

ved udskrift på papir eller ved at blive vist på en computerskærm. I modsætning til et papirdokument, der uden videre er læsbart, vil et digitalt dokument således altid skulle gennemgå en behandling, før det kan læses.

Digital kommunikation omfatter bl.a. kommunikation ved brug af e-post (e-mail). Andre former for digital kommunikation kan være anvendelse af webteknologier, hvor der f.eks. kommunikeres med en offentlighed myndighed via myndighedens hjemmeside, eller kommunikation mellem datasystemer uden direkte menneskelig indblanding, f.eks. automatisk overførsel af digitale dokumenter fra en myndighed til en anden.

Med hensyn til betydningen af formkrav i lovgivningen mv. anfører arbejdsgruppen generelt, at krav om skriftlighed og underskrift kan tjene en række forskellige formål. Der kan f.eks. være tale om at skabe sikkerhed for, at en meddelelse stammer fra en bestemt person, eller om forskellige bevisfunktioner, herunder bevissikring af meddelelsens indhold, af at meddelelsen er modtaget eller godkendt, eller af tidspunktet for modtagelsen af meddelelsen. Der henvises til redegørelsen side 21 ff.

Arbejdsgruppen peger på, at en personlig underskrift er med til at give en meddelelse troværdighed. En underskrift på et dokument er som regel udtryk for, at den, der har underskrevet dokumentet, har godkendt dokumentet, herunder f.eks. påtaget sig en forpligtelse i overensstemmelse med dokumentets indhold. Medmindre dokumentet indeholder iøjnefaldende rettelser, vil man endvidere normalt gå ud fra, at dokumentet ikke er ændret efter underskrivelsen.

Ved digital kommunikation kan de tilsvarende krav til meddelelsen sikres ved anvendelse af en såkaldt digital signatur, der kan betragtes som en digital underskrift. En digital signatur bygger på et krypteringssystem, hvorved meddelelsens autencitet (at den stammer fra den angivne afsender) og integritet (at den ikke er ændret undervejs) kan sikres. Der henvises til redegørelsen side 16 ff.

Lov nr. 417 af 31. maj 2000 om elektroniske signaturer indeholder særlige regler om signaturer, som er forbundet med en særlig høj grad af sikkerhed både teknisk og i forbindelse med udstedelsen af det certifikat, der er knyttet til signaturen – de såkaldte »kvalificerede certifikater«. Ved siden heraf findes en række ikke-kvalificerede signaturer, hvor der f.eks. ikke stilles de samme krav til proceduren i forbindelse med udstedelsen af det certifikat, der er knyttet til den digitale signatur. Det kan i den forbindelse nævnes, at Ministeriet for Videnskab, Teknologi og Udvikling har

forestået udviklingen af den såkaldte OCES-standard (Certifikatpolitik for Offentlige Certifikater til Elektronisk Service), som er udtryk for den offentlige politik for anvendelse af digitale signaturer ved kommunikation med det offentlige. Der henvises til redegørelsen side 18.

2.3. Persondataloven

Lov nr. 429 af 31. maj 2000 om behandling af personoplysninger (persondataloven) gælder bl.a. for behandling af personoplysninger, som helt eller delvist foretages ved hjælp af elektronisk databehandling, jf. lovens § 1, stk. 1. Persondataloven omfatter enhver form for information om en identificerbar fysisk person. Loven gælder også for domstolenes behandling af personoplysninger.

Efter persondatalovens § 41, stk. 3, skal den dataansvarlige og databehandleren træffe de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at personoplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes, samt mod, at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med loven.

I medfør af persondatalovens § 41, stk. 1, har Justitsministeriet udstedt bekendtgørelse nr. 528 og nr. 535 af 15. juni 2000 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles henholdsvis af den offentlige forvaltning og domstolene. Eksterne kommunikationsforbindelser må efter § 14 i bekendtgørelserne kun etableres, hvis der træffes særlige foranstaltninger for at sikre, at uvedkommende ikke gennem disse forbindelser kan få adgang til personoplysninger.

Om denne bestemmelse hedder det i Datatilsynets vejledning af 2. april 2001 til bekendtgørelse nr. 528 af 15. juni 2000 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning, bl.a.:

»Bestemmelsen gælder enhver form for telekommunikation i forbindelse med behandling af personoplysninger, f.eks. forsendelse af oplysninger med telefax eller ekstern e-post, etablering af terminaladgang ved opkaldsmodem, adgang til oplysninger via myndighedens hjemmeside og etablering af internetadgang fra arbejdspladser på myndighedens interne net. De særlige sikkerhedsforanstaltninger skal træffes efter myndighedens vurdering af sikkerhedsrisici i det konkrete tilfælde, herunder med hensyntagen til karakteren af de omhandlede oplysninger...

Ved tilslutning til Internet eller andre åbne net skal der træffes foranstaltninger, som sikrer imod uved-