DATATILSYNET

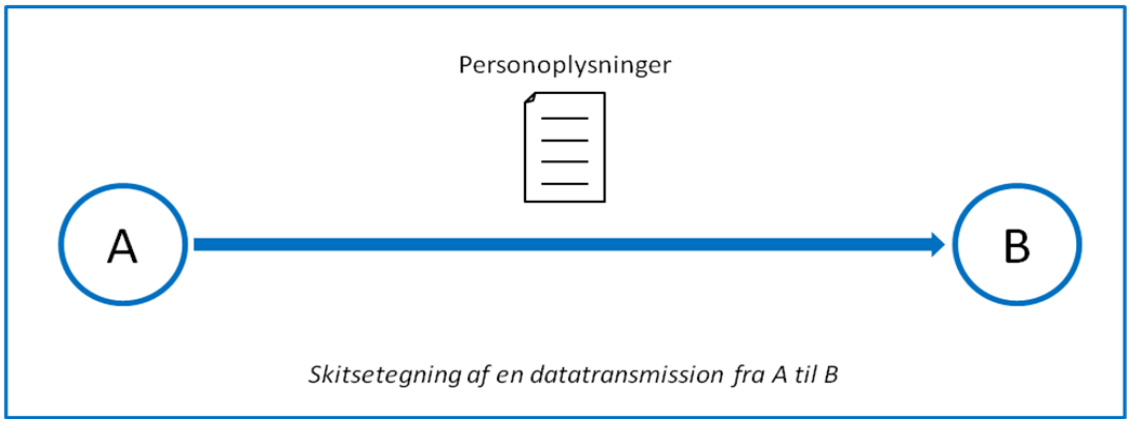
It-sikkerhedstekst ST2

Overvejelser om sikring mod, at personoplysninger kommer til uvedkommendes kendskab i forbindelse med datatransmission

Dokumentnavn: ST2
Version 1
Juli 2014

Overvejelser om sikring mod, at personoplysninger kommer til uvedkommendes kendskab i forbindelse med datatransmission

I det følgende betragtes en forholdsvis enkel situation med kun to parter (A og B), hvor personoplysninger overføres fra afsender (A) til modtager (B) ved hjælp af datatransmission.



Figur 1

Datatransmission af personoplysninger er en behandling af personoplysninger i persondatalovens forstand. Den dataansvarlige for datatransmissionen har ansvaret for at træffe de fornødne sikkerhedsforanstaltninger mod, at personoplysninger kommer til uvedkommendes kendskab.

Dataansvarlig

Persondataloven § 3, nr. 4, definerer den dataansvarlige som:

> *"Den fysiske eller juridiske person, offentlige myndighed, institution eller ethvert andet organ, der alene eller sammen med andre afgør, til hvilket formål og med hvilke hjælpemidler der må foretages behandling af oplysninger."*

Da der indgår flere parter i en datatransmission, rejser det spørgsmålet om, hvem der er dataansvarlig og dermed har ansvaret for at træffe sikkerhedsforanstaltninger.

Hvis det fx er afsenderen (A), der har besluttet/valgt at foretage datatransmissionen til modtageren (B), så vil det som hovedregel være afsenderen (A), der er dataansvarlig for datatransmissionen. Omvendt hvis fx det er modtageren (B), der pålægger afsenderen (A) at foretage datatransmissionen, så vil det som hovedregel være modtageren (B), der er dataansvarlig for datatransmissionen.

I en konkret situation kan det forholde sig anderledes, og hvem der er dataansvarlig i forbindelse med en given datatransmission, må altid afgøres ud fra de aktuelle forhold og omstændigheder.

Krav til den dataansvarlige i forbindelse med datatransmission

Den dataansvarlige har ansvaret for at sikre, at behandling af personoplysninger lever op til persondatalovens bestemmelser, herunder at træffe sikkerhedsforanstaltninger mod, at personoplysninger kommer til uvedkommendes kendskab ved datatransmission. I denne forbindelse kan der peges på persondataloven § 41, stk. 3,:

> *"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. Tilsvarende gælder for databehandlere."*

Endvidere er der for dataansvarlige inden for den offentlige sektor fastsat nærmere regler i sikkerhedsbekendtgørelsen[1]. Reglerne er uddybet i vejledningen til sikkerhedsbekendtgørelsen[2]. Når der behandles personoplysninger i privat sektor, skal der i nogle tilfælde foreligge en forudgående tilladelse til databehandlingen fra Datatilsynet[3]. I tilladelsen kan der være stillet specifikke krav til sikkerheden.

Beskyttelsesbehov og krav

Personoplysninger klassificeres som – almindelige personoplysninger (mindst sensitive), fortrolige personoplysninger (mere sensitive) og følsomme personoplysninger (mest sensitive). Generelt er beskyttelsesbehovet større, jo mere sensitive personoplysninger der transmitteres.

Det er i første række den dataansvarlige, der skal gøre sig overvejelser om beskyttelsesbehovet for de personoplysninger, der transmitteres.

En særlig problemstilling opstår, hvis forskellige typer af personoplysninger transmitteres sammen. I så fald skal sikkerhedsforanstaltningerne indrettes efter de mest sensitive personoplysninger.

Risiko

Ved datatransmission af personoplysninger er der en risiko for, at uvedkommende får kendskab til de personoplysninger, der transmitteres. Dette kan fx ske ved:

- Aflytning af datatransmissionen.
- At der under datatransmissionen dannes og lagres kopier af data i kortere eller længere tid, enten hos afsender (A), modtager (B) eller hos fx et teleselskab, hvis netværk benyttes ved datatransmissionen.
- At de transmitterede personoplysninger havner hos en forkert modtager.

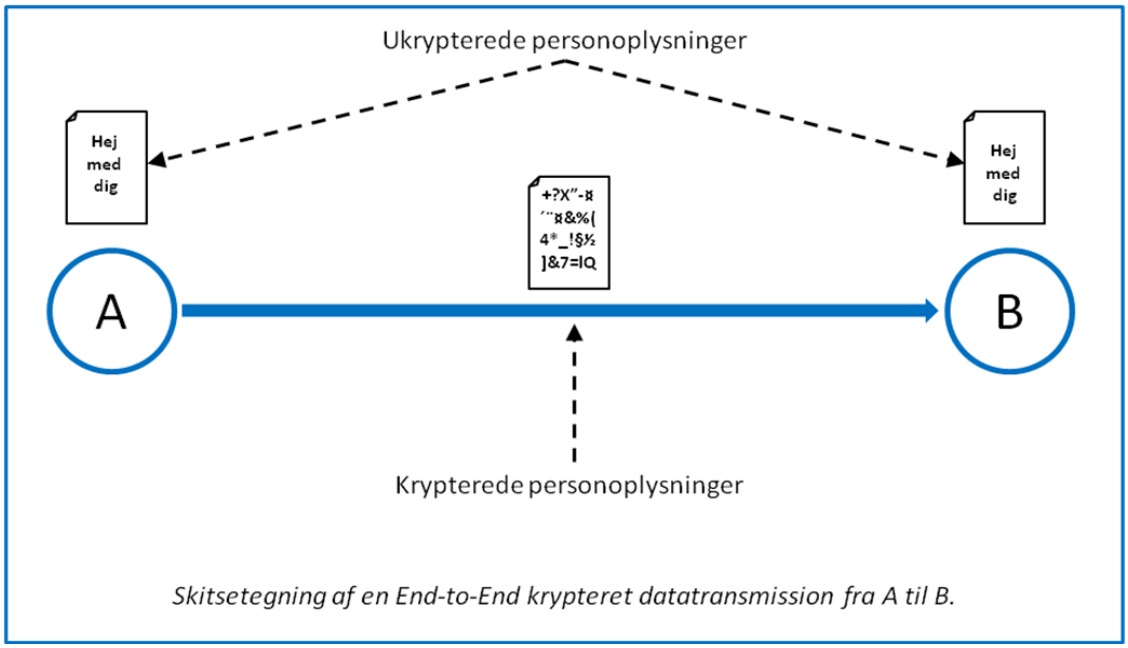
I en konkret situation kan risici for, at personoplysninger, der transmitteres, kommer til uvedkommendes kendskab, med fordel afdækkes i en risikoanalyse.

[1] Sikkerhedsbekendtgørelsen (Bkg. nr. 528 af 15. juni 2000 som ændret ved bkg. nr. 201 af 22. marts 2001)
[2] Vejledningen til sikkerhedsbekendtgørelsen (Vejl. nr. 37 af 02. april 2001)
[3] http://www.datatilsynet.dk/blanketter/generelt-om-anmeldelse/

Sikkerhedsforanstaltninger ved datatransmission

Med baggrund i beskyttelsesbehovet og de risici, der er forbundet med datatransmission, skal den dataansvarlige sikre sig, at der er etableret passende sikkerhedsforanstaltninger mod, at transmitterede personoplysninger kommer til uvedkommendes kendskab.

Det mest almindelige er, at der medvirker andre end afsender (A) og modtager (B) ved datatransmissionen, fx en teleudbyder eller internetudbyder. I denne situation er en effektiv sikkerhedsforanstaltning ved datatransmission, anvendelse af End-to-End[4] kryptering, fx en krypteret tunnel, ubrudt hele vejen fra afsender (A) til modtager (B).



Figur 2

Kryptering kan, hvis den er etableret korrekt og anvendt rigtigt, sikre fortrolighed af de personoplysninger, der transmitteres.

- Hvis en datatransmission aflyttes, vil kryptering sikre mod uvedkommendes kendskab til indholdet af datatransmissionen.
- Kryptering sikrer også mod uvedkommendes kendskab, fx ved adgang til eventuelle lagrede kopier hos tele- eller internetudbydere.
- Endvidere vil krypterede data, der havner hos en forkert modtager, være sikret mod uvedkommendes kendskab, forudsat at det kun er den tiltænkte modtager, der kan dekryptere data.

[4] *End-to-End* kryptering betyder: (i) at indholdsdata krypteres hos afsenderen inden afsendelsen, (ii) at indholdsdata er og forbliver krypteret under hele transmissionen (infrastrukturen), og (iii) at indholdsdata først dekrypteres hos den rette modtager efter modtagelsen.

Overvejelser vedrørende kryptering

Når der anvendes kryptering til at sikre en datatransmission, er det relevant at overveje:

- Om der anvendes en løsning baseret på en anerkendt krypteringsalgoritme.
- Om der bruges krypteringsnøgler af tilstrækkelig længde.
- Om adgangen til krypteringsnøgler fx skal være beskyttet af password.
- Hvorledes krypteringsnøgler og passwords, som beskytter adgangen til krypteringsnøgler, skal distribueres.

Ved at vælge en løsning til kryptering af datatransmission, baseret på en anerkendt krypteringsalgoritme, drager man nytte af akkumuleret viden, og man kan benytte en krypteringsalgoritme, som har vist sit værd i praksis.

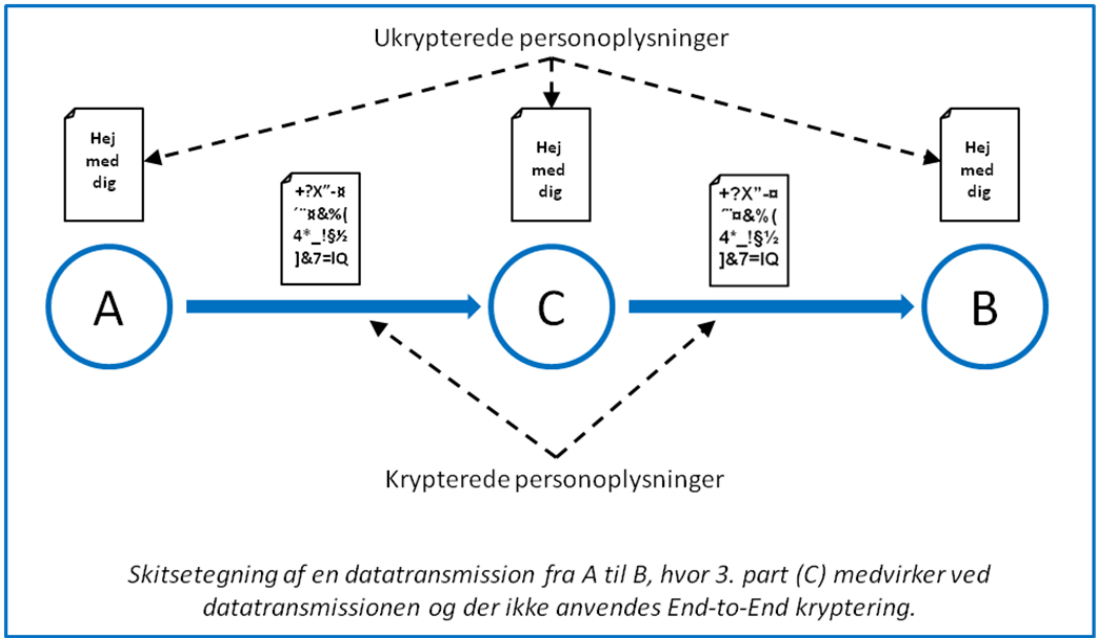
Hvad der på et givet tidspunkt anses for at være en tilstrækkelig længde af krypteringsnøgler, er noget, der ændrer sig over tid i takt med den teknologiske udvikling. En for kort nøglelængde vil resultere i en svag kryptering, der nemt kan brydes. En væsentlig faktor i vurderingen af krypteringsnøglens længde er den tidsperiode, hvori personoplysninger skal være beskyttet, hvilket normalt strækker sig langt ud over selve transmissionstiden. Beskyttelsesbehovet strækker sig ofte over flere år.

I nogle situationer anvendes passwords til at give adgang til brug af krypteringsnøgler. Et sådan password må som udgangspunkt ikke være nemmere at gætte end den krypteringsnøgle, som passwordet giver adgang til, og det skal beskyttes lige så godt som krypteringsnøglen. Et password, som er for kort, eller som ikke har en tilstrækkelig kompleksitet, vil relativt nemt kunne brydes og dermed give adgang til krypteringsnøgler. I praksis kan der fx forekomme situationer, hvor der anvendes svage passwords fx fordi de er korte, og i disse tilfælde kan andre kompenserende sikkerhedsforanstaltninger tages i anvendelse. Der kan fx træffes sikkerhedsforanstaltninger, som begrænser antallet af forsøg til at indtaste password. Hvilke andre sikkerhedsforanstaltninger, der evt. skal etableres ved anvendelse af password fx med kort længde, må den dataansvarlige vurdere ud fra den konkrete situation.

Krypteringsnøgler og passwords, som giver adgang til krypteringsnøgler, skal distribueres på en sikker måde. Hvordan det udføres, må den dataansvarlige tage stilling til ud fra de konkrete forhold. Det er fx ikke sikkert at sende disse i en ukrypteret e-mail

Medvirken fra 3. part

I det følgende betragtes et mere komplekst scenarie, hvor personoplysninger overføres fra afsender (A) til modtager (B) via en medvirkende 3. part (C). I scenariet krypteres personoplysninger før afsendelse fra afsender (A) og dekrypteres efter modtagelse hos 3. part (C). Personoplysningerne forekommer ukrypteret hos 3. part (C) i et vist tidsrum. 3. part (C) krypterer personoplysningerne i forbindelse med videre overførsel til modtager (B) og modtager (B) dekrypterer personoplysningerne efter modtagelse.



Skitsetegning af en datatransmission fra A til B, hvor 3. part (C) medvirker ved datatransmissionen og der ikke anvendes End-to-End kryptering.

Figur 3

Hvis man er dataansvarlig i et sådan eller lignende scenarie, er der yderligere overvejelser at gøre om risici og sikkerhedsforanstaltninger. Sikre løsninger vil normalt tillige blive mere komplekse og vanskeligere at implementere og administrere i denne type scenarie.

Med i den dataansvarliges overvejelser bør også indgå, at 3. parten (C), som medvirker ved datatransmissionen, måske også kan udføre lignende opgaver for andre (i det følgende betegnet kunder).

Yderligere risici, der kan opstå i et sådan scenarie kan være, at:

- Den dataansvarlige har utilstrækkelig kontrol med 3. parten (C).
- Uvedkommendes adgang til dine ukrypterede data hos 3. parten (C).
- Andre kunders adgang til dine data.
- Samme krypteringsnøgle og/eller password benyttes til flere kunder hos 3. parten (C).

Som dataansvarlig kan det være vanskeligt at finde ud af, præcis hvem hos en 3. part (C) der har adgang til dine ukrypterede data.

Hvis 3. parten (C) også behandler data for andre kunder, kan der være risici i forbindelse med tilstrækkelig adskillelse af forskellige kunders data. Andre kunder kan måske få adgang til dine data eller omvendt, fx ved en teknisk eller menneskelig fejl hos 3. parten (C).

Hvis det er 3. part (C), der administrerer og distribuerer krypteringsnøgler og passwords, kan der være en risiko for, at samme krypteringsnøgle og/eller password bliver anvendt til andre kunder.

En mere detaljeret risikoanalyse vil i de fleste tilfælde være nødvendig for at afdække risici forbundet med 3. partens (C) medvirken i en datatransmission.

I situationen med 3. parts (C) medvirken ved datatransmission introduceres der yderligere risici, og det vil derfor være nødvendigt at indføre modsvarende sikkerhedsforanstaltninger for at sikre mod uvedkommendes adgang til data.

- Der vil typisk være behov for at indgå aftaler med 3. parten (C). Aftalerne skal leve op til kravene til databehandleraftaler i persondataloven[5] og for offentlige dataansvarlige tillige sikkerhedsbekendtgørelsen[6].
- Den dataansvarlige skal ligeledes overveje, hvorledes det kan sikres, at data holdes adskilt fra andre kunders data.
- Den dataansvarlige skal endvidere sikre sig kontrol med, hvem der undervejs evt. har adgang til data i ukrypteret form.
- Distribution af krypteringsnøgler og passwords skal være under den dataansvarliges kontrol, således at den dataansvarlige har kontrol med, hvem der kan få adgang til at dekryptere data eller kan få mulighed for at dekryptere data og hermed få adgang til personoplysninger.

Er situationen, at der anvendes mere end én 3. part i en krypteret datatransmission, eller at 3. parten (C) anvender underleverandører, vil kompleksiteten og risici øges yderligere. De sikkerhedsforanstaltninger, den dataansvarlige skal indføre, øges modsvarende. Dvs. løsningen bliver endnu vanskeligere at implementere og administrere på en sikker måde.

Anbefaling

For at sikre personoplysninger bedst muligt under datatransmission anbefaler Datatilsynet anvendelse af End-to-End kryptering. End-to-End kryptering er, håndteret på rette måde, særdeles sikker.

End-to-End kryptering eliminerer de omtalte yderligere risici i situationen, hvor en 3. part (C) medvirker ved datatransmissionen. End-to-End kryptering forebygger også yderligere risici i den situation, hvor en ukendt part medvirker ved datatransmissionen, fx en ukendt underleverandør til 3. parten (C).

www.datatilsynet.dk
dt@datatilsynet.dk
(+45) 3319 3200

DATATILSYNET

[5] Persondatalovens § 42, stk. 2
[6] Sikkerhedsbekendtgørelsens § 7