

Datatilsynets angivelse af praksis om brug af internettet:

”Denne regel medfører efter Datatilsynets opfattelse bl.a., at der ved tilslutning til internet eller andre åbne net skal træffes foranstaltninger, som sikrer imod uvedkommende trafik og forhindrer adgang fra det åbne net til den dataansvarliges interne net.

Efter Datatilsynets opfattelse bør den dataansvarlige som minimum træffe følgende foranstaltninger:

- Etablering og vedligeholdelse af en firewall, som sikrer gennemførelse af myndighedens sikkerhedspolitik, herunder f.eks. spærring for adgang til suspekte hjemmesider.
- Ajourføring af servere og pc-arbejdspladser med sikkerhedsopdateringer, som sikrer mod ondsindet udnyttelse af sårbarheder i de anvendte programmer.
- Etablering af virusværn, som løbende holdes ajourført. Et virusværn vil bl.a. sikre mod en del af den ondsindede spyware.
- Opsætning af sikkerhedsindstillingerne i browseren og e-post klienten på de enkelte pc-arbejdspladser, således at der opnås den ønskede sikkerhedspolitik omkring websteder, cookies og modtagelse af eksekverbar kode (plug-ins m.v.)

Efter en vurdering af den konkrete sikkerhedsrisiko og under hensyntagen til øvrige sikkerhedsforanstaltninger kan yderligere sikkerhedsforanstaltninger være hensigtsmæssige, herunder f.eks. installation af anti-spyware programmer på de enkelte pc-arbejdspladser.”

Datatilsynet udtaler sig ikke om medarbejdernes adfærd i denne forbindelse.