om persondatabeskyttelse. Det bestemmes, at certificeringstjenesteudbyderen alene må indsamle personoplysninger direkte fra den pågældende person eller med denne persons udtrykkelige samtykke. Personoplysningerne må kun indsamles i det omfang, det er nødvendigt for udstedelsen eller opretholdelsen af et certifikat.

Et åbent marked

Direktivet indeholder et forbud mod forudgående autorisation af nøglecentre som en betingelse for at kunne udbyde certificeringstjenester til elektroniske signaturer.

Ved forudgående autorisation forstås enhver tilladelse, hvis udstedelse forudsætter, at de nationale myndigheder træffer en afgørelse, inden nøglecentret kan udbyde sine certificeringstjenester samt enhver anden foranstaltning med samme virkning.

Dette skal sikre, at nøglecentrene får mulighed for at udbyde deres produkter på tværs af grænserne i hele EU, med det resultat at den samlede konkurrence på dette specielle område styrkes til fordel for forbrugerne og erhvervslivet. De må derved formodes at få tilbudt en række produkter, der kan give nye muligheder for sikker elektroniske informationsudveksling. Et frit marked vil således stimulere udbudet af certificeringstjenesteydelser i hele EU.

Der indføres dog samtidig en pligt for medlemsstaterne til at etablere et passende tilsyn med nøglecentre, der udsteder kvalificerede certifikater til elektroniske signaturer. Der åbnes mulighed for, at medlemsstaterne kan overlade etableringen af sådanne systemer til markedsaktørerne i form af selv-regulering.

Medlemsstaterne skal anerkende certifikater, udstedt af certificeringstjenesteudbydere fra lande uden for EØS, på lige fod med certifikater udstedt af certificeringstjenesteudbydere fra EØS hvis 1) tredjelands-nøglecenter opfylder direktivets krav og er akkrediteret i forbindelse med en frivillig akkrediteringsordning i et EU-land, 2) hvis et EU-nøglecenter, der opfylder direktivets krav, indestår for tredjelandsudbyderens certifikater, eller 3) hvis tredjelands-certifikatet eller tredjelands-udbyderen er anerkendt i henhold til en international aftale.

Retlig anerkendelse af elektroniske signaturer

Direktivet indeholder i et vist omfang regler om retsvirkningerne af elektroniske signaturer. Direktivet indeholder således et forbud mod at »diskriminere« elektroniske signaturer i relation til retskraft og anerkendelse som bevis, alene fordi signaturen er elektronisk eller ikke lever op til visse sikkerhedskrav.

Dette »diskriminationsforbud« indebærer, at medlemsstaterne ikke må frakende elektroniske signaturers retsvirkninger m.v., alene fordi de er i elektronisk form. Forbudet betyder derimod ikke, at medlemsstaterne ikke af andre årsager kan behandle elektroniske signaturer anderledes end håndskrevne underskrifter. Er en elektronisk signatur f.eks. udvirket ved en teknik, som kun yder en meget begrænset beskyttelse mod forfalskninger m.v., vil det således ikke være i strid med »diskriminationsforbudet« at behandle sådanne signaturer anderledes end håndskrevne underskrifter på grund af det lave sikkerhedsniveau.

Direktivet indeholder også en bestemmelse om, at anvendelse af de ovennævnte »avancerede« elektroniske signaturer, dvs. elektroniske signaturer, som lever op til særligt strenge sikkerhedskrav, skal anses for at opfylde formkrav om underskrift på papirdokumenter. Dette gælder dog, hvis en medlemsstat anerkender anvendelsen af elektroniske signaturer i den pågældende sammenhæng.

Det vil, som anført ovenfor således fortsat være op til medlemsstaterne at bestemme, på hvilke områder man vil acceptere brugen af elektronisk kommunikation og elektroniske signaturer. Bestemmelsen indebærer imidlertid, at medlemsstaterne på de områder, hvor man efter national ret stiller krav om signatur på elektroniske meddelelser, skal acceptere, at avancerede elektroniske signaturer opfylder dette krav. Ved kommunikation med det offentlige giver direktivet dog mulighed for, at medlemsstaterne kan stille strengere sikkerhedskrav til de elektroniske signaturer, hvis disse krav er objektive, gennemsigtige, rimelige og ikke-diskriminerende.

Endelig indeholder direktivet en regel om, at medlemsstaterne skal sikre, at »avancerede« elektroniske signaturer kan anvendes som bevis ved retshandlinger. I præamblen til direktivet er det præciseret, at reglerne ikke ændrer på princippet om retternes frie bevisbedømmelse.

Den danske procedure vedrørende direktivet

Direktivforslaget har været forelagt Folketingets Europaudvalg den 15. maj 1998 med Forskningsministeriets notat af 7. maj 1998 forud for Rådsmødet (telekommunikation) den 19. maj 1998.

Direktivforslaget har endvidere været omtalt i Forskningsministeriets samlenotat af 13. november 1998 med henblik på orientering af Folketingets Europaudvalg forud for Rådsmødet (telekommunikation) den 27. november 1998. Direktivforslaget har endvidere været nævnt i referat til Folketingets Europaud-