Opdateret: 06.05.15

Datatilsynets krav og anbefalinger i forbindelse med overførsel af personoplysninger via internettet i den private sektor

Datatilsynet besluttede i 2007 at overveje persondatalovens sikkerhedskrav i relation til private virksomheders overførsel af personoplysninger via internettet.

I den forbindelse har Datatilsynet foretaget en bred høring af organisationer mv. Høringssvarene er gengivet i et notat.

Læs Datatilsynets høringsnotat.

Læs oversigt over høringssvar.

Datatilsynet har – efter behandling i Datarådet – besluttet, at de krav og anbefalinger, som er omtalt nedenfor, indtil videre vil blive lagt til grund i tilsynets administration af persondatalovens sikkerhedskrav i forhold til den private sektor.

Dermed forsøger Datatilsynet at finde en fornuftig balance mellem mulighederne for bredt i samfundet at anvende internettet og e-mail som effektive kommunikationsmidler over for behovet for at beskytte personoplysninger mod misbrug, tab mv.

Datatilsynet sondrer mellem kommunikation via hjemmesider og kommunikation via e-mail. Grunden til det er, at de aktuelle muligheder for at beskytte oplysningerne er forskellige for de to typer af dataoverførsel.

Datatilsynets beslutning går ud på, at tilsynet kun stiller **udtrykkeligt krav om kryptering** ved:

- overførsel af **følsomme** oplysninger via hjemmesider,
- overførsel af **personnumre** via hjemmesider, samt
- tilfælde, hvor behandlingen af personoplysninger i den private sektor sker efter tilladelse med **vilkår** om konkrete sikkerhedsforanstaltninger ved transmission over internettet.

I en række andre situationer **anbefaler** Datatilsynet, at personoplysninger beskyttes, når de overføres via internettet.

Datatilsynet opfordrer samtidig alle interessenter til at lade hensyn til beskyttelse af personoplysninger indgå ved udformning og valg af nye tekniske løsninger til overførsel af persondata.

Det er således Datatilsynets håb, at der i takt med, at nye digitale løsninger udvikles og vinder udbredelse, også bliver bedre muligheder for at beskytte personoplysninger effektivt og uden store omkostninger for de involverede.

De krav og anbefalinger, som Datatilsynet nu har formuleret, må derfor tages op til fornyet overvejelse, efterhånden som nye tekniske muligheder for databeskyttelse bliver let tilgængelige.

Uddybende information om Datatilsynets krav og anbefalinger

Persondatalovens krav om databeskyttelse

Persondataloven stiller krav om, at virksomheder, organisationer, foreninger mv. beskytter alle de personoplysninger, som de behandler, med tilstrækkelige sikkerhedsforanstaltninger.

Efter loven er det som udgangspunkt op til den enkelte virksomhed at vurdere og beslutte, hvilke sikkerhedsforanstaltninger der er nødvendige i en given situation.

Kravet om beskyttelse gælder bl.a., når oplysninger overføres via internettet. Det gælder også, når virksomheden mv. giver kunder og andre personer mulighed for at sende oplysninger til eller modtage oplysninger fra virksomheden via sin hjemmeside.

Overførsel af personoplysninger via hjemmesider

Kommunikationen via hjemmesider kan sikres ved hjælp af SSL kryptering e.l. Der er mulighed for at implementere forskellige grader af kryptering, herunder også det, der betegnes som ”stærk kryptering” (128 bit SSL/TLS-forbindelse).

Anvendelsen af sikker kommunikation kræver ikke implementering af en særlig løsning hos virksomhedens kunder eller brugere af hjemmesiden.

Løsningen medfører samtidig, at brugerne via hjemmesidens certifikat kan sikre sig, at der kommunikeres med den rette modtager.

Krav om kryptering af følsomme personoplysninger

Overførsel af **følsomme** personoplysninger via hjemmesider **skal** ske krypteret.

Manglende kryptering kan medføre påbud fra Datatilsynet og i yderste konsekvens politianmeldelse og straf.

Krav om kryptering af personnumre

Overførsel af **personnumre** via hjemmesider **skal** ske krypteret.

Manglende kryptering kan medføre påbud fra Datatilsynet og i yderste konsekvens politianmeldelse og straf.

Anbefaling om kryptering af almindelige private personoplysninger

Datatilsynet anbefaler, at overførsel af almindelige **private (fortrolige)** personoplysninger via hjemmesider beskyttes ved kryptering.

Særligt om overførsel af personoplysninger via hjemmesider fra virksomhed til bruger

Hvis brugere via hjemmesiden får adgang til personoplysninger – f.eks. om sig selv – skal der også skabes sikkerhed for, at oplysningerne ikke udleveres til uvedkommende. Dette kan ske ved anvendelse af pinkode eller digital signatur. Hvis der gives adgang til følsomme personoplysninger, anbefaler Datatilsynet brug af digital signatur.

Overførsel af personoplysninger via e-mail

Krav om kryptering, når det følger af Datatilsynets vilkår

Sker en behandling efter tilladelse fra Datatilsynet, skal eventuelle vilkår om kryptering i tilladelsen følges. Det vil være tilfældet for:

- **private forskningsprojekter**
- **advarselsregistre og kreditoplysningsbureauer**
- **andre private virksomheder mv. med tilladelse fra Datatilsynet, hvor der er fastsat vilkår om kryptering**

Manglende kryptering kan medføre påbud fra Datatilsynet og i yderste konsekvens politianmeldelse og straf.

Den enkelte virksomheds vurdering

Har Datatilsynet ikke stillet vilkår til virksomheden mv. om kryptering, er det som udgangspunkt op til den enkelte virksomhed at vurdere og beslutte, hvilke sikkerhedsforanstaltninger der er nødvendige, når personoplysninger overføres ved e-mail.

Den enkelte virksomheds beslutning må tages ud fra en vurdering af bl.a.:

- Typen af oplysninger og den sammenhæng, de indgår i, herunder hvilke konsekvenser tab af oplysninger kan have.
- Om der er tale om overførsel af personoplysninger mellem:
  - to professionelle parter som f.eks. advokater, fagforeninger, revisorer mv., hvor andre personer omtales, eller
  - en professionel aktør og en privat person som f.eks. en kunde, en klient, et medlem mv.
- De omkostninger, som er forbundet med at iværksætte sikkerhedsforanstaltninger.

Datatilsynet anbefaler kryptering

- **når følsomme personoplysninger sendes med e-mail via internettet**

  Datatilsynet anbefaler, at der anvendes kryptering, når en e-mail eller et vedhæftet dokument hertil indeholder følsomme personoplysninger og sendes via internettet.

- **når personnummer sendes med e-mail via internettet**

  På grund af personnummerets særlige karakter anbefaler Datatilsynet, at personnumre kun sendes via internettet, hvis der anvendes kryptering.

Det er tilsynets vurdering, at det i mange tilfælde vil være muligt for virksomheder, der ønsker at benytte e-mail uden kryptering, at undlade at anføre personnummeret i den e-mail eller det dokument, som fremsendes. Det gælder også i situationer, hvor en virksomhed ønsker at besvare en e-mail fra en privat person, hvori personen selv har sendt sit personnummer uden brug af kryptering.

- **når password og lignende sendes med e-mail via internettet**

  Datatilsynet anbefaler, at der anvendes kryptering, når en e-mail eller et vedhæftet dokument hertil indeholder informationer, som giver adgang til følsomme personoplysninger eller personnummer.

Datatilsynet
Borgergade 28, 5
1300 København K
Tlf.: 33 19 32 00
Fax.: 33 19 32 18
E-mail: dt@datatilsynet.dk