10 OG 11)*

Gennemsigtighedskravene i artikel 10 og 11 finder anvendelse på databehandling på arbejdspladsen. Arbejdstagerne skal underrettes om eventuelle overvågningsforanstaltninger, om formålene med den behandling, hvortil personoplysningerne er bestemt, og om alle yderligere forhold, der er nødvendige for at garantere en rimelig behandling.

De nye teknologier har gjort behovet for gennemsigtighed endnu mere åbenlyst, da de muliggør skjult indsamling og videre behandling af potentielt enorme mængder personoplysninger.

3.1.3 *AUTOMATISKE AFGØRELSER (ARTIKEL 15)*

Artikel 15 i databeskyttelsesdirektivet indrømmer registrerede ret til ikke at være undergivet afgørelser, der har retsvirkning for dem, eller som berører dem i væsentlig grad, og som alene er truffet på grundlag af automatisk behandling af oplysninger, der er bestemt til at vurdere bestemte personlige forhold, såsom arbejdsindsats, medmindre afgørelsen er nødvendig som led i indgåelsen eller opfyldelsen af en kontrakt, er hjemlet i EU's eller medlemsstatens lovgivning, eller er baseret på den registreredes udtrykkelige samtykke.

3.2 Forordning 2016/679 – den generelle forordning om databeskyttelse

Den generelle forordning om databeskyttelse indeholder og skærper kravene i databeskyttelsesdirektivet. Den indfører endvidere nye forpligtelser for alle registeransvarlige, herunder arbejdsgiverne.

3.2.1 *DATABESKYTTELSE GENNEM DESIGN*

I henhold til artikel 25 i den generelle forordning om databeskyttelse skal de registeransvarlige gennemføre databeskyttelse gennem design og standardindstillinger. Et

[12] Der findes et eksempel på den balance, der skal findes, i sagen *Köpke mod Tyskland*, [2010] ECHR 1725, (URL: http://www.bailii.org/eu/cases/ECHR/2010/1725.html), i hvilken en ansat blev afskediget som følge af en skjult videoovervågningsoperation, som arbejdsgiveren foretog i samarbejde med et privatdetektivbureau. Mens domstolen i denne sag konkluderede, at de nationale myndigheder havde fundet en rimelig balance mellem arbejdsgiverens legitime interesse (beskyttelse af virksomhedens ejendomsrettigheder), den ansattes ret til respekt for privatliv og den offentlige interesse i retssikkerheden, bemærkede den ligeledes, at de forskellige berørte interesser i fremtiden kunne blive vægtet anderledes som følge af den teknologiske udvikling.

eksempel: Når en arbejdsgiver udleverer udstyr til sine ansatte, bør de mest privatlivsvenlige løsninger vælges, hvis der anvendes sporingsteknologier. Der skal også tages hensyn til dataminimering.

3.2.2 *KONSEKVENSANALYSE VEDRØRENDE DATABESKYTTELSE*

Artikel 35 i den generelle forordning om databeskyttelse indeholder krav om, at en registeransvarlig skal foretage en konsekvensanalyse vedrørende databeskyttelse (DPIA), hvis en type behandling, navnlig ved brug af nye teknologier og i medfør af sin karakter, omfang, sammenhæng og formål, sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder. Et eksempel kan være et tilfælde med systematisk og omfattende vurdering af personlige forhold vedrørende fysiske personer, der er baseret på automatisk behandling, herunder profilering, og som danner grundlag for afgørelser, der har retsvirkning for den fysiske person eller på tilsvarende vis i betydelig grad påvirker den pågældende.

Såfremt konsekvensanalysen vedrørende databeskyttelse viser, at den registeransvarlige ikke i tilstrækkelig grad kan afhjælpe de identificerede risici – dvs. at restrisiciene er høje – skal den registeransvarlige høre tilsynsmyndigheden inden behandlingen (artikel 36, stk. 1), som klarlagt i WP29's retningslinjer om konsekvensanalyser vedrørende databeskyttelse[13].

3.2.3 *"BEHANDLING I FORBINDELSE MED ANSÆTTELSESFORHOLD"*

I artikel 88 i den generelle forordning om databeskyttelse hedder det, at medlemsstaterne ved lov eller i medfør af kollektive overenskomster kan fastsætte mere specifikke bestemmelser for at sikre beskyttelse af rettighederne og frihedsrettighederne i forbindelse med behandling af ansattes personoplysninger i ansættelsesforhold. Disse bestemmelser kan navnlig anvendes med henblik på:

- ansættelse
- opfyldelse af ansættelseskontrakten (herunder opfyldelse af forpligtelser fastsat ved lov eller i kollektive overenskomster)
- ledelse, planlægning og tilrettelæggelse af arbejdet
- ligestilling og mangfoldighed på arbejdspladsen
- sundhed og sikkerhed på arbejdspladsen
- beskyttelse af en arbejdsgivers eller kundes ejendom
- (individuel) udøvelse og nydelse af rettigheder og fordele i forbindelse med ansættelse og
- ophør af ansættelsesforhold.

I henhold til artikel 88, stk. 2, skal disse bestemmelser omfatte passende og specifikke foranstaltninger til beskyttelse af den registreredes menneskelige værdighed, legitime interesser og grundlæggende rettigheder, særlig med hensyn til:

- gennemsigtighed i behandlingen
- overførsel af personoplysninger inden for en koncern eller gruppe af foretagender, der udøver en fælles økonomisk aktivitet, og

[13] WP29, *Retningslinjer om konsekvensanalyse vedrørende databeskyttelse (DPIA) og bestemmelse af, om behandling vil resultere i en "høj risiko", jf. forordning 2016/679*, WP248, 4. april 2017, url: http://ec.europa.eu/newsroom/document.cfm?doc_id=44137, s. 18.

- overvågningssystemer på arbejdspladsen.

I denne udtalelse har arbejdsgruppen udstukket retningslinjer for lovlig anvendelse af ny teknologi i en række specifikke situationer og beskrevet passende og specifikke foranstaltninger til beskyttelse af de ansattes menneskelige værdighed, legitime interesser og grundlæggende rettigheder.

4. Risici

De moderne teknologier giver mulighed for at spore de ansatte over tid, på tværs af deres arbejdsplads og hjem, ved hjælp af mange forskellige enheder såsom smartphones, desktopcomputere, tablets, køretøjer og wearables. Hvis ikke behandlingen begrænses, og hvis ikke den er gennemsigtig, er der stor risiko for, at arbejdsgiverens legitime interesse i effektivitetsforbedring og beskyttelse af virksomhedens aktiver bliver til uberettiget og indgribende overvågning.

Teknologier til kommunikationsovervågning kan også have en negativ indvirkning på de ansattes grundlæggende rettigheder til at organisere sig, afholde medarbejdermøder og kommunikere fortroligt (herunder retten til at søge oplysninger). Overvågning af kommunikation og adfærd presser de ansatte til at tilpasse sig for at undgå, at der detekteres noget, der opfattes som unormalt, på samme måde som den intensive anvendelse af tv-overvågning har påvirket borgernes adfærd på offentlige steder. På grund af de muligheder, som disse teknologier rummer, er de ansatte måske ikke bevidst om, hvilke personoplysninger der behandles og til hvilket formål, ligesom det også er muligt, at de ikke engang er bekendt med, at den pågældende overvågningsteknologi anvendes.

Overvågning af brugen af it-udstyr er også forskellig fra andre mere synlige observations- og overvågningsværktøjer som tv-overvågning, da overvågningen kan ske i det skjulte. Hvis ikke der findes nogen letforståelig og umiddelbart tilgængelig politik for overvågning på arbejdspladsen, er de ansatte ikke nødvendigvis bevidst om, at der finder overvågning sted og konsekvenserne heraf, og de er derfor ikke i stand til at udøve deres rettigheder. "Overindsamlingen" af data i sådanne systemer udgør en yderligere risiko, f.eks. i de systemer, der indsamler wi-fi-lokaliseringsdata.

Den stigende mængde oplysninger, der genereres på arbejdspladsen, kan også sammen med de nye teknikker til dataanalyse og krydsmatching medføre risiko for uforenelig viderebehandling. Ulovlig viderebehandling omfatter bl.a. anvendelse af systemer, der er installeret lovligt for at beskytte ejendommen, til overvågning af de ansattes disponibilitet, indsats og kundevenlighed. Andre former for ulovlig viderebehandling omfatter anvendelse af data, som indsamles via et tv-overvågningssystem, til regelmæssigt at overvåge de ansattes adfærd og indsats og anvendelse af data fra geolokaliseringssystemer (f.eks. wi-fi- eller bluetooth-sporing) til konstant at tjekke en ansats bevægelser og adfærd.

Sådanne former for sporing kan krænke de ansattes ret til privatliv, uanset om overvågningen er systematisk eller lejlighedsvis. Risikoen er ikke begrænset til analysen af indholdet i kommunikation. En analyse af metadata om en person kan således også resultere i detaljeret overvågning af en persons leve- og adfærdsmønstre, der i lige så høj grad krænker personens ret til privatliv.

Den omfattende anvendelse af overvågningsteknologier kan også begrænse de ansattes vilje (og de kanaler, de kan bruge) til at underrette arbejdsgiverne om uregelmæssigheder eller ulovlige handlinger foretaget af overordnet personale og/eller andre ansatte, der truer med at skade forretningen (især kundedata) eller arbejdspladsen. Det er ofte nødvendigt, at en ansat sikres anonymitet, før han eller hun griber ind og rapporterer sådanne forhold. Overvågning, der krænker de ansattes ret til privatliv, kan hæmme nødvendig kommunikation til relevante medarbejdere. I sådanne tilfælde kan de etablerede interne ordninger for rapportering af uregelmæssigheder blive ineffektive[14].

5. Scenarier

Dette afsnit indeholder en række scenarier for databehandling på arbejdspladsen, hvor nye teknologier og/eller videreudviklinger af eksisterende teknologier har – eller kan få – potentiale til at udgøre en stor risiko for de ansattes privatliv. I alle disse tilfælde bør arbejdsgiverne overveje, hvorvidt:

- behandlingen er nødvendig, og hvis ja, hvilket retsgrundlag der finder anvendelse
- den foreslåede behandling af personoplysninger er rimelig for de ansatte
- behandlingen står i et rimeligt forhold til de rejste bekymringer og
- behandlingen er gennemsigtig.

5.1 Behandlingsaktiviteter under ansættelsesproceduren

Brugen af sociale medier blandt fysiske personer er omfattende, og det er relativt almindeligt, at brugerprofiler er offentligt tilgængelige, alt efter hvilke indstillinger kontohaveren har valgt. Arbejdsgiverne kan derfor tro, at det er berettiget at gennemgå potentielle kandidaters sociale profiler under ansættelsesproceduren. Dette gælder også andre offentligt tilgængelige oplysninger om den potentielle nye medarbejder.

Arbejdsgiverne bør imidlertid ikke gå ud fra, at de, blot fordi en persons profil på de sociale medier er offentligt tilgængelig, har lov til at behandle disse oplysninger til deres egne formål. En sådan behandling kræver et retsgrundlag, såsom en legitim interesse. I denne forbindelse bør arbejdsgiveren – forud for en gennemgang af en persons profil på de sociale medier – tage hensyn til, om ansøgerens profil er en arbejdsrelateret profil eller en privat profil, da dette kan være en vigtig indikator for, om det er lovligt at gennemgå oplysningerne eller ej. Derudover er arbejdsgivere kun berettiget til at indsamle og behandle personoplysninger vedrørende jobansøgere, i det omfang indsamlingen af disse oplysninger er nødvendig og relevant for bestridelsen af det job, der ansøges om.

Data, der indsamles under ansættelsesproceduren, bør generelt slettes, så snart det ligger fast, at ansøgeren ikke vil få tilbudt jobbet, eller at den pågældende person ikke accepterer

[14] Se f.eks. WP29, *Udtalelse 1/2006 om anvendelsen af EU's databeskyttelsesregler på interne ordninger for rapportering af uregelmæssigheder på områderne regnskabsføring, intern regnskabskontrol, revision, bekæmpelse af korruption samt kriminalitet i bank- og finanssektoren*, WP117, 1. februar 2006, url: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2006/wp117_da.pdf.

jobbet[15]. Ansøgeren skal endvidere underrettes behørigt om en sådan behandling forud for ansættelsesproceduren.

Der findes ikke noget retsgrundlag for, at en arbejdsgiver kræver, at potentielle nye medarbejdere skal "blive venner" med deres potentielle nye arbejdsgiver eller på anden vis give adgang til indholdet i deres profiler.

Eksempel

I forbindelse med ansættelsen af nyt personale tjekker en arbejdsgiver kandidaternes profiler på forskellige sociale netværker og indlemmer oplysninger herfra (og andre oplysninger, der er tilgængelige på internettet) i screeningprocessen.

Kun hvis det er nødvendigt for jobbet at gennemgå oplysninger om kandidaterne på de sociale medier, f.eks. for at kunne vurdere, om der er specifikke risici forbundet med en kandidats bestridelse af et bestemt job, og kun hvis kandidaterne er blevet behørigt informeret herom (f.eks. i jobannoncen), kan arbejdsgiveren have et retsgrundlag, jf. artikel 7, litra f), for at gennemgå offentligt tilgængelige oplysninger om kandidaterne.

5.2 Behandlingsaktiviteter ved screening af allerede ansatte

Takket være profilerne på de sociale medier og udviklingen af nye analyseteknologier har arbejdsgiverne (eller kan arbejdsgiverne få) teknisk mulighed for at screene de ansatte permanent ved at indsamle oplysninger om deres venner, meninger, tro, interesser, vaner, opholdssteder, holdninger og adfærd og i den forbindelse registrere oplysninger, herunder følsomme oplysninger, om de ansattes privatliv og familieliv.

Screening af allerede ansattes profiler på de sociale medier bør generelt ikke finde sted.

Desuden bør arbejdsgiverne afholde sig fra at stille krav om, at en ansat eller jobansøger giver adgang til oplysninger, som personen deler med andre på de sociale medier.

Eksempel
En arbejdsgiver overvåger LinkedIn-profilerne for tidligere ansatte, der er omfattet af en konkurrenceklausul. Formålet med denne overvågning er at tjekke, at de tidligere ansatte overholder disse klausuler. Overvågningen er begrænset til disse tidligere ansatte.

Så længe arbejdsgiveren kan bevise, at overvågningen er nødvendig for at beskytte hans eller hendes legitime interesser, at der ikke findes andre mindre indgribende metoder, og at de tidligere ansatte er blevet behørigt underrettet om omfanget af den regelmæssige kontrol af deres offentlige kommunikation, kan arbejdsgiveren gøre retsgrundlaget i artikel 7, litra f), i databeskyttelsesdirektivet gældende.

[15] Se også Europarådet, *Henstilling CM/Rec(2015)5 fra Ministerkomitéen til medlemsstaterne om behandling af personoplysninger i ansættelsesforhold*, punkt 13.2 (1. april 2015, url: https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805c3f7a). I tilfælde, hvor arbejdsgiveren ønsker at opbevare oplysningerne med henblik på senere jobmuligheder, skal den registrerede underrettes herom og have mulighed for at gøre indsigelse mod en sådan videre behandling, hvorefter dataene i påkommende tilfælde skal slettes (id.).

Derudover bør de ansatte ikke pålægges at anvende en profil på et socialt medie, som arbejdsgiveren stiller til rådighed. Også selv om dette specifikt er ønskværdigt i lyset af deres opgaver (f.eks. talsmand for en virksomhed), skal de have mulighed for at anvende en ikke-arbejdsrelateret, ikke-offentlig profil i stedet for den "officielle" arbejdsgiverrelaterede profil, og dette bør fastsættes i ansættelseskontraktens betingelser og vilkår.

5.3 Behandlingsaktiviteter ved overvågning af brugen af IKT på arbejdspladsen

Traditionelt blev overvågningen af elektronisk kommunikation på arbejdspladsen (f.eks. telefon, internetsøgning, e-mail, instant messaging, VOIP osv.) opfattet som den primære trussel mod de ansattes privatliv. I sit *Arbejdsdokument om overvågning af elektronisk kommunikation på arbejdspladsen* fra 2001 fremsatte WP29 en række konklusioner vedrørende overvågning af brugen af e-mail og internet. Disse konklusioner gælder fortsat, men der skal tages højde for den teknologiske udvikling, der har givet mulighed for nye, potentielt mere indgribende og omsiggribende overvågningsmetoder. Denne udvikling omfatter bl.a.:

- værktøjer til forebyggelse af datatab (DLP), som overvåger udgående kommunikation med henblik på at detektere potentielle brud på datasikkerheden
- Next-Generation Firewalls (NGFW) og Unified Threat Management-systemer (UTM), som kan omfatte en bred vifte af overvågningsteknologier, herunder "deep packet inspection", "TLS interception", webstedsfiltrering, indholdsfiltrering, "on-appliance reporting", oplysninger om brugerid og (som beskrevet ovenfor) forebyggelse af datatab. Disse teknologier kan også anvendes individuelt, alt afhængig af arbejdsgiveren
- sikkerhedsapplikationer og -foranstaltninger, der involverer registrering af den ansattes adgang til arbejdsgiverens systemer
- eDiscovery-teknologi, som henviser til enhver proces, hvor der søges efter elektroniske data med henblik på at anvende dem som bevismateriale
- sporing af brugen af applikationer og udstyr via usynlig software, enten på desktopcomputeren eller i en cloud
- brug af kontorapplikationer på arbejdspladsen som en cloud-tjeneste, der i teorien giver mulighed for at registrere de ansattes aktiviteter meget nøjagtigt
- overvågning af de ansattes personlige udstyr (f.eks. pc'er, mobiltelefoner, tablets), som de bruger på deres arbejdsplads ifølge en specifik anvendelsespolitik, såsom Bring Your Own Device (BYOD – brug af eget udstyr) og Mobile Device Management-teknologi (MDM), som muliggør distribuering af applikationer, data og konfigurationsindstillinger, samt patches til mobilt udstyr og
- brug af wearable udstyr (f.eks. helbreds- og fitnessudstyr).

Det er muligt, at en arbejdsgiver implementerer en alt i én-overvågningsløsning, f.eks. en serie sikkerhedspakker, der giver arbejdsgiveren mulighed for at overvåge al brug af IKT på arbejdspladsen, i stedet for blot at overvåge e-mail og/eller websteder, sådan som det tidligere var tilfældet. Konklusionerne i WP55 finder anvendelse på alle systemer, der muliggør en sådan overvågning[16].

[16] Se også *Copland mod Det Forenede Kongerige*, (2007) 45 EHRR 37, 25 BHRC 216, 2 ALR Int'l 785, [2007] ECHR 253 (url: http://www.bailii.org/eu/cases/ECHR/2007/253.html), hvor domstolen fastslog, at e-mail, der

Eksempel

En arbejdsgiver vil indføre TLS-kontroludstyr til dekryptering og inspektion af sikker trafik med det formål at detektere eventuel skadelig kommunikation. Udstyret kan desuden registrere og analysere alle en ansats online aktiviteter på virksomhedens netværk.

Brugen af krypterede kommunikationsprotokoller anvendes i stigende grad til at beskytte online datastrømme, der involverer personoplysninger, mod at blive opfanget. Dette kan imidlertid også udgøre et problem, da krypteringen gør det umuligt at overvåge indkommende og udgående data. TLS-kontroludstyr dekrypterer datastrømmen, analyserer indholdet i sikkerhedsøjemed og krypterer derefter datastrømmen igen.

I dette eksempel gør arbejdsgiveren sine legitime interesser gældende – nødvendigheden af at beskytte netværket og de personoplysninger vedrørende ansatte og kunder, der ligger på dette netværk, mod uautoriseret adgang eller datalækage. Overvågningen af alle en ansats online aktiviteter er imidlertid et uforholdsmæssigt tiltag, som griber ind i retten til kommunikationshemmelighed. Arbejdsgiveren bør først undersøge, om der findes andre, mindre indgribende midler, som kan beskytte kundeoplysningernes fortrolighed og netværkssikkerheden.

I det omfang opfangningen af en del af TLS-trafikken kan kvalificeres som strengt nødvendig, skal udstyret konfigureres på en måde, der forhindrer permanent registrering af den ansattes aktivitet, f.eks. ved at blokere mistænkelig indkommende og udgående trafik og omdirigere brugeren til en informationsportal, hvor han eller hun kan anmode om at få revideret en sådan automatisk afgørelse. Hvis generel registrering i en vis udstrækning findes strengt nødvendig, kan udstyret også konfigureres, så det ikke lagrer logdata, medmindre udstyret signalerer en hændelse, idet omfanget af de indsamlede oplysninger minimeres.

Arbejdsgiveren kan som god praksis tilbyde de ansatte en alternativ, ikke-overvåget adgang. Dette kan gøres ved at tilbyde gratis wi-fi eller stand alone-udstyr eller -terminaler (med egnede sikkerhedsforanstaltninger til sikring af kommunikationens fortrolighed), hvor de ansatte kan udøve deres legitime ret til i en vis udstrækning at bruge arbejdsfaciliteter til private formål[17]. Derudover bør arbejdsgiverne overveje visse typer trafik, hvis opfangning bringer den rette balance mellem deres legitime interesser og de ansattes privatliv – f.eks. anvendelse af privat webmail, besøg på netbanker og sundhedswebsteder – i fare, med det formål at konfigurere udstyret korrekt, så der ikke opfanges kommunikation under forhold, som ikke er i overensstemmelse med proportionalitetsprincippet. De ansatte bør underrettes om den type kommunikation, som udstyret overvåger.

---

sendes fra arbejdspladsen, og oplysninger, der stammer fra overvågningen af internetbrug, kan være en del af en ansats privatliv og private korrespondance, og at indsamling og lagring af sådanne oplysninger uden den ansattes kendskab dertil ville udgøre et indgreb i den ansattes rettigheder, selv om domstolen ikke fastslog, at sådan overvågning aldrig er nødvendig i et demokratisk samfund.

[17] Se *Halford mod Det Forenede Kongerige*, [1997] ECHR 32, (url: http://www.bailii.org/eu/cases/ECHR/1997/32.html), hvor domstolen fastslog, at telefonopkald fra arbejdspladsen og hjemmefra kan være omfattet af begreberne "privatliv" og "korrespondance", jf. artikel 8, stk. 1, [i konventionen], og *Barbulescu mod Rumænien*, [2016] ECHR 61, (url: http://www.bailii.org/eu/cases/ECHR/2016/61.html) vedrørende anvendelse af en instant messaging-arbejdskonto til personlig korrespondance, hvor domstolen fastslog, at arbejdsgiverens overvågning af kontoen var begrænset og forholdsmæssig. Dommer Pinto de Alberquerque argumenterede i sin afvigende holdning for, at der skulle findes en hårfin balance.

Der bør udarbejdes en politik for, hvem der har adgang til mistænkelige logdata og til hvilke formål. De ansatte skal have uhindret og permanent adgang til denne politik, som skal vejlede dem om acceptabel og uacceptabel brug af netværket og faciliteterne. Dette giver de ansatte mulighed for at tilpasse deres adfærd, så de ikke bliver overvåget, når de på lovlig vis bruger it-faciliteterne på arbejdspladsen til private formål. Det er god praksis at evaluere politikken mindst en gang om året for at vurdere, om den valgte overvågningsløsning giver de ønskede resultater, og om der findes andre, mindre indgribende værktøjer, som kan give de samme resultater.

Uanset hvilken teknologi der anvendes, og hvilke muligheder den rummer, finder retsgrundlaget i artikel 7, litra f), kun anvendelse, hvis behandlingen opfylder visse betingelser. For det første skal de arbejdsgivere, der anvender disse produkter og applikationer, overveje, om de foranstaltninger, de iværksætter, er forholdsmæssige, og om der kan iværksættes yderligere tiltag for at begrænse databehandlingen eller mindske dens omfang og virkning. Som et eksempel på god praksis kan disse overvejelser foretages inden for rammerne af en konsekvensanalyse vedrørende databeskyttelse, inden der indføres nogen form for overvågningsteknologi. For det andet skal arbejdsgiverne gennemføre og oplyse om politikker for acceptabel anvendelse sammen med deres politikker for beskyttelse af privatlivets fred, i hvilke de beskriver den tilladte anvendelse af virksomhedens netværk og udstyr og giver nærmere oplysninger om den behandling, der finder sted.

I nogle lande kræver udarbejdelsen af en sådan politik rent juridisk en godkendelse i et samarbejdsudvalg eller en tilsvarende arbejdstagerrepræsentation. I praksis udarbejdes disse politikker ofte af it-medarbejderne. Eftersom de primært har fokus på sikkerheden og ikke på de ansattes berettigede forventninger om beskyttelse af deres privatliv, anbefaler WP29, at et repræsentativt udsnit af de ansatte altid er med til at vurdere overvågningens nødvendighed og politikkens logik og tilgængelighed.

Eksempel

En arbejdsgiver indfører et værktøj til forebyggelse af datatab med automatisk overvågning af udgående e-mails med det formål at forebygge uautoriseret overførsel af ejendomsretsbeskyttede data (f.eks. en kundes personoplysninger), uanset om en sådan overførsel er uforsætlig eller ej. Når en e-mail opfattes som en potentiel kilde til et brud på datasikkerheden, iværksættes der yderligere undersøgelser.

Igen gør arbejdsgiveren sin legitime interesse i at beskytte kundernes personoplysninger og arbejdsgiverens aktiver mod uautoriseret adgang og datalækage gældende. Et sådant værktøj til forebyggelse af datatab kan imidlertid også medføre unødvendig behandling af personoplysninger – f.eks. kan en falsk positiv advarsel udmønte sig i uautoriseret adgang til legitime e-mails, som de ansatte har sendt (og som f.eks. kan være personlige e-mails).

Derfor skal nødvendigheden af et værktøj til forebyggelse af datatab og indførelsen heraf kunne dokumenteres fuldt ud for at sikre den rette balance mellem arbejdsgiverens legitime interesser og de ansattes grundlæggende rettigheder til beskyttelse af deres personoplysninger. For at arbejdsgiveren skal kunne gøre sine legitime interesser gældende, skal der være iværksat visse foranstaltninger til risikoafhjælpning. F.eks. skal de regler, som systemet følger, når det karakteriserer en e-mail som et potentielt brud på datasikkerheden, være helt gennemskuelige for brugerne, og såfremt værktøjet opfatter en e-mail, der er ved at blive sendt, som et potentielt brud på datasikkerheden, skal en advarsel underrette e-mailens afsender herom, inden e-mailen afsendes, så afsenderen har mulighed for at annullere den.

I nogle tilfælde er det muligt at overvåge sine ansatte, ikke så meget ved hjælp af specifikke teknologier, men ganske enkelt fordi de ansatte forventes at anvende online applikationer, som arbejdsgiveren stiller til rådighed, og som behandler personoplysninger. Det er anvendelsen af cloud-baserede kontorapplikationer (f.eks. dokumentredigeringsprogrammer, kalendere, sociale netværker) et eksempel på. Det skal sikres, at de ansatte kan udpege visse private områder, som arbejdsgiveren kun har adgang til i helt særlige tilfælde. Dette kan f.eks. være relevant for en kalender, som ofte også bruges til private aftaler. Hvis den ansatte markerer en aftale som "privat" eller angiver dette i selve aftalens indhold, bør arbejdsgiveren (og de øvrige ansatte) ikke have lov til at tjekke aftalens indhold.

Kravet om overholdelse af nærhedsprincippet betyder i denne sammenhæng nogle gange, at der slet ikke må finde overvågning sted. Det er f.eks. tilfældet, når et forbud mod anvendelse af kommunikationstjenester kan undgås ved at blokere visse websteder. Hvis det er muligt at blokere websteder i stedet for løbende at overvåge al kommunikation, skal det vælges at foretage en sådan blokering for at overholde nærhedsprincippet.

Der skal generelt lægges mere vægt på at forebygge end på at detektere – arbejdsgiverens interesser tilgodeses bedre ved at forebygge internetmisbrug med tekniske midler end ved at bruge ressourcer på at detektere et misbrug.

5.4 Behandlingsaktiviteter ved overvågning af brugen af IKT uden for arbejdspladsen

Brugen af IKT uden for arbejdspladsen er blevet mere og mere udbredt med den stigende tendens til hjemmearbejde, fjernarbejde og brug af eget udstyr. Disse

teknologiers mange muligheder kan udgøre en risiko for de ansattes ret til privatliv, da de overvågningssystemer, der findes på arbejdspladserne, i mange tilfælde forlænges til de ansattes hjemmesfære, når de bruger sådant udstyr. .

5.4.1 *OVERVÅGNING VED HJEMME- OG FJERNARBEJDE*

Det bliver mere og mere almindeligt, at arbejdsgiverne giver de ansatte mulighed for at fjernarbejde, f.eks. hjemmefra og/eller mens de er ude at rejse. Dette er en af de helt centrale faktorer bag det forhold, at der skelnes mindre mellem arbejdsplads og hjem. Generelt indebærer dette, at arbejdsgiveren udleverer IKT-udstyr eller software til de ansatte, som, når udstyret eller softwaren er installeret i deres hjem/på deres eget udstyr, giver dem den samme adgang til arbejdsgiverens netværk, systemer og ressourcer, som de ville have haft, hvis de befandt sig på arbejdspladsen, alt afhængig af konfigureringen.

Fjernarbejde kan bestemt være en positiv udvikling, men det er også forbundet med flere risici for arbejdsgiveren. Ansatte, der har fjernadgang til arbejdsgiverens infrastruktur, er f.eks. ikke bundet af de fysiske sikkerhedsforanstaltninger, der er iværksat på arbejdspladsen. Det betyder med andre ord, at når der ikke er truffet egnede tekniske foranstaltninger, er risikoen for uautoriseret adgang større, hvilket kan resultere i tab eller ødelæggelse af oplysninger, herunder personoplysninger vedrørende ansatte eller kunder, som arbejdsgiveren måtte ligge inde med.

For at begrænse dette risikoområde kan arbejdsgiverne måske tro, det er berettiget at anvende softwarepakker (enten på stedet eller i en cloud), som f.eks. kan registrere tasteanslag og musebevægelser, screen capturing (enten vilkårligt eller med faste intervaller), registrere, hvilke applikationer der er blevet anvendt (og hvor længe de er blevet anvendt), og på kompatibelt udstyr aktivere webcams og indsamle optagelser derfra. Disse teknologier fås overalt, bl.a. hos tredjeparter såsom udbydere af cloud-tjenester.

Den behandling, der kan foretages med disse teknologier, er imidlertid uforholdsmæssig, og det er meget usandsynligt, at arbejdsgiveren kan gøre sine legitime interesser gældende som retsgrundlag for f.eks. at registrere en ansats tasteanslag og musebevægelser.

Det centrale er at afhjælpe den risiko, som hjemme- og fjernarbejde udgør, på en forholdsmæssig og ikke for indgribende måde, uanset hvordan muligheden tilbydes, og uanset hvilken teknologi der foreslås anvendt, især hvis grænsen mellem arbejdsbrug og privat brug er flydende.

5.4.2 *BRING YOUR OWN DEVICE (BYOD – BRUG AF EGET UDSTYR)*

Da forbrugerelektronik bliver mere og mere populært, får flere og flere funktioner og kan mere og mere, anmoder de ansatte af og til arbejdsgiverne om lov til at bruge deres eget udstyr i arbejdsøjemed. Dette fænomen går under betegnelsen "Bring Your Own Device" eller BYOD.

Effektiv implementering af BYOD kan give de ansatte en række fordele, herunder større jobtilfredshed, øget mentalt velvære generelt, øget jobeffektivitet og større fleksibilitet. Den ansattes udstyr vil dog pr. definition også blive brugt personligt, og dette vil ofte ske på bestemte tidspunkter (f.eks. om aftenen og i weekenderne). Det er derfor meget muligt, at arbejdsgiveren i forbindelse med den ansattes brug af eget udstyr kommer til at behandle

ikke-arbejdsrelaterede oplysninger om den ansatte og sandsynligvis også om andre familiemedlemmer, der også bruger det pågældende udstyr.

I ansættelsesforhold knyttes risikoen for krænkelse af privatlivets fred i forbindelse med BYOD ofte sammen med overvågningsteknologier, der indsamler identifikatorer såsom MAC-adresser, eller tilfælde, hvor en arbejdsgiver skaffer sig adgang til en ansats udstyr med henblik på at foretage en sikkerhedsscanning, f.eks. for malware. I sidstnævnte tilfælde findes der en række kommercielle løsninger, der gør det muligt at scanne privat udstyr, men brugen heraf kan potentielt give adgang til alle data på det pågældende udstyr, så de skal bruges med forsigtighed. De sektioner på privat udstyr, der formodes kun at være til privat brug (f.eks. mappen med billeder, der er taget med udstyret), må arbejdsgiveren i princippet ikke skaffe sig adgang til.

Overvågningen af sådant udstyrs position og trafik kan opfattes som en legitim interesse i at beskytte de personoplysninger, som arbejdsgiveren har ansvaret for som registeransvarlig. Dette kan imidlertid være ulovligt, når der er tale om en ansats personlige udstyr, hvis der i forbindelse med denne overvågning opfanges data vedrørende den ansattes privatliv og familieliv. For at forhindre overvågningen af private oplysninger skal der være iværksat passende foranstaltninger, som gør det muligt at skelne mellem privat og arbejdsmæssig brug af udstyret.

Arbejdsgiverne bør endvidere implementere metoder, hvorved deres egne data på udstyret kan overføres sikkert mellem udstyret og deres netværk. Dette kan f.eks. gøres ved at konfigurere udstyret til at route al trafik tilbage til firmanetværket via et VPN, hvilket giver en vis grad af sikkerhed. Hvis en sådan foranstaltning er indført, skal arbejdsgiveren imidlertid også tænke på, at det installerede overvågningssoftware indebærer en risiko for krænkelse af den ansattes privatliv i de perioder, hvor den ansatte bruger udstyret privat. Der kan f.eks. anvendes udstyr, som giver mulighed for yderligere beskyttelse, såsom en virtuel sandkasse (hvor dataene holdes inden for en bestemt app).

Omvendt må arbejdsgiveren også overveje at forbyde privat brug af specifikt arbejdsudstyr, hvis ikke det på nogen måde er muligt at forhindre, at den private brug overvåges, f.eks. hvis udstyret giver fjernadgang til personoplysninger, for hvilke arbejdsgiveren er registeransvarlig.

5.4.3 *MOBILE DEVICE MANAGEMENT (MDM)*

Mobile Device Management giver arbejdsgiverne mulighed for at lokalisere udstyr på afstand, implementere specifikke konfigurationer og/eller applikationer og slette data på anmodning. Arbejdsgiveren kan enten selv stå for dette eller få en tredjepart til at gøre det. MDM-tjenester giver endvidere arbejdsgiverne mulighed for at registrere eller spore udstyret i realtid, også selv om det ikke er meldt stjålet.

Der bør foretages en konsekvensanalyse vedrørende databeskyttelse, inden en sådan teknologi indføres, når teknologien er ny, eller når den er ny for den registeransvarlige. Hvis konsekvensanalysen vedrørende databeskyttelse viser, at MDM-teknologien er nødvendig under visse forhold, bør der foretages en vurdering af, om den resulterende databehandling er i overensstemmelse med proportionalitets- og nærhedsprincippet. Arbejdsgiverne skal sikre, at de data, der indsamles som led i denne fjernlokalisering, behandles til et bestemt formål og ikke er eller bliver en del af et mere omfattende program med løbende overvågning af de ansatte. Selv til bestemte formål skal sporingen begrænses. Sporingssystemer kan indrettes til

at registrere lokaliseringsdata uden at vise dem til arbejdsgiveren. I så fald skal der kun kunne opnås adgang til lokaliseringsdataene, hvis udstyret mistes eller meldes stjålet.

Ansatte, hvis udstyr er omfattet af MDM-tjenester, skal underrettes fuldt ud om, hvilken sporing der finder sted, og hvilke konsekvenser dette har for dem.

5.4.4 *WEARABLE UDSTYR*

Arbejdsgivere fristes i stigende grad til at udlevere wearable udstyr til deres ansatte med henblik på at spore og overvåge deres helbred og aktivitet på – og nogle gange også uden for – arbejdspladsen. En sådan form for databehandling indebærer imidlertid behandling af oplysninger om helbredsforhold og er derfor ulovlig i henhold til artikel 8 i databeskyttelsesdirektivet.

I lyset af det ulige forhold mellem arbejdsgiver og arbejdstager, hvor arbejdstageren er økonomisk afhængig af arbejdsgiveren, og følsomheden af oplysninger om helbredsforhold er det højst usandsynligt, at der kan gives et retsgyldigt udtrykkeligt samtykke til sporing eller overvågning af sådanne oplysninger, da de ansatte under alle omstændigheder normalt ikke kan give deres samtykke "frit". Selv om arbejdsgiveren får oplysningerne om helbredsforhold indsamlet af en tredjepart, som kun giver arbejdsgiveren aggregerede oplysninger om den generelle udvikling i helbredsforhold, er behandlingen stadig ulovlig.

Som beskrevet i *Udtalelse nr. 05/2014 om anonymiseringsteknikker*[18] er det teknisk meget vanskeligt at sikre fuldstændig anonymisering af data. Selv i et miljø med over 1 000 ansatte vil arbejdsgiveren stadig være i stand til at identificere de enkelte ansatte, som lider af særlige helbredsproblemer såsom forhøjet blodtryk eller overvægt, da han eller hun også har adgang til en række andre oplysninger om de ansatte.

Eksempel

En virksomhed giver sine ansatte fitnessovervågningsudstyr i gave. Udstyret tæller det antal skridt, de ansatte tager, og registrerer deres hjerterytme og søvnmønster over tid.

De resulterende oplysninger om helbredsforhold bør kun være tilgængelige for de ansatte og ikke for arbejdsgiveren. Alle de data, der overføres mellem de ansatte (som registrerede) og udbyderen af udstyret/tjenesten (som registeransvarlig), vedrører kun disse to parter.

Da oplysningerne om de ansattes helbredsforhold også potentielt kan behandles af den kommercielle part, der har fremstillet udstyret, eller som udbyder tjenesten til arbejdsgiveren, skal arbejdsgiveren evaluere fabrikantens og/eller tjenesteudbyderens politik for beskyttelse af privatlivets fred for at sikre, at der ikke sker ulovlig behandling af oplysningerne om de ansattes helbredsforhold.

5.5 Behandlingsaktiviteter vedrørende tid og tilstedeværelse

Systemer, der giver arbejdsgiverne mulighed for at bestemme, hvem der må komme ind i deres virksomhed og/eller visse områder af deres virksomhed, kan også bruges til at spore de ansattes aktiviteter. Disse systemer har ganske vist eksisteret i flere år, men der anvendes i

[18] WP29, *Udtalelse nr. 05/2014 om anonymiseringsteknikker*, WP216, 10. april 2014, url: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_da.pdf.

stigende grad nye teknologier, som er beregnet til at spore de ansattes tid og tilstedeværelse, herunder teknologier, der behandler biometriske data, og andre, som f.eks. kan spore mobilt udstyr.

Mens disse systemer kan udgøre en væsentlig del af en arbejdsgivers revisionsspor, indebærer de også en risiko for, at der indsamles for omfattende viden om og foretages for omfattende kontrol af de ansattes aktiviteter på arbejdspladsen.

Eksempel

En arbejdsgiver har et serverrum, hvor forretningsfølsomme oplysninger samt personoplysninger om ansatte og kunder lagres i digital form. For at overholde de retlige forpligtelser til at sikre dataene mod uautoriseret adgang har arbejdsgiveren installeret et adgangskontrolsystem, der registrerer indgange og udgange for de ansatte, der har behørig tilladelse til at komme i rummet. Såfremt noget af udstyret fjernes, eller uautoriserede personer opnår adgang til nogle af dataene, eller disse mistes eller bliver stjålet, giver det register, som arbejdsgiveren fører, mulighed for at fastslå, hvem der havde adgang til rummet på det pågældende tidspunkt.

Da denne behandling er nødvendig og vejer tungere end de ansattes ret til privatliv, kan den forfølge en legitim interesse, jf. artikel 7, litra f), hvis de ansatte er blevet behørigt underrettet om behandlingen. Løbende overvågning af hyppigheden af og de nøjagtige tidspunkter for de ansattes indgange og udgange er imidlertid ikke berettiget, hvis dataene også anvendes til andre formål, f.eks. evaluering af de ansattes arbejdsindsats.

5.6 Behandlingsaktiviteter ved hjælp af videoovervågningssystemer

Videoovervågning og -tilsyn skaber stadig de samme problemer med krænkelse af de ansattes ret til privatliv som tidligere, idet de gør det muligt at registrere arbejdstagernes adfærd[19]. De mest relevante ændringer i anvendelsen af denne teknologi i ansættelsesforhold er muligheden for uhindret fjernadgang til de indsamlede data (f.eks. via en smartphone), de mindre kameraer (og de øgede muligheder, de indebærer, f.eks. højopløsning) og den behandling, der kan foretages med nye videoanalyser.

Med de muligheder, som videoanalyse giver, kan arbejdsgiveren overvåge arbejdstagernes ansigtsudtryk automatisk for at identificere afvigelser fra forud fastlagte bevægelsesmønstre (f.eks. på en fabrik) osv. Dette er uforholdsmæssigt i forhold til de ansattes rettigheder og frihedsrettigheder og derfor generelt ulovligt. En sådan behandling vil sandsynligvis også involvere profilering og eventuelt automatiske afgørelser. Derfor bør arbejdsgiverne afholde sig fra at anvende teknologier til ansigtsgenkendelse. Der kan være enkelte undtagelser fra denne regel, men de scenarier kan ikke bruges som belæg for, at det generelt er legitimt at anvende sådanne teknologier[20].

5.7 Behandlingsaktiviteter, som involverer de køretøjer, de ansatte bruger

[19] Se ovenstående henvisning til sagen *Köpke mod Tyskland*. Det skal desuden bemærkes, at det i nogle retskredse er blevet erklæret lovligt at installere systemer som f.eks. tv-overvågning med henblik på at dokumentere ulovlig adfærd, jf. sagen *Bershka* ved den spanske forfatningsdomstol.

[20] Derudover skal behandling af biometriske data til identifikationsformål tage udgangspunkt i en undtagelse i henhold til artikel 9, stk. 2, i den generelle forordning om databeskyttelse.

Teknologier, der giver arbejdsgiverne mulighed for at overvåge deres køretøjer, er vidt udbredt, især i transportvirksomheder og virksomheder med store vognparker.

Arbejdsgivere, der anvender køretøjstelematik, indsamler data om både køretøjet og den enkelte ansatte, der bruger det pågældende køretøj. Disse data kan omfatte ikke blot køretøjets (og dermed den ansattes) position, som indsamles via almindelige GPS-sporingssystemer, men også en lang række andre oplysninger, såsom kørselsadfærd, alt afhængig af den anvendte teknologi. Visse teknologier gør det også muligt løbende at overvåge såvel køretøjet som føreren (f.eks. systemer, der registrerer data vedrørende hændelser).

En arbejdsgiver kan være forpligtet til at installere sporingsteknologi i køretøjer for at overholde andre retlige forpligtelser, f.eks. for at garantere de ansattes sikkerhed, når de kører i de pågældende køretøjer. Arbejdsgiveren kan desuden have en legitim interesse i altid at kunne lokalisere køretøjerne. Selv om arbejdsgiveren har en legitim interesse i at nå disse mål, skal det først vurderes, hvorvidt behandlingen til disse formål er nødvendig, og hvorvidt den faktiske implementering er i overensstemmelse med proportionalitets- og nærhedsprincippet. Når ansatte har lov til at anvende firmabiler privat, er den primære foranstaltning, som en arbejdsgiver kan iværksætte for at overholde disse principper, en opt-out-løsning. De ansatte bør i princippet have mulighed for at slukke midlertidigt for lokaliseringsudstyret, når særlige omstændigheder berettiger det, herunder f.eks. i forbindelse med et lægebesøg. På den måde kan den ansatte på eget initiativ beskytte visse private lokaliseringsdata. Arbejdsgiveren skal sikre, at de indsamlede data ikke udsættes for ulovlig viderebehandling, herunder sporing og evaluering af de ansatte.

Derudover skal arbejdsgiveren klart underrette de ansatte om, at der er installeret sporingsudstyr i de firmabiler, de kører i, og at deres bevægelser registreres, når de benytter bilerne (og at deres kørselsadfærd muligvis også registreres, alt afhængig af den anvendte teknologi). Det bedste er, at disse oplysninger sættes op i samtlige biler inden for førerens synsfelt.

Det er muligt, at de ansatte bruger firmabilerne uden for arbejdstiden, f.eks. til privat kørsel, alt efter de specifikke politikker, der gælder for brugen af de pågældende køretøjer. I lyset af lokaliseringsdataenes følsomhed er det usandsynligt, at der findes et retsgrundlag for at overvåge de ansattes køretøjers position uden for arbejdstiden. Skulle det imidlertid være nødvendigt, skal det overvejes at anvende en teknologi, der står i et rimeligt forhold til risikoen. Dette kunne f.eks. betyde, at en bils position, der registreres for at undgå tyveri, ikke registreres uden for arbejdstiden, medmindre køretøjet forlader et større fastlagt område (en region eller måske endda et land). Derudover vil positionen kun blive vist i nødstilfælde, idet arbejdsgiveren først gør positionen synlig, når køretøjet forlader det fastlagte område, ved at skaffe sig adgang til de data, systemet allerede har lagret.

Som nævnt i WP29 *Udtalelse nr. 13/2011 om geolokaliseringstjenester i intelligente mobile enheder*[21]:

"Bilsporingsenheder er ikke medarbejdersporingsudstyr. Deres funktion er at spore eller monitorere positionen af de køretøjer, hvori de er installeret. Arbejdsgivere må ikke betragte

[21] WP29, *Udtalelse nr. 13/2011 om geolokaliseringstjenester i intelligente mobile enheder*, WP185, 16. maj 2011, url: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp185_da.pdf.

dem som enheder til sporing eller monitorering af føreres eller andre medarbejderes adfærd eller færden, f.eks. ved at sende meddelelser vedrørende køretøjets hastighed."

Og som der står i *Udtalelse 5/2005 om brug af lokaliseringsdata med henblik på at yde tillægstjenester*[22]:

"Behandling af lokaliseringsdata kan retfærdiggøres, hvis det sker som led i overvågning af person- eller godstransport eller forbedring af ressourcefordeling for tjenester i spredte områder (f.eks. driftsplanlægning i realtid), eller hvis det sker af hensyn til den ansattes sikkerhed eller de varer eller køretøjer, som han eller hun er ansvarlig for. Omvendt finder gruppen, at databehandlingen går for vidt, hvis medarbejderne under alle omstændigheder frit kan organisere deres rejseaktivitet, eller hvis det sker med det ene formål at overvåge den ansattes arbejde, når dette kan gøres på anden vis."

5.7.1 SYSTEMER TIL REGISTRERING AF DATA VEDRØRENDE HÆNDELSER

Systemer til registrering af data vedrørende hændelser giver arbejdsgiverne teknisk mulighed for at behandle en stor mængde personoplysninger om de ansatte, der bruger firmabilerne. Sådanne enheder anbringes i stigende grad i køretøjerne med det formål at lave videooptagelser, eventuelt med lyd, hvis der sker et uheld. Systemerne kan optage på bestemte tidspunkter, f.eks. ved pludselig opbremsning, voldsomme retningsskift eller uheld, hvor de lagrer sekunderne umiddelbart før, hændelsen indtræder, men de kan også indstilles til løbende overvågning. De indsamlede oplysninger kan efterfølgende bruges til at observere og korrigere en persons kørselsadfærd med henblik på at forbedre den. Desuden omfatter mange af disse systemer en GPS til sporing af køretøjets position i realtid, og det er muligt at lagre andre oplysninger vedrørende kørslen (såsom køretøjets hastighed) til videre behandling.

Dette udstyr anvendes især ofte i transportvirksomheder og virksomheder med store vognparker. Anvendelsen af systemer til registrering af data vedrørende hændelser er imidlertid kun lovlig, hvis det er nødvendigt at behandle de indsamlede personoplysninger om de ansatte til et legitimt formål, og behandlingen sker i overensstemmelse med proportionalitets- og nærhedsprincippet.

Eksempel

Et transportfirma udstyrer alle dets køretøjer med et videokamera i førerhuset, som optager billede og lyd. Formålet med at behandle disse data er at forbedre de ansattes køreevner. Kameraerne er konfigureret til at lagre optagelser, når der indtræder hændelser som f.eks. pludselige opbremsninger eller voldsomme retningsskift. Firmaet regner med, at det har et retsgrundlag for behandlingen i kraft af dets legitime interesse i, jf. artikel 7, litra f), i direktivet, at beskytte de ansattes og andre føreres sikkerhed.

Firmaets legitime interesse i at overvåge førerne har imidlertid ikke forrang over førernes ret til beskyttelse af personoplysninger. Løbende overvågning af de ansatte med sådanne kameraer udgør et alvorligt indgreb i deres ret til privatliv. Der findes andre metoder (f.eks. installation af udstyr, der forhindrer brug af mobiltelefon) og andre sikkerhedssystemer

[22] WP29, *Udtalelse 5/2005 fra Artikel 29-gruppen om brug af lokaliseringsdata med henblik på at yde tillægstjenester*, WP115, 25. november 2005, url: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2005/wp115_da.pdf.

(f.eks. et avanceret nødbremsesystem eller et vognbaneskiftalarmsystem) til forebyggelse af uheld, som kan være bedre egnet. Desuden er der stor sandsynlighed for, at en sådan videooptagelse resulterer i behandling af personoplysninger vedrørende tredjeparter (såsom fodgængere), og i så fald er firmaets legitime interesse ikke nok til at retfærdiggøre behandlingen.

5.8 Behandlingsaktiviteter, der involverer offentliggørelse af oplysninger om ansatte til tredjeparter

Det er blevet mere og mere almindeligt, at virksomheder sender oplysninger om deres ansatte til kunderne med det formål at garantere pålidelig levering af en tjeneste. Disse oplysninger kan være alt for omfattende, alt afhængig af omfanget af de leverede tjenester (der kan f.eks. være indsat et billede af den ansatte). På grund af magtubalancen kan de ansatte imidlertid ikke give et frit samtykke til arbejdsgiverens behandling af deres personoplysninger, og hvis ikke databehandlingen står i et rimeligt forhold til målet, har arbejdsgiveren ikke noget retsgrundlag herfor.

Eksempel

Et budfirma sender en e-mail til sine kunder med et link til buddets (den ansattes) navn og position. Firmaet ville også indsætte et pasbillede af buddet, idet det gik ud fra, at det havde et retsgrundlag for denne behandling i kraft af dets legitime interesse (artikel 7, litra f), i direktivet) i, at kunden kunne tjekke, om buddet rent faktisk var den rigtige person.

Det er imidlertid ikke nødvendigt at sende buddets navn og billede til kunden. Eftersom der ikke er nogen legitim grund til denne behandling, har budfirmaet ikke lov til at videregive disse personoplysninger til kunderne.

5.9 Behandlingsaktiviteter, der involverer internationale overførsler af HR-oplysninger og andre oplysninger om de ansatte

Arbejdsgiverne anvender i stigende grad cloud-baserede applikationer og tjenester, f.eks. dem, der er beregnet til håndtering af HR-oplysninger, og online kontorapplikationer. Anvendelsen af de fleste af disse applikationer resulterer i international overførsel af data fra og vedrørende de ansatte. Som tidligere nævnt i udtalelse 8/2001 fastlægges det i artikel 25 i direktivet, at overførsler af personoplysninger til et tredjeland uden for EU kun må finde sted, hvis det pågældende tredjeland sikrer et tilstrækkeligt beskyttelsesniveau. Overførslerne skal ske i overensstemmelse med direktivets bestemmelser, uanset baggrunden herfor.

Det skal således sikres, at disse bestemmelser om internationale dataoverførsler bliver overholdt. WP29 gentager sin tidligere holdning om, at det er bedre at sikre tilstrækkelig beskyttelse end at henvise til undtagelserne i artikel 26 i databeskyttelsesdirektivet. Når samtykke gøres gældende, skal det være givet specifikt, utvetydigt og frit. Det skal imidlertid også sikres, at de data, der sendes ud af EU/EØS, og den efterfølgende adgang, som koncernens øvrige enheder får til dataene, begrænses til det, der er strengt nødvendigt for det påtænkte formål.

6. Konklusioner og anbefalinger

6.1 Grundlæggende rettigheder

Indholdet af ovenstående kommunikation og de trafikdata, der vedrører denne kommunikation, nyder den samme beskyttelse af de grundlæggende rettigheder som "analog" kommunikation.

Elektronisk kommunikation, der finder sted på arbejdspladser, kan være omfattet af begreberne "privatliv" og "korrespondance", jf. artikel 8, stk. 1, i den europæiske konvention. På baggrund af det nuværende databeskyttelsesdirektiv kan arbejdsgivere kun indsamle data til legitime formål, og behandlingen skal ske under passende forhold (skal f.eks. være forholdsmæssig og nødvendig, være af reel og aktuel interesse og ske på en lovlig, klar og gennemsigtig måde) og med et gyldigt retsgrundlag for behandling af personoplysninger indsamlet fra eller genereret via elektronisk kommunikation.

Det forhold, at en arbejdsgiver er ejer af de elektroniske midler, udelukker ikke, at de ansatte har ret til kommunikationshemmelighed, hemmeligholdelse af de tilhørende lokaliseringsdata og korrespondancehemmelighed. Sporing af de ansattes position via deres eget eller det af virksomheden udleverede udstyr bør begrænses til det, der er strengt nødvendigt for et legitimt formål. I forbindelse med Bring Your Own Device er det særdeles vigtigt, at de ansatte får mulighed for at beskytte deres private kommunikation mod enhver form for arbejdsrelateret overvågning.

6.2 Samtykke – legitim interesse

Ansatte er stort set aldrig i stand til frit at give, afvise at give eller trække et samtykke tilbage som følge af det afhængighedsforhold, der består mellem arbejdsgiver og arbejdstager. I lyset af denne magtubalance kan ansatte kun give et frit samtykke under særlige omstændigheder, når det at acceptere eller afvise et tilbud overhovedet ikke har nogen konsekvenser.

Arbejdsgivernes legitime interesse kan nogle gange gøres gældende som retsgrundlag, men kun hvis behandlingen er strengt nødvendig for et legitimt formål og sker i overensstemmelse med proportionalitets- og nærhedsprincippet. Der bør foretages en proportionalitetstest forud for indførelsen af et overvågningsværktøj for at se på, om alle dataene er nødvendige, om behandlingen vejer tungere end den overordnede ret til privatliv, som ansatte også har på deres arbejdsplads, og hvilke foranstaltninger der skal træffes for at sikre, at krænkelser af retten til privatliv og kommunikationshemmelighed begrænses til et minimum.

6.3 Gennemsigtighed

De ansatte skal underrettes effektivt om al overvågning, der måtte finde sted, om formålet med og forholdene omkring denne overvågning samt om de muligheder, de har for at forhindre, at deres data bliver opfanget af overvågningsteknologier. Politikker og regler vedrørende legitim overvågning skal være klare og umiddelbart tilgængelige. Arbejdsgruppen anbefaler, at et repræsentativt udsnit af de ansatte inddrages i udarbejdelsen og evalueringen af sådanne regler og politikker, da de fleste former for overvågning har potentiale til at krænke de ansattes ret til privatliv.

6.4 Proportionalitet og dataminimering

Databehandling på arbejdspladsen skal stå i et rimeligt forhold til de risici, en arbejdsgiver løber. Internetmisbrug kan f.eks. detekteres, uden at det er nødvendigt at analysere et

websteds indhold. Hvis misbruget kan forebygges (f.eks. ved anvendelse af webfiltre), har arbejdsgiveren ikke nogen overordnet ret til at foretage overvågning.

Derudover er et totalforbud mod personlig kommunikation upraktisk, og håndhævelsen heraf kan kræve et uforholdsmæssigt overvågningsniveau. Der skal lægges mere vægt på at forebygge end på at detektere – arbejdsgiverens interesser tilgodeses bedre ved at forebygge internetmisbrug med tekniske midler end ved at bruge ressourcer på at detektere et misbrug.

De oplysninger, der registreres under den løbende overvågning, og dem, der bliver vist til arbejdsgiveren, skal begrænses til et minimum. De ansatte skal have mulighed for midlertidigt at slukke for lokaliseringsudstyr, når omstændighederne berettiger det. Løsninger, der f.eks. sporer køretøjer, kan indrettes til at registrere lokaliseringsdata uden at vise dem til arbejdsgiveren.

Arbejdsgiverne skal tage hensyn til princippet om dataminimering, når de beslutter sig for at indføre nye teknologier. Oplysningerne må ikke lagres længere end højst nødvendigt inden for en bestemt opbevaringsperiode. Når oplysningerne ikke længere er nødvendige, skal de slettes.

6.5 Cloud-tjenester, online applikationer og internationale overførsler

Når de ansatte forventes at anvende online applikationer, som behandler personoplysninger (såsom online kontorapplikationer), skal arbejdsgiverne overveje at give de ansatte mulighed for at udpege visse private områder, som arbejdsgiverne under ingen omstændigheder har adgang til, f.eks. en privat e-mail- eller dokumentmappe.

Anvendelsen af de fleste cloud-applikationer resulterer i international overførsel af oplysninger om de ansatte. Det skal sikres, at overførsler af personoplysninger til et tredjeland uden for EU kun finder sted, hvis det pågældende tredjeland sikrer et tilstrækkeligt beskyttelsesniveau, og at de data, der sendes ud af EU/EØS, og den efterfølgende adgang, som koncernens øvrige enheder får til dataene, begrænses til det, der er strengt nødvendigt for det påtænkte formål.

* * *

Udfærdiget i Bruxelles, den 8. juni 2017

På Artikel 29-gruppens vegne
Formand
Isabelle FALQUE-PIERROTIN