SKATTEMINISTERIET

j.nr. 07-054162
Dato : 3. april 2007

Til

Folketingets Skatteudvalg

Hermed sendes svar på spørgsmål nr. 202 af 20. marts 2007.
(Alm. del).

Kristian Jensen

/Tina R. Olsen

Spørgsmål 202:
"Kan ministeren oplyse om der i forbindelse med et stigende antal hjemmearbejdspladser i Skat er nogen særlige regler omkring datasikkerhed?"

Svar:
Problemstillingen kan groft sagt deles op i en menneskelig og en teknisk datasikkerhed.

Den menneskelige datasikkerhed varetages primært ved, at alle SKATs medarbejdere er omfattet af tavshedspligt i henhold til skatteforvaltningslovens § 17. Desuden underskriver medarbejderne ved ansættelsen en tavshedserklæring, der medvirker til at gøre medarbejderne opmærksomme på, hvad det er for en type af informationer, de kan få adgang til, og at disse informationers fortrolighed og integritet ikke må brydes.

SKAT er en enhedsforvaltning, og medarbejderne skal kunne yde borgere og virksomheder den optimale service overalt i landet. Der er derfor ikke fra centralt hold lagt tekniske begrænsninger på, hvad den enkelte medarbejder kan få adgang til i SKATs systemer. Det er op til den lokale ledelse at bestemme, hvilke data og it-systemer de enkelte medarbejdere skal have adgang til.

SKAT informerer desuden medarbejderne om, at man udelukkende må tilgå informationer, som er relevante for det daglige arbejde, og SKAT logger alle opslag og ændringer i SKATs informationer.

Den tekniske datasikkerhed varetages ved, at medarbejderen får udleveret en sikkerhedstoken (teknisk anordning), der løbende danner éngangspassword, der benyttes som supplement til medarbejderens bruger-ID og password i forbindelse med hver logon til SKATs systemer.

Derudover underskriver medarbejderen ved modtagelsen af token en erklæring, som sikrer, at medarbejderen ved, at:

- tokenen er personlig, og at PIN-koden til tokenen ikke må oplyses til andre
- bortkommer tokenen, eller er der mistanke om, at PIN-koden til tokenen er kendt af andre, skal SKATs IT-center kontaktes straks
- SKATs informationer ikke må lagres på udstyr, som ikke tilhører SKAT
- medarbejderen sikrer, at udskrevne informationer ikke kan læses eller fjernes af vedkommende.

SKATs hjemmearbejdspladser er teknisk sikrede på en sådan måde, at forbindelsen mellem arbejdspladsen kun kan etableres ved at oplyse bruger-ID, password og éngangspassword. Forbindelsen er krypteret med stærk kryptering, således at

informationerne ikke kan læses af uvedkommende under transporten mellem SKAT og arbejdspladsen. Herudover er alle SKATs hjemmearbejds-pc'eres harddiske krypterede.