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

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.

1. 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 personoplysnin-ger, anbefaler Datatilsynet brug af digital signatur.

2. Overførsel af personoplysninger via e-mail

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.

Læs mere her:

https://www.datatilsynet.dk/erhverv/internettet/krav-og-anbefalinger-ifm-overfoersel-af-personoplysninger-via-internettet/