

Notat  
om

Sikkerhed ved transmission af personoplysninger via internettet i den private sektor

---

- 1. Baggrund**
- 2. Persondataloven og andre regler**
- 3. Datatilsynets praksis**
- 4. Datatilsynets foreløbige overvejelser**

## **1. Baggrund**

Datatilsynet er den statslige myndighed, der administrerer [lov om behandling af personoplysninger \(i daglig tale blot persondataloven\)](#)<sup>1</sup>. Som led heri behandler Datatilsynet bl.a. klagesager og besvarer forespørgsler, udtaler sig om lovforslag og udkast til bekendtgørelser og cirkulærer mv., foretager inspektioner samt foretager undersøgelser af egen drift overfor myndigheder, virksomheder og organisationer, når tilsynet bliver bekendt med mulige brud på loven. Datatilsynet fører tilsyn med enhver behandling, der er omfattet af persondataloven, bortset fra domstolenes handlinger.

Det er forudsat i de almindelige bemærkninger til persondataloven, at Datatilsynet i første række bør tage sigte på at kunne udøve sin virksomhed gennem generelle retningslinier og ved en serviceorienteret rådgivning og vejledning.

Spørgsmålet om sikkerhedskrav i forbindelse med transmission af personoplysninger via internettet indgår ofte i tilsynets sager. Det indgår i klagesager, som registrerede personer rejser ved tilsynet. Det indgår i tilsynets høringssvar over love og bekendtgørelse. Tilsynet stiller spørgsmål til dette under inspektioner og i forbindelse med egen-drift sager. Og sidst – men ikke mindst – kommer dette spørgsmål op, når tilsynet giver vejledning til virksomheder, organisationer og myndigheder om, hvordan de skal indrette sig for at efterleve persondataloven.

Datatilsynet har på denne baggrund behov for at fastlægge, hvilke sikkerhedskrav der fremover skal stilles til private dataansvarlige i forbindelse med transmission af fortrolige eller følsomme personoplysninger over det åbne internet.

---

<sup>1</sup> Lov nr. 429 af 31. maj 2000 om behandling af personoplysninger med senere ændringer.

I afsnit 2 i dette notat beskrives de regler i persondataloven, som er grundlaget for, at personoplysninger skal beskyttes med passende sikkerhedsforanstaltninger ved transmission over internet. I afsnittet beskrives endvidere regler i anden lovgivning, der stiller krav til private dataansvarlige, herunder e-handelsloven.

Tilsynet har allerede udtalt sig om kravene til sikkerheden i en række tilfælde. Tilsynets hidtidige praksis gengives i notatets afsnit 3.

I afsnit 4 findes Datatilsynets foreløbige overvejelser om, hvorvidt den hidtidige praksis skal fastholdes.

Tilsynets overvejelser skal bl.a. ses i lyset af den debat, der blev udløst efter tilsynets besvarelse af forskellige spørgsmål fra Biblioteksstyrelsen.

### **1.1. Datatilsynets udtalelse til Biblioteksstyrelsen**

I et brev af 12. juli 2005 besvarede Datatilsynet en henvendelse fra Biblioteksstyrelsen. Biblioteksstyrelsen havde bl.a. spurgt, om det i forbindelse med bestilling i bibliotek.dk er korrekt at anvende ikke-krypteret e-mail til fremsendelse af kvittering for afgivne bestillinger indeholdende titel på det bestilte materiale.

Oplysninger om en borgers bibliotekslån er en fortrolig oplysning. I overensstemmelse med sikkerhedsvejledningen svarede Datatilsynet derfor Biblioteksstyrelsen, at fremsendelse af elektroniske reserveringsmeddelelser, der indeholder titel og forfatter på det reserverede materiale, kræver kryptering.

Sagen gav anledning til en del omtale og debat, og Datatilsynet valgte efterfølgende at gøre en særlig undtagelse fra de sikkerhedskrav, som tilsynet generelt stiller til offentlige myndigheder. Undtagelsen gælder foreløbig i en periode på 5 år, hvor tilsynet således accepterer, at bibliotekerne fortsætter med at sende ukrypterede e-mails med oplysninger om reserverede bøger.

### **1.2. Datatilsynets udtalelse om kryptering i den private sektor**

I udtalelsen til Biblioteksstyrelsen besvarede Datatilsynet også et spørgsmål om, hvad der gælder for e-boghandlers udsendelse af e-post-kvittering. Datatilsynet tilkendegav – i overensstemmelse med sin hidtidige praksis – at sikkerhedskravet om kryptering bør følges, både når den dataansvarlige er en offentlig myndighed, og når der er tale om en privat virksomhed.

Datatilsynets udtalelse medførte en række henvendelser fra borgere, der ønskede at få oplyst, hvad der gælder i en lang række tilfælde, hvor private dataansvarlige transmitterer personoplysninger over det åbne internet.

Der er i den forbindelse bl.a. spurgt til e-mail-kvitteringer ved køb af bøger og musik ved internetboghandler eller musikbutikker, e-mail-kvitteringer for køb af andre varegrupper på nettet, hvor forbrugeren modtager en ukrypteret kvitteringsmail, modtagelse af ukrypterede nyhedsbreve, e-mails fra internetsteder med anbefaling af andre varer, som kan være af interesse for forbrugeren, samt fremsendelse af e-mails indeholdende oplysninger om brugernavn og password.

Foranlediget af sagen kom Datatilsynet endvidere i dialog med forskellige brancheorganisationer, og der blev fra flere sider stillet spørgsmålstejn ved de krav, der fulgte af tilsynets hidtidige praksis.

Datatilsynet besluttede herefter at afklare, hvilke sikkerhedskrav der fremover skal stilles til private dataansvarlige i forbindelse med transmission af fortrolige eller følsomme personoplysninger over det åbne internet.

Som et led i denne proces har tilsynet udformet dette notat til brug for en høring af myndigheder, brancheorganisationer mv. Notatet og høringen er desuden tilgængelige på Datatilsynets hjemmeside – [www.datatilsynet.dk](http://www.datatilsynet.dk)

## **2. Persondataloven og andre regler**

### **2.1. Persondatalovens sikkerhedskrav**

Persondatalovens kapitel 11 indeholder regler om behandlingssikkerhed.

I § 41, stk. 1, er det fastsat, at personer, virksomheder mv., der udfører arbejde under den dataansvarlige eller databehandleren, og som får adgang til oplysninger, kun må behandle disse efter instruks fra den dataansvarlige, med mindre andet følger af lov eller bestemmelser fastsat i henhold til lov.

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

Persondatalovens krav om datasikker bygger på artikel 17 i databeskyttelsesdirektivet fra 1995: [Europaparlamentet og Rådets direktiv af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger](#)<sup>2</sup>.

Det er forudsat, at sikkerhedsforanstaltningerne under hensyn til det aktuelle tekniske niveau og de omkostninger, som er forbundet med deres iværksættelse, skal tilvejebringe et tilstrækkeligt sikkerhedsniveau i forhold til de risici, som behandlingen indebærer, og arten af de oplysninger, som skal beskyttes, jf. direktivets artikel 17, stk. 1, 2. afsnit.

Det er endvidere forudsat, at gennemførelsen af databeskyttelsesdirektivet ikke må medføre en forringelse af den beskyttelse, som registerlovgivningen ydede, jf. direktivets betragtning 10.

Det er endvidere fremhævet, at iværksættelsen af de fornødne sikkerhedsforanstaltninger er særligt påkrævet, hvis behandlingen omfatter fremsendelser af oplysninger i et net, jf. herved direktivets artikel 17, stk. 1, 1. afsnit.

---

<sup>2</sup> Direktiv 95/46/EF

I forbindelse med gennemførelsen af databeskyttelsesdirektivet skulle det af Justitsministeriet nedsatte Udvalg om Registerlovgivningen dels på baggrund af direktivet dels i lyset af den tekniske udvikling udforme et forslag til ny lovgivning om beskyttelse af personoplysninger mv.

I lovforslaget til persondataloven<sup>3</sup> er udvalgets forslag gengivet. Det fremgår bl.a., at udvalget finder, at sikkerhedsforanstaltningerne grundlæggende bør indeholde følgende elementer: Fysisk sikkerhed, organisatoriske forhold, systemtekniske forhold, samt uddannelse og instruktion.

Samtidig pegede Registerudvalget navnlig på følgende sikkerhedsforanstaltninger, der – alt efter omstændighederne – kan komme på tale: Sikring af bygninger og lokaler, formel autorisation af brugerne, adgangskoder (password), benyttelsesstatistik, logning af transaktioner, registrering af uautoriserede adgangsforsøg, kryptering, regler for udskrifter, regler for destruktions, uddannelse samt tilsyn.

I lovforslaget til persondatalovens, afsnit 4.2.12. ”Særligt om ny informationsteknologi” beskrives gældende ret i afsnit 4.2.12.1. Det fremgår bl.a., at Registertilsynet i sin praksis f.eks. har udtalt sig om kryptering i forbindelse med forsendelse af elektronisk post via internettet.

Af afsnit 4.2.12.2. om udvalgets overvejelser fremgår bl.a., at registerudvalget bemærkede, at den moderne informationsteknologi medfører stærkt forbedrede kommunikationsmuligheder, som det med tiden vil være naturligt at anvende med henblik på en faktisk styrkelse af den databeskyttelsesretlige regulering. Internettet og tilsvarende netværk bør i den forbindelse spille en fremtrædende rolle, idet denne teknologi bør nyttiggøres, så snart mulighederne herfor er tilstrækkeligt sikre og de dataansvarlige og tilsynsmyndighederne må forventes at være i stand til udnytte teknologien.

I lovforslaget tiltrådte Justitsministeriet, at der ikke efter lovgivningen pålægges de dataansvarlige en pligt til at anvende nærmere bestemte former for informationsteknologi, f.eks. internettet, i forbindelse med behandling af oplysninger. Justitsministeriet fandt det – ligesom registerudvalget – naturligt, at det overlades til de berørte myndigheder, virksomheder mv. selv at vurdere, om de fornødne rammer for at tage edb-tekniske hjælpemidler i brug er til stede. Det blev samtidig anført, at Registertilsynet har oprettet en hjemmeside på internettet, som indeholder information om en række forhold, herunder bl.a. om Registertilsynet, om lovgivningen samt om publikationer og rapporter.

## **2.2. Sikkerhedsbekendtgørelsen med tilhørende vejledninger**

En udmøntning af princippet i § 41, stk. 3, er for den offentlige forvaltning bl.a. sket i sikkerhedsbekendtgørelsen<sup>4</sup>.

Af sikkerhedsbekendtgørelsens § 14 fremgår, at der kun må etableres eksterne kommunikationsforbindelser, hvis der træffes særlige foranstaltninger for at sikre, at uvedkommende ikke gennem disse forbindelser kan få adgang til personoplysninger.

<sup>3</sup> L 147, Folketingsåret 1999-2000

<sup>4</sup> Bekendtgørelse nr. 528 af 15. juni 2000 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning. Bekendtgørelsen kan læses på Datatilsynets hjemmeside, [www.datatilsynet.dk](http://www.datatilsynet.dk), under punktet ”Lovgivning”.

I Datatilsynets sikkerhedsvejledning<sup>5</sup> er det nærmere angivet, hvorledes sikkerhedsbekendtgørelsens krav vil kunne opfyldes. Det er bl.a. fremhævet, at der ved transmission af oplysninger over det åbne internet generelt er en risiko for, at oplysningerne undervejs læses og endog ændres af uvedkommende. Derudover er der en risiko for, at parterne i kommunikationen ikke er dem, de udgiver sig for. Disse risici må vurderes af den dataansvarlige i den konkrete situation, således at der kan træffes de fornødne sikkerhedsforanstaltninger.

Hvad angår fortrolighed kan denne sikres ved forsvarlig kryptering af de transmitterede oplysninger. Hvis der er tale om transmission af fortrolige oplysninger, herunder personnummer, skal der som minimum foretages en kryptering. Hvis de transmitterede oplysninger er af følsom karakter (omfattet af persondatalovens § 7, stk. 1 og § 8, stk. 1), skal der anvendes en stærk kryptering, baseret på en anerkendt algoritme.

Sikkerhed for autenticitet (afsenders og modtagers identitet) og integritet (de transmitterede oplysningers ægthed) må sikres i fornødent omfang ved anvendelse af passende sikkerhedsforanstaltninger, f.eks. elektronisk signatur eller individuelle, fortrolige adgangskoder.

### 2.3. Sikkerhedskrav til private dataansvarlige

Der er ikke udstedt en bekendtgørelse, der udmønter kravene til sikkerheden i den private sektor. Det generelle krav i lovens § 41, stk. 3, er imidlertid det samme i den private sektor som i den offentlige.

I en række tilfælde – f.eks. når Datatilsynet giver tilladelser til forskellige private dataansvarlige – anbefaler tilsynet, at der i videst muligt omfang tilrettelægges sikkerhedsforanstaltninger i overensstemmelse med sikkerhedsbekendtgørelsen for den offentlige forvaltning.

#### 2.3.1. Datatilsynets vilkår i tilladelser

En række af de tilladelser, som Datatilsynet meddeler i den private sektor, indeholder vilkår om kryptering. Disse vilkår stilles i medfør af persondatalovens § 50, stk. 1, nr. 5, hvorefter tilsynet i forbindelse med de tilladelser, som tilsynet meddeler efter lovens § 50, stk. 1, 2 og 4, kan fastsætte nærmere vilkår for udførelsen af behandlingerne til beskyttelse af de registreredes privatliv.

Datatilsynets tilladelser til *private forskere* indeholder således standardmæssigt følgende vilkår:

”Ved overførsel af personhenførbare oplysninger via internet eller andet eksternt netværk skal der træffes de fornødne sikkerhedsforanstaltninger mod, at oplysningerne kommer til uvedkommendes kendskab. Oplysningerne skal som minimum være forsvarligt krypteret under hele transmissionen. Ved anvendelse af interne net skal det sikres, at uvedkommende ikke kan få adgang til oplysningerne.”

Datatilsynets tilladelser til *kreditoplysningsbureauer* indeholder standardmæssigt følgende vilkår:

”Fremsendelse af oplysninger over det åbne internet må alene ske i forsvarlig krypteret form.”

---

<sup>5</sup> Vejledning nr. 37 af 2. april 2001 til bekendtgørelse nr. 528 af 15. juni 2000 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning. Vejledningen kan læses på Datatilsynets hjemmeside [www.datatilsynet.dk](http://www.datatilsynet.dk) under punktet ”Lovgivning”.

”Hvis der gives bureauets abonnenter adgang til oplysningerne via en hjemmeside, skal der endvidere etableres en ordning, således at der kun gives adgang til oplysningerne efter indtastning af en adgangskode (password). Hvis oplysningerne gøres tilgængelige over det åbne internet, skal oplysningerne sendes i forsvarlig krypteret form.”

Tilsvarende hedder det i tilsynets standardvilkår til *advarselsregistre*:

”Udsendelse af lister i elektronisk form ved brug af e-post over det åbne internet må alene ske i forsvarlig krypteret form.”

”Hvis der gives medlemmerne/deltagerne i ordningen adgang til oplysningerne via en hjemmeside, må dette alene ske efter indtastning af en adgangskode (password). Hvis oplysningerne gøres tilgængelige over det åbne internet, skal oplysningerne sendes i forsvarlig krypteret form.”

I en tilladelse (gengivet på s. 74-75 i Datatilsynets årsberetning for 2005) til Centralregister for ”Min sidste Vilje” har Datatilsynet bl.a. meddelt Brancheorganisationen Danske Bedemænd følgende vilkår:

”Der må kun etableres eksterne kommunikationsforbindelser, hvis der træffes særlige foranstaltninger for at sikre, at uvedkommende ikke gennem disse forbindelser kan få adgang til personoplysninger.”

### **2.3.1. Påbud fra Datatilsynet**

Datatilsynet kan efter persondatalovens § 59, stk. 3, påbyde en privat dataansvarlig at træffe bestemte tekniske og organisatoriske sikkerhedsforanstaltninger mod, at der behandles oplysninger, som ikke må behandles, at oplysninger 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 praksis vil tilsynet ofte formulere sine krav om kryptering som en anmodning eller en anbefaling, idet tilsynets erfaring er, at sådanne anmodninger og anbefalinger i praksis efterleves.

I tilfælde af, at en privat dataansvarlig ikke følger en sådan anmodning eller anbefaling, er tilsynet imidlertid gået videre og har meddelt påbud efter lovens § 59, stk. 3.

I tilfælde af, at en privat dataansvarlig ikke følger et sådant påbud, vil tilsynets næste skridt normalt være en politianmeldelse.

Politianmeldelse som følge af manglende efterlevelse af et påbud om kryptering ved kommunikation over internet er sket i et enkelt tilfælde. Sagen vedrørte en organisation, som på sin hjemmeside havde en formular til fremsendelse af oplysninger om politisk overbevisning – dvs. oplysninger af følsom karakter, og der var ikke implementeret kryptering. Efter Datatilsynets politianmeldelse efterkom organisationen Datatilsynets påbud således, at det ikke længere var muligt at udfylde en online indmeldelsesblanket på organisationens hjemmeside. Sagen er omtalt i afsnit 3.2. om sager fra Datatilsynets praksis.

## 2.4. Andre krav til private dataansvarlige

Ud over persondatalovens krav til sikkerhed, skal der samtidig tages højde for, at der ved salg af varer over internettet er flere love – ud over persondataloven – der beskytter forbrugerne.

Forholdet reguleres blandt andet af e-handelsloven<sup>6</sup>.

Det følger af lovens § 12, stk. 1, at en tjenesteyder uden unødigt forsinkelse elektronisk skal bekræfte modtagelsen af en elektronisk ordre. Af § 12 stk. 2, følger, at en elektronisk ordre og den elektroniske ordrebekræftelse, jf. stk. 1, anses som modtaget, når adressaterne har adgang til disse. Det fremgår ikke af loven eller bemærkningerne hertil, hvad det nærmere indhold skal være af den elektroniske ordrebekræftelse.

Det følger imidlertid af lovens § 1, stk. 2, nr. 2, at loven ikke finder anvendelse på forhold, der vedrører persondatabeskyttelse.

Anvendelse af betalingskort ved e-handel reguleres i lov om visse betalingsmidler<sup>7</sup>. Det følger af § 4, at lovens formål er at sikre, at betalingsmidler, der er omfattet af denne lov, er sikre og velfungerende. Efter stk. 2 skal et betalingssystem indrettes og virke således, at der sikres brugerne gennemsigtighed, frivillighed, beskyttelse mod misbrug samt fortrolighed om brugerens anvendelse af betalingsmidlet. Der skal løbende træffes de juridiske, organisatoriske, driftsmæssige, tekniske og sikkerhedsmæssige foranstaltninger, som er nødvendige for, at der er tale om et sikkert og velfungerende betalingssystem.

Efter lovens § 8 har brugeren krav på en kvittering ved enhver transaktion, som iværksættes med betalingsmidlet, medmindre brugeren på anden måde har let adgang til oplysninger om, hvorvidt og hvornår den pågældende transaktion er gennemført.

Af lovbemærkningerne til § 8 fremgår, at ved fjernsalg, herunder handel på internettet, kan bestemmelsen eksempelvis opfyldes ved at sende en e-mail til brugeren, eller ved at brugeren kan klikke sig ind på udstederens hjemmeside og der se, hvilke transaktioner der er registreret på brugerens konto.

Det følger af lovens § 17, stk. 1, at bestemmelsen er præceptiv. Af kommentaren til bestemmelsen i Karnov fremgår, at brugeren derfor ikke på forhånd kan fraskrive sig muligheden for at få kvittering eller på anden måde få let adgang til oplysninger om, hvorvidt og hvornår transaktion er gennemført, men brugeren kan i forbindelse med den enkelte transaktion give afkald herpå.

De nordiske forbrugerombudsmand har i oktober 2002 udsendt standpunkt (vejledning) til handel og markedsføring på internettet<sup>8</sup>. Det fremgår indledningsvis af standpunktet, at når der i standpunktet står ”skal”, betyder det, at det er et krav efter lovgivningen i alle nordiske lande. Hvis der står ”bør” er det et udtryk for ombudsmændenes mening.

<sup>6</sup> Lov nr. 227 af 22. april 2002 om tjenester i informationssamfundet, herunder visse aspekter af elektronisk handel. Loven implementerer Europaparlamentets og Rådets direktiv 2000/31/EF af 8. juni 2000 om visse retlige aspekter af informationssamfundstjenester, navnlig elektronisk handel, i det indre marked.

<sup>7</sup> Lovbekendtgørelse nr. 1505 af 20. december 2004

<sup>8</sup> Dokumentet kan findes på <http://www.forbrug.dk/klage/love/forbrugerlove/mfl/retningslinjer/internettet-e-handel/>

Af standpunktet fremgår, at forbrugere ved indgåelse af elektronisk aftale snarest efter bestilling skal modtage en elektronisk kvittering på, at bestillingen er modtaget. Endvidere fremgår det, at den erhvervsdrivende også skal sende en ordrebekræftelse, der indeholder oplysninger vedrørende den konkrete bestilling, herunder hvad der er bestilt, og oplysninger om pris og betaling. Vedrørende betaling fremgår det, at transmission af betalingskortoplysninger og andre koder vedrørende betalingssystemer på internettet altid bør være stærkt krypteret. Det samme gælder for den efterfølgende opbevaring af betalingsoplysninger på en server med forbindelse til internettet. Øvrige betalingsdata så som kundeoplysninger og ordreoplysninger *bør* ligeledes være beskyttet ved kryptering eller på anden måde, der sikrer, at oplysningerne ikke er åbent tilgængelige/læselige for uvedkommende på internettet

Omkring sikkerhed på hjemmesiden fremgår det af vejledningen, at den erhvervsdrivende bør give klare og tydelige oplysninger om, i hvilket omfang de indgivne handels- og personoplysninger holdes fortrolige. Kunde/ordredata bør være beskyttede ved kryptering eller på anden måde, der sikrer, at oplysningerne ikke er åbent tilgængelige/læsbare for uvedkommende på internettet. Dette gælder såvel under transmission som under den efterfølgende opbevaring på en server, der er tilgængelig fra internettet. Hvis de pågældende data ikke er beskyttet som nævnt, bør forbrugeren gøres tydeligt opmærksom herpå.

### 3. Datatilsynets praksis

Såvel Register- som Datatilsynet har i flere sager taget stilling til sikkerhedskravene til transmission af fortrolige og følsomme personoplysninger over det åbne internet.

#### 3.1. Sager fra Registertilsynets praksis

##### *Registertilsynets sag 1997-213-032*

Registertilsynet udtalte i denne sag at følsomme patientoplysninger, der via internettet sendes mellem offentlige myndigheder i sundhedssektoren, som minimum skal være krypterede, og at krypteringen skal være af en sådan art, at oplysningerne vil være beskyttet med den fornødne høje sikkerhed. Sagen er omtalt i Registertilsynets årsberetning fra 1997 s. 123.

##### *Registertilsynets sag 1997-54-018*

I fortsættelse af Registertilsynets inspektion hos et kreditoplysningsbureau henledte tilsynet i anledning af det af bureauet anførte om videregivelse via internet bl.a. opmærksomheden på, at der efter lov om private registre § 6, stk. 4, skulle træffes de fornødne sikkerhedsforanstaltninger mod, at oplysninger i et edb-register misbruges eller kommer til uvedkommendes kendskab. Tilsynet noterede sig, at der var etableret adgangsprocedurer med kontrol. Datatransmissionen var imidlertid ikke sikret gennem kryptering, hvilket Registertilsynet anbefalede skete, idet det efter tilsynets opfattelse ville udgøre en væsentlig forbedring af sikkerheden.

Herudover behandlede Registertilsynet i slutningen af 90'erne flere sager om offentlige myndigheders kommunikation via internet. Disse vedrørte f.eks. transmission af oplysninger om personnumre og andre fortrolige oplysninger.

Tilsynets praksis var, at fortrolige oplysninger som minimum skulle være krypterede, og at krypteringen skulle være af en sådan art, at oplysningerne vil være beskyttet med den fornødne høje sikkerhed, i tilfælde hvor oplysningerne skulle transporteres via internettet.

### 3.2. Sager fra Datatilsynets praksis

#### *Datatilsynets sag 2001-215-0067*

Sagen drejede sig om elektronisk flyttemeddelelse på Københavns Kommunes hjemmeside, der ikke var krypteret. Datatilsynet udtalte i den forbindelse, at når der er tale om transmission af fortrolige oplysninger, herunder personnummer, skal der som minimum foretages kryptering. Endvidere udtalte Datatilsynet, at de omhandlede sikkerhedsregler gælder for enhver behandling af personoplysninger, der foretages for den offentlige forvaltning, og reglerne kan ikke fraviges ved hverken en orientering af borgerne om sikkerhedsmanglerne eller ved indhentelse af et samtykke fra borgerne til fravigelsen.

#### *Datatilsynets sag 2001-233-0009*

Der var tale om en forespørgsel vedrørende salg af kontaktlinser over internettet via en dansk hjemmeside. Datatilsynet udtalte i den forbindelse, at oplysninger om styrken på de ønskede kontaktlinser er at betragte som en helbredsoplysning omfattet af persondatalovens § 7. Endvidere udtalte Datatilsynet, at sikkerhedsreglerne i persondatalovens § 41, stk. 3, skulle iagttages, hvilket efter Datatilsynets opfattelse medfører, at der ved transmission af følsomme oplysninger over det åbne internet skal foretages en stærk kryptering, baseret på en anerkendt algoritme i forbindelse med salg af kontaktlinser over internettet.

#### *Datatilsynets sag 2001-631-0066*

Sagen drejede sig om en virksomheds behandling af oplysninger på dens webside. Virksomheden udførte bogholdervirksomhed, og i den forbindelse blev der transmitteret oplysninger om persons skatteforhold, herunder oplysninger om frikort, trækprocent og fradragsoplysninger, samt oplysninger om løn og sygedagpenge via internettet i ukrypteret stand. Datatilsynet udtalte, at hvis der er tale om transmission af oplysninger som f.eks. personnummer og oplysninger om en enkeltpersons økonomiske forhold, skal der som minimum foretages en kryptering. Hvis de transmitterede oplysninger er af følsom karakter, skal der anvendes en stærk kryptering, baseret på en anerkendt algoritme.

#### *Datatilsynets sag 2001-631-0067*

Datatilsynet henvendte sig af egen drift til privat skole vedrørende overførsel af personnumre via det åbne internet til skolen i ukrypteret form. Datatilsynet udtalte, at der ved transmission af oplysninger om personnumre over det åbne internet efter tilsynets opfattelse som minimum bør foretages kryptering. Der bør i øvrigt foretages kryptering, hvis andre oplysninger, som må betragtes som fortrolig (f.eks. oplysninger om økonomiske forhold o.l.) transmitteres. Hvis der er tale om følsomme oplysninger omfattet af persondatalovens §§ 7 og 8, skal der som minimum anvendes en stærk kryptering, baseret på en anerkendt algoritme. De beskrevne sikkerhedskrav bør følges, både når den dataansvarlige er en offentlig myndighed, og når der er tale om en privat virksomhed mv. Tilsynet udtalte endvidere, at det således er Datatilsynets opfattelse, at persondatalovens § 41, stk. 3, medfører, at der som udgangspunkt må stilles samme krav til datasikkerheden i private virksomheder mv. som i den offentlige forvaltning.

#### *Datatilsynets sager 2002-631-xxxx*

Datatilsynet tog af egen drift en række sager op vedrørende politiske partiers og politiske ungdomsforeningers hjemmesider, hvor der var mulighed for at indmelde sig. Datatilsynet henvendte sig til de enkelte foreninger og orienterede om, at der efter Datatilsynets opfattelse ved transmittering af fortrolige oplysninger, herunder personnummer, som minimum bør foretages en kryptering. Hvis de transmitterede oplysninger er af følsom karakter, skal der anvendes en stærk kryptering.

ring, baseret på en anerkendt algoritme. Datatilsynet udtalte endvidere, at oplysninger om medlemskab af et politisk parti er en fortrolig og endog følsom oplysning, jf. persondatalovens § 7, stk. 1. Oplysninger om, at man ønsker at blive medlem, må ligeledes betragtes som en oplysning om politisk tilhørsforhold, og altså en følsom oplysning. Datatilsynet foreslog på den baggrund foreningerne at træffe foranstaltninger til at sikre, at transmissionen af oplysninger sikres på en måde, så risikoen for, at oplysningerne kommer til uvedkommendes kendskab, minimeres, og udbad sig underretning om, hvad foreningerne ville foretage. Alle foreninger på nær én imødekom Datatilsynets forslag.

#### *Datatilsynets sag 2002-631-xxxx*

I en af de egen drift-sager, som Datatilsynet tog op vedrørende politiske partiers og politiske ungdomsforeningers hjemmesider, blev Datatilsynets henvendelse med forslag om kryptering ikke imødekommet. Datatilsynet anvendte derfor sine beføjelser efter persondataloven og påbød i medfør af persondatalovens § 59, stk. 1 og 3, partiet at bringe sin behandling af personoplysninger i forbindelse med elektronisk indmeldelse i partiet via partiets hjemmesider i overensstemmelse med lovens krav om stærk kryptering ved transmission af følsomme oplysninger over åbne net eller at ophøre med at stille muligheden for elektronisk indmeldelse i partiet til rådighed.

Da partiet endvidere ikke efterkom Datatilsynets påbud, fandt tilsynet det nødvendigt at politianmelde partiet for overtrædelse af persondatalovens bestemmelse i § 41, stk. 3, om datasikkerhed og for at have undladt at efterkomme Datatilsynets påbud.

Datatilsynet kunne derefter konstatere, at formularen var fjernet fra hjemmesiden, og Datatilsynets påbud dermed efterkommet. Herefter sluttede sagen. Politiet lukkede også deres sag.

#### *Datatilsynets sag 2003-213-0173*

Sagen drejede sig om en banks fremsendelse af en ukrypteret e-post indeholdende et personnummer som svar på en henvendelse til banken via en krypteret side på bankens hjemmeside. Datatilsynet udtalte i den forbindelse, at tilsynet havde noteret sig, at banken havde fastsat retningslinier for anvendelse af e-post/notes-mail samt internettet for bankens medarbejdere. Datatilsynet noterede sig endvidere, at banken foranlediget af det skete havde indskærpet sikkerhedsreglerne over for den pågældende medarbejder, og at banken generelt havde orienteret sine medarbejdere om reglerne på ny.

#### *Datatilsynets sag 2003-631-0110*

Datatilsynet henvendte sig af egen drift til en virksomhed vedrørende virksomhedens videregivelse af oplysninger om e-postadresser og om afslag på jobansøgning til en række jobansøgere. Jobafslaget blev sendt til alle ansøger i én samlet e-post, hvor samtlige ansøgers e-postadresser fremgik af modtagerfeltet. Det er Datatilsynet opfattelse, at sikring af, at e-postadresser og e-postens indhold, som dermed også kan henføres til personer, ikke kommer til uvedkommendes kendskab, er omfattet af den dataansvarliges forpligtigelse efter § 41, stk. 3. Datatilsynet fandt derfor, at virksomheden ved udsendelsen af e-posten med oplysning om, at alle adressaterne havde fået afslag på deres jobansøgning, havde overtrådt kravene i persondatalovens § 41, stk. 3. I tilknytning hertil henledte Datatilsynet endvidere opmærksomheden på, at det bl.a. følger af sikkerhedsvejledningen, at der ved transmission af fortrolige oplysninger som minimum skal foretages kryptering.

*Datatilsynets sag 2003-632-0056*

Sagen drejede sig om et hospital, der sendte en e-post med fortrolige oplysninger om en patient til en speciallæge. Der skete derefter spredning af patientoplysningerne fra lægens computer på grund af en virus på computeren, som bevirkede, at e-posten blev videregivet til en række e-postadresser indeholdt i lægens adressekartotek. Datatilsynet bemærkede, at den omhandlede e-post efter tilsynets opfattelse indeholdt fortrolige oplysninger, som tillige var af følsom karakter, herunder oplysninger om helbredsmæssige forhold og strafbare forhold. Datatilsynet konstaterede, at der hverken var anvendt kryptering eller digital signatur ved afsendelsen af e-posten, hvilket Datatilsynet anså som en alvorlig tilsidesættelse af såvel kravene til datasikkerhed som kravet om god databehandlingsskik. Datatilsynet henstillede, at amtet i overensstemmelse med persondatalovens krav om god databehandlingsskik og behandlingssikkerhed etablerede hensigtsmæssige sagsbehandlingsprocedurer i forbindelse med ekstern e-post samt gav den fornødne instruktion til medarbejdere, der behandler personoplysninger.

*Datatilsynets sag 2004-216-0198*

Sagen drejede sig om en privat organisations webside, hvor der i forbindelse med køb af billetter skulle opgives personnummer, og der skete i den forbindelse ukrypteret transmission af personnummeret via internettet. Datatilsynet udtalte, at der ved transmission af oplysninger om personnumre over det åbne internet efter tilsynets opfattelse som minimum bør foretages kryptering. Der bør også foretages kryptering, hvis andre oplysninger, som må betragtes som fortrolige (f.eks. oplysninger om økonomiske forhold o.l.), transmitteres.

*Datatilsynets sag 2004-323-0132*

En kommune rettede henvendelse til Datatilsynet med en forespørgsel om, hvorvidt en jobansøgning, der er modtaget elektronisk via e-post, kan besvares via e-post uden brug af digital signatur. Datatilsynet udtalte i den forbindelse, at en stillingsansøgning samt svar herpå må betragtes som fortrolige, og at der derfor skal foretages kryptering, når svar på ansøgningen sendes via internettet. Samtidig oplyste Datatilsynet, at det ikke er muligt at samtykke sig ud af sikkerhedskravene ved f.eks. at undlade at bruge digital signatur eller lignende.

*Datatilsynets sag 2006-313-0353*

Sagen drejede sig om en kommunes fremsendelse af en ukrypteret e-post, som indeholdt oplysninger om restance vedrørende betaling af børne- og/eller ægtefællebidrag. Datatilsynet udtalte, at restanceoplysninger i forbindelse med afregning af børnebidrag/ægtefællebidrag efter tilsynets opfattelse er oplysninger af fortrolig karakter. På den baggrund udtalte Datatilsynet, at der ved transmission af fortrolige oplysninger over det åbne internet som minimum skal foretages kryptering. Datatilsynet bemærkede desuden, at det ikke umiddelbart fremgik af kommunens "Lokale uddybende sikkerhedsregler", at e-post indeholdende fortrolige eller følsomme personoplysninger skal fremsendes krypteret. Datatilsynet anbefalede således, at det fremover skulle fremgå af kommunens sikkerhedsregler, at fortrolig og følsom information skal krypteres, hvis den sendes via e-post.

*Datatilsynets sag 2005-2214-0008*

Sagen drejede sig om en registrering hos et kreditoplysningsbureau. I forbindelse med sagens behandling havde kreditoplysningsbureauet anvendt elektronisk post til besvarelse af den registreredes henvendelse. Den fremsendte e-post indeholdte den registreredes skylderklæring, hvoraf den registreredes personnummer fremgik. Datatilsynet udtalte, at der ved transmission af oplysninger om personnumre over det åbne internet efter tilsynets opfattelse som minimum bør foretages kryptering. Der bør også foretages kryptering, hvis andre oplysninger, som må betragtes som fortrolige (f.eks. oplysninger om økonomiske forhold o.l.), transmitteres.

Datatilsynet udtalte videre, at oplysning om, at en person er registreret i et kreditoplysningsbureau, efter tilsynets opfattelse er en oplysning, der ikke bør sendes ukrypteret over det åbne internet. Det er således tilsynets opfattelse, at oplysning om, at en person er registreret i et kreditoplysningsbureau er af privat og fortrolig karakter. Den omstændighed, at oplysningen kan videregives til bureauets abonnenter, ændrer ikke herved, idet abonnenternes adgang til oplysningerne er begrænset til tilfælde, hvor den pågældende skal have kredit. Oplysningerne er således ikke frit tilgængelige.

Datatilsynet meddelte på denne baggrund kreditoplysningsbureauet, at tilsynet under henvisning til persondatalovens krav om datasikkerhed anbefalede, at bureauet ikke sendte oplysninger om registreringer via almindelig ukrypteret e-post.

#### **4. Datatilsynets foreløbige overvejelser**

Persondatalovens § 41, stk. 3, som er beskrevet i afsnit 2 i dette notat, fastlægger de overordnede krav til den dataansvarliges behandlingssikkerhed.

Det er som nævnt i afsnit 2 forudsat, at sikkerhedsforanstaltningerne under hensyn til det aktuelle tekniske niveau og de omkostninger, som er forbundet med deres iværksættelse, skal tilvejebringe et tilstrækkeligt sikkerhedsniveau i forhold til de risici, som behandlingen indebærer, og arten af de oplysninger, som skal beskyttes, jf. databeskyttelsesdirektivets artikel 17, stk. 1, 2. afsnit.

Fastlæggelsen af sikkerhedsniveauet må således ske efter en afvejning af på den ene side det aktuelle tekniske niveau og omkostningerne i forbindelse med foranstaltningernes iværksættelse og på den anden side de risici, som behandlingen indebærer, samt hvilke oplysningstyper der er tale om.

Det må samtidig tages i betragtning, at der med persondataloven ikke er tilsigtet et lavere niveau for datasikkerhed end efter den tidligere registerlovgivning.

Endelig må tilsynet tage hensyn til, at såvel direktivet som persondataloven identificerer fremsendelse af oplysninger i et net som en behandling, der medfører, at de fornødne sikkerhedsforanstaltninger er særligt påkrævet.

##### **4.1. Risici ved brug af internet**

Det må efter Datatilsynets opfattelse lægges til grund, at internettet – uden brug af ekstra sikkerhedstiltag – ikke er et sikkert net. Ved et sikkert net forstås et net, hvor oplysningerne ikke undervejs kan tilgås af uvedkommende.

Ved transmission af oplysninger over internet er der efter Datatilsynets opfattelse generelt en risiko for, at oplysningerne undervejs læses og endog ændres af uvedkommende. Dette har tilsynet tillige anført i sin vejledning til sikkerhedsbekendtgørelsen i den offentlige forvaltning omtalt ovenfor i afsnit 2.2.

Det har af og til været nævnt, at fremsendelse via internet er som at sende oplysningerne på et åbent postkort. Denne sammenligning er efter Datatilsynets opfattelse beskrivende.

## 4.2 Datatilsynets umiddelbare vurderinger

Efter Datatilsynets opfattelse er det her relevant at sondre mellem transmission via den dataansvarliges *hjemmeside* og transmission ved anvendelse af *e-post*.

### 4.2.1. Transmission af oplysninger via en hjemmeside

Efter Datatilsynets opfattelse findes der løsninger, der kan sikre, at oplysningerne krypteres, når de fremsendes via en hjemmeside. Den dataansvarlige har således mulighed for at implementere en løsning, hvor kommunikationen via hjemmesiden foregår sikkert ved hjælp af SSL kryptering eller lign. Anvendelsen af den sikre kommunikation kræver ikke implementering af en særlig løsning hos brugeren. Der er endvidere mulighed for at implementere forskellige grader af kryptering, herunder også det, der betegnes som ”stærk kryptering”.

Det er endvidere tilsynets vurdering, at omkostningerne ved sådanne løsninger ikke er større, end at udgiften står mål med den beskyttelse af personoplysninger, som opnås ved løsningen.

**Ved fremsendelse via en formular på den dataansvarliges hjemmeside er det derfor tilsynets umiddelbare vurdering, at kravet om beskyttelse af oplysningerne ved kryptering fortsat er passende. Efter tilsynets opfattelse skal der således fortsat anvendes kryptering ved fremsendelse af private (fortrolige) personoplysninger – herunder personnumre.**

**Tilsynet finder også fortsat, at krypteringen bør være ”stærk”, hvis oplysningerne er af følsom karakter. Dvs. hvis der er tale om oplysninger omfattet af persondatalovens §§ 7 og 8. Disse bestemmelser omfatter oplysninger om racemæssig eller etnisk baggrund, politisk, religiøs eller filosofisk overbevisning, fagforeningsmæssige tilhørsforhold og oplysninger om helbredsmæssige og seksuelle forhold samt oplysninger om strafbare forhold, væsentlige sociale problemer og andre rent private forhold mv.**

### 4.2.2. Transmission af oplysninger via e-post

En anden kategori omhandler kommunikation via e-post. Her findes der også løsninger. Disse er imidlertid ikke så ligetil at implementere – såvel afsender som modtager skal således kunne kommunikere sikkert.

Der findes forskellige løsninger til sikker kommunikation via e-post. Der er bl.a. mulighed for at sende sikker e-post ved hjælp af digital signatur (OCES).

Herudover kan f.eks. bruges centrale postkasser som e-Boks. Det kan også forekomme, at den dataansvarlige selv har etableret en løsning. Dette kan f.eks. være i forbindelse med et pengeinstituts netbank.

Løsningerne er teknologisk mulige, og med det gratis OCES certifikat til borgerne er det som udgangspunkt alene de dataansvarlige, der har omkostninger ved etablering af løsningerne. Datatilsynet vurderer umiddelbart, at omkostningerne ved etablering af løsninger til sikker e-post kommunikation ikke er større, end at de står mål med behovet for at beskytte private (fortrolige) og/eller følsomme personoplysninger ved kommunikation over internet.

Anvendelsen af disse løsninger er imidlertid ikke særligt udbredt blandt borgerne. Der vil derfor være en del borgere, der ikke vil kunne modtage sikker e-post. Ulempen for de berørte virksomheder kan således være, at en del af deres kommunikation med kunder mv. ikke kan ske digitalt men må foregå med almindelig post. Kravet om kryptering vil derfor i praksis kunne udgøre en barriere for digitalisering og effektivisering.

Også på dette område må udgangspunkt tages i, at internettet ikke er sikkert.

Det må desuden tages i betragtning, at Register- og Datatilsynets praksis hidtil har været, at oplysninger af privat (fortrolig) karakter – herunder personnumre – samt oplysninger af følsom karakter skal beskyttes ved transmission via internet, herunder ved fremsendelse på e-post.

Sammenholdt med forudsætningen om, at persondataloven ikke skal medføre et lavere niveau for datasikkerhed end efter den tidligere registerlovgivning, taler dette for, at det hidtidige krav om kryptering, hvor hensynet til beskyttelsen af personoplysningerne er afgørende, fastholdes – selv om anvendelse af sikre løsninger i praksis – endnu – er forbundet med vanskeligheder.

På den anden side er det som beskrevet ovenfor også forudsat, at sikkerhedsforanstaltningerne under hensyn til **det aktuelle tekniske niveau** og de omkostninger, som er forbundet med deres iværksættelse, skal tilvejebringe et tilstrækkeligt sikkerhedsniveau i forhold til de risici, som behandlingen indebærer, og arten af de oplysninger, som skal beskyttes, jf. databeskyttelsesdirektivets artikel 17, stk. 1, 2. afsnit.

Ved vurderingen af, hvilke krav der skal gælde, må det aktuelle tekniske niveau derfor også tages i betragtning.

Der må henses til, hvad der i praksis kan lade sig gøre – og efter Datatilsynets umiddelbare opfattelse tillige til, om de tilgængelige løsninger er af en sådan karakter, at de i praksis kan anvendes bredt af de berørte.

**I følgende tilfælde er der efter Datatilsynets umiddelbare opfattelse så stort et behov for beskyttelse, at kravet om kryptering i hvert fald må fastholdes:**

1. **Transmission af personoplysninger ved brug af e-post i forbindelse med private forskningsprojekter bør under alle omstændigheder ske krypteret. Under henvisning til de særlige muligheder, der eksisterer for behandling af oplysninger i videnskabeligt og statistisk øjemed, er det efter Datatilsynets opfattelse nødvendigt, at den private forsker beskytter oplysningerne mod, at de kan komme til uvedkommendes kendskab.**

**Kryptering har siden 2000 været et fast vilkår i Datatilsynets tilladelser til behandlinger af følsomme oplysninger, der foretages for en privat dataansvarlig, og som udelukkende finder sted i statistisk eller videnskabeligt øjemed.**

2. **Fremsendelse af e-post fra advarselsregistre og kreditoplysningsbureauer. Dette har været en del af tilsynets vilkår siden 2000. Under henvisning til oplysningernes karakter og de betydelige ulemper for den berørte person eller virksomhed, det kan medføre, hvis oplysningerne kommer til uvedkommendes kendskab, er det tilsynets opfattelse, at oplysningerne også fortsat kun må transmitteres over internet, hvis der**

anvendes kryptering.

Kravet om kryptering skal efter Datatilsynets opfattelse fortsat gælde for enhver kommunikation fra advarselsregisteret eller kreditoplysningsbureauet – herunder til såvel abonnenter som til registrerede personer og virksomheder. Kravet om kryptering bør endvidere fortsat gælde for abonnenternes fremsendelse af informationer om de registrerede til bureauet.

3. Fremsendelse af e-post indeholdende følsomme oplysninger omfattet af persondatalovens §§ 7 og 8. Her er det tilsynets umiddelbare opfattelse, at oplysningernes karakter medfører, at behovet for at beskytte oplysningerne vejer tungest i forhold til de ulemper, et krav om kryptering medfører for de dataansvarlige.

Datatilsynet vil overveje, om der vil kunne accepteres undtagelser fra kravet om kryptering ved transmission af følsomme oplysninger, og hvordan tilfælde, hvor dette skal kunne ske, afgrænses.

Elementer, der eventuelt kan indgå i vurderingen, er, om den berørte person (kunden) har valgfrihed – altså om personen kan vælge at gå et andet sted hen, hvis han ikke vil være kunde hos en dataansvarlig, der ikke tilbyder beskyttelse af følsomme personoplysninger ved e-post kommunikation. Det kan eventuelt også indgå i overvejelserne, om kunden selv vælger denne kommunikationsform over for virksomheden.

4. Datatilsynet vil desuden overveje, om der er andre områder, hvor der transmitteres personoplysninger af privat – men ikke af følsom – karakter, hvor kryptering ligeledes fortsat bør være et krav ved anvendelse af e-post.

Datatilsynet vil i den forbindelse overveje, om der fortsat skal være krav om kryptering, hvis et personnummer sendes i en e-post via internettet i den private sektor.

I alle andre tilfælde vil Datatilsynet overveje – i hvert fald indtil videre – eventuelt at frafalde kravet om kryptering ved brug af e-post i den private sektor. Det gælder f.eks. for e-post indeholdende oplysninger om bestilte eller købte varer i e-handelsløsninger, økonomiske forhold i forbindelse med bankforretninger, afslag på jobansøgninger og andre private, men ikke følsomme personoplysninger.

Det understreges samtidig, at Datatilsynets umiddelbare vurdering ikke medfører, at et samtykke fra den berørte person bliver afgørende for, om der skal ske kryptering. Som det fremgår af afsnit 3 om tilsynets praksis, har tilsynet hidtil haft den opfattelse, at sikkerhedsreglerne ikke kan fraviges ved indhentelse af et samtykke fra borgerne.