PROSA den 17/4-2007

Til

Folketingets

Retsudvalget

Christiansborg

Vedr. Problemer i forbindelse med implementering af Terrorloven

PROSA – Forbundet af It-professionelle, har fået en række henvendelser fra medlemmer der er ansat hos tele- og internetudbyderme. Det har nu vist sig, at it-ansatte, der skal deltage i arbejdet med at logge teledata i forbindelse med Terrorloven, skal sikkerhedsgodkendes i kategorien ”Yderst Hemmelig” .

”Yderst Hemmelig” er den højeste militære kategori for sikkerhedsgodkendelse svarende til NATO klassifikationen ”Cosmic Top Secret”.

Vi har ikke grundlag for at vurdere, om det faktisk er nødvendigt, at disse personer sikkerhedsgodkendes på det niveau, som PET stiller krav om. Men da den højeste kategori stiller meget omfattende krav både til den enkelte person og omkring behandling af data (se uddrag af ”Cirkulære vedrørende sikkerhedsbeskyttelse”), mener vi, at man igen bør overveje, om det er nødvendigt, at niveauet altid skal ligge så højt og hvor mange der er behov for, skal være omfattet.

Det er på grundlag af de sager, vi har set, vores opfattelse at PET i praksis overlader det til arbejdsgiverne at vurdere, hvor mange personer, der er behov for at få sikkerhedsgodkendt. Det er vores opfattelse, at antallet af personer, der skal sikkerhedsgodkendes, skal begrænses mest muligt, i overensstemmelse med kravene i henhold til cirkulæret.

Det er imidlertid vores hidtidige erfaring, at arbejdsgiverne foretrækker, at alle i en driftsafdeling, bliver sikkerhedsgodkendt, da dette vil kunne lette den daglige tilrettelæggelse af arbejdet. Dette skal vejes op imod de krav og de gener, der er for medarbejdere ved at blive og være sikkerhedsgodkendt på dette niveau. På denne baggrund vil vi anmode om, at man igen overvejer at stille krav om at reducere antallet af personer, der skal sikkerhedsgodkendes på dette niveau.

Den 19. marts skrev vi til PET (vedlagt som bilag), fordi det fremgår af deres godkendelsesskema og den tilhørende vejledning, at arbejdsgiveren skal underskrive et ansøgningsskema – der indeholder mange fortrolige og private oplysninger, som er et normalt ansættelsesforhold uvedkommende (rejser, medlemskab af lovlige foreninger, gæld m.m. og til dels seksuel orientering, idet ens samlever skal oplyses).

Vi mener ikke, at der er nogen form for argumentation for, at arbejdsgiveren skal have disse oplysninger. Det er også i strid med, hvad PET selv har udmeldt i en pressemeddelelse om spørgsmålet. Vi mener desuden også, at det er i strid med Persondataloven, at PET forlanger, at en lønmodtager skal give alle disse oplysninger til sin arbejdsgiver. Vi bemærker, at konsekvensen af at sige nej til at give sin arbejdsgiver disse oplysninger er, at man ikke kan udføre det ønskede arbejde og i yderste konsekvens mister sit arbejde. Denne risiko er i sagens natur større, jo flere der kræves sikkerhedsgodkendt.

Vi har derfor opfordret PET til at ændre proceduren. Men har nu næsten en måned senere fortsat ikke fået nogen form for svar på vores henvendelse. Dette mener vi selvfølgelig er utilfredsstillende, ikke mindst fordi godkendelserne i stort tal netop nu pågår og de, der skal sikkerhedsgodkendes, således helt ubegrundet, i strid med love og regler og med risiko for ubehagelige konsekvenser leverer disse oplysninger til deres arbejdsgiver.

Så vidt vi har forstået gennem telefonisk kontakt til PET, er begrundelsen for arbejdsgiverens underskrift alene, at man ønsker en tilkendegivelse fra arbejdsgiveren på, at det er rigtigt, at den omhandlede medarbejder ønskes sikkerhedsgodkendt. Det er vores opfattelse, at denne tilkendegivelse må kunne foretages på et særskilt dokument.

Vi står gerne til rådighed med henblik på en uddybning.

Med venlig hilsen

PROSA

v/ Hanne Lykke Jespersen

Sikkerhedscirkulære

CIR nr 204 af 07/12/2001

Cirkulære vedrørende sikkerhedsbeskyttelse af informationer af fælles interesse for landene i NATO, EU eller WEU, andre klassificerede informationer samt informationer af sikkerhedsmæssig beskyttelsesinteresse i øvrigt

http://www.stm.dk/Index/dokumenter.asp?o=13&n=1&d=1352&s=1&str=stor

A. Informationer af fælles interesse for landene i NATO, EU eller WEU

I. Klassificering

§ 1. Alle informationer mærket med betegnelsen NATO, EU eller WEU samt nationale informationer af fælles interesse for landene i NATO, EU eller WEU skal, i det omfang de kræver sikkerhedsbeskyttelse, klassificeres efter nedenstående regler.

1) YDERST HEMMELIGT (»COSMIC TOP SECRET«, »TRÈS SECRET UE«, »FOCAL TOP SECRET«)

Denne klassifikationsgrad skal anvendes om informationer, hvis videregivelse uden dertil indhentet bemyndigelse ville kunne forvolde Danmark eller landene i NATO, EU eller WEU overordentlig alvorlig skade.

2) HEMMELIGT (»NATO SECRET«, »SECRET UE«, »WEU SECRET«)

Denne klassifikationsgrad skal anvendes om informationer, hvis videregivelse uden dertil indhentet bemyndigelse ville kunne forvolde Danmark eller landene i NATO, EU eller WEU alvorlig skade.

3) FORTROLIGT (»NATO CONFIDENTIAL«, »CONFIDENTIEL UE«, »WEU CONFIDENTIAL«)

Denne klassifikationsgrad skal anvendes om informationer, hvis videregivelse uden dertil indhentet bemyndigelse ville kunne forvolde Danmark eller landene i NATO, EU eller WEU skade.

4) TIL TJENESTEBRUG (»NATO RESTRICTED«, »RESTREINT UE«, »WEU RESTRICTED«)

Denne klassifikationsgrad anvendes om informationer, der ikke må offentliggøres eller komme til uvedkommendes kendskab.

…

IV. Sikkerhedsgodkendelse af elektroniske informationssystemer.

§ 25. Elektronisk behandling af informationer klassificeret YDERST HEMMELIGT kræver i hvert enkelt tilfælde en særskilt tilladelse fra den nationale sikkerhedsmyndighed.

§ 26. Alle former for elektroniske informationssystemer og netværk beregnet til frembringelse, bearbejdning, kommunikation eller lagring af informationer klassificeret HEMMELIGT eller FORTROLIGT skal sikkerhedsgodkendes af den nationale sikkerhedsmyndighed.

§ 27. Nye versioner af programmel til anvendelse i sikkerhedsgodkendte informationssystemer skal sikkerhedsgodkendes af den nationale sikkerhedsmyndighed før ibrugtagning.

§ 28. Kommunikationssystemer (f.eks. telefax, videokonference, og telefon/modem) beregnet til informationer klassificeret TIL TJENESTEBRUG eller højere skal sikkerhedsgodkendes af den nationale sikkerhedsmyndighed.

§ 29. Sikkerhedsgodkendelse efter §§ 26-28 skal sikre, at informationssystemet, netværket m.v. opfylder gældende sikkerhedskrav inden ibrugtagning. Den nationale sikkerhedsmyndighed bør derfor inddrages på det tidligst mulige tidspunkt i forbindelse med planlægning af anskaffelse af elektroniske informationssystemer eller netværk, eller ved ændringer af tidligere godkendte elektroniske informationssystemer eller netværk.

§ 30. Som led i sikkerhedsgodkendelsen påhviler det de enkelte styrelser at udarbejde

systemspecifikke sikkerhedskrav og en sikkerhedsinstruks, der godkendes af den nationale sikkerhedsmyndighed.

Stk. 2. Udarbejdelsen af systemspecifikke sikkerhedskrav skal påbegyndes på et så tidligt tidspunkt i projektet som muligt for derefter at blive revideret og uddybet i takt med projektets udvikling.

Stk. 3. Systemspecifikke sikkerhedskrav er en fuldstændig og nøjagtig beskrivelse af, hvilke sikkerhedsprincipper og sikkerhedskrav der skal opfyldes. Disse krav udgør en integreret del af systemdokumentationen.

…