Datasikkerhed

Retningslinjerne for personfølsomme oplysninger

Institut for Folkesundhed

Aarhus Universitet

Institut for Folkesundhed
Datamanagement, nsb
Version 1.0
2015

Indholdsfortegnelse

1 Introduktion

De data, der anvendes ved Institut for Folkesundhed, til registerforskning eller undersøgelser, er omfattet af Persondataloven, EU's Databeskyttelsesdirektiv, samt en række bekendtgørelser, som der kan læses om her: http://www.datatilsynet.dk/lovgivning/introduktion/

Derfor er det vigtigt, at gøre sig det klart, at man ikke udenvidere kan gå i gang med at tilegne sig data og anvende disse data i sin forskning. Det først man løber ind i loven er:

> Lov nr. 429 af 31. maj 2000 om behandling af personoplysninger indeholder i kapitel 12:
>
> **"Som hovedregel skal enhver behandling af personoplysninger, som omfattes af loven, anmeldes til Datatilsynet, inden behandlingen iværksættes."**
>
> Kilde: https://www.retsinformation.dk/Forms/R0710.aspx?id=849

Dette betyder, at det skal fortages en anmeldes til Datatilsynet, hvorefter man kan få en tilladelse.

Der er dog visse tilfælde, hvor en anmeldes til Datatilsynet ikke er nødvendigt:

> Lov nr. 429 af 31. maj 2000 om behandling af personoplysninger indeholder i kapitel 12.
>
> "Myndigheden skal kun anmelde de *behandlinger af personoplysninger*, som myndigheden er dataansvarlig for. Der er ingen pligt til at anmelde behandlinger, der alene omfatter anonyme oplysninger. Ifølge lov om behandling af personoplysninger § 3, nr. 1, forstås ved personoplysninger »enhver form for information om en identificeret eller identificerbar fysisk person (den registrerede)«.
>
> Ved »identificerbar person« forstås en person, der direkte **eller indirekte** kan identificeres, bl.a. ved et identifikationsnummer eller et eller flere elementer, der er særlige for en given persons fysiske, fysiologiske, psykiske, økonomiske, kulturelle eller sociale identitet."
>
> Elektronisk behandling af oplysninger om bestemte personer vil være omfattet af lovgivningen, uanset om personerne kun er bipersoner i behandlingen.
>
> Kilde: https://www.retsinformation.dk/Forms/R0710.aspx?id=849

Skal du anmelde det du vil foretage dig til Datatilsynet, så kan man benytte dette link til at komme i gang: http://www.datatilsynet.dk/blanketter/om-blanketter/

Nogle undersøger, dataadgange og databehandlinger kan endvidere kræve flere tilladelser fra andre myndigheder f.eks. Danmarks Statistik (DST), Landspatientregistret (LPR), Seruminstituttet (SSI), De praktiserende lægers og regionernes fælles enhed for kvalitetsudvikling (DAK-E), Klinisk Epidemiologisk Afdeling (LABKA), Den videnskabsetiske komite etc.

Ud over Datatilsynet m.f. tilladelser, så kan der også være krav om interne tilladelser fra instituttet, som kan være alt fra vejleder til institutlederen. F.eks. er alle aftaler vedr. Danmarks Statistik underlagt institutlederen, som er ansvarshavende for disse aftaler.

Som det fremgår af ovenstående, så er der mange forholde, der skal tages i betragtning og hvor overtrædelser kan være omfattet af forvaltnings- og straffeloven, samt instituttets sikkerheds- og ansættelsespolitik.

Derfor, spørg først din leder og få evt. vejledning i Datamanagement gruppen inden du går i gang.

2 Sikkerhed i praksis

Når alle tilladelserne er på plads, så står du med flere praktiske problemer, som der skal tænkes over. Dette vil typisk være spørgsmål som:

- Hvordan sikre man sig?
- Hvordan opbevare jeg data?
- Hvordan sender jeg data?
- Hvem må se mine data?
- …

Det er der ikke et endegyldigt svar på dette og listen af skandaler, hvor det er gået galt, er er om end, meget lang - selv om der også disse steder har været gjort mange tiltage for beskytte personfølsomme oplysninger.

Men, i dette afsnit er der givet er række forslag til, hvor da du selv kan mindske risikoen for sikkerhedsbrister og hvordan du kan minimere de evt. skader, som en brist kan medfører.

2.1 Kan du undgå at dine data er personfølsomme?

Data kan være personfølsomme på flere måder:

1. Der indgår et cpr. Nummer.
2. Der indgår navn, adresse, tlf. nummer, e-mail etc.
3. Personer er med på billeder eller er på anden måde visuelt genkendelige.
4. Oplysningerne er anonyme, men enkelt personer kan afledes af data.

Der hvor vi gerne skal hen med vores data er, hvor (hvis det er muligt):

5. Oplysningerne er anonyme og oplysningerne er ikke umiddelbart identificerbare.
6. Data er aggregerede, f.eks. et gennemsnit af mindst 5 personer.

Betragt nummereringen, som en rangliste for størrelse af dit sikkerhedsproblem.

Kan du komme længere ned på listen, så falder risikoen for skader efter en evt. brist.

Men andre ord: Opbevar mindst muligt oplysninger, der er personfølsomme!

2.2 Kan du anonymiserer dine oplysninger?

En måde at øge sikkerheden på er en om kodning af de personfølsomme oplysningerne.

Oftest er det ingen grund til at bruge f.eks. er cpr-nummer, som nøgle til observationer. Du kan ligeså godt anvende en krypteringsalgoritme, som generer et nyt unikt nummer, som ikke direkte er sporbar. Eller endnu bedre kalde dem 1, 2, 3…, de der så ikke kan regnes baglens til et cpr-nummer.

Hos Danmarks Statistik (DST) bruger de f.eks. et pnr-nummer, som er en krypteret udgave af et cpr-nummer.

Dette betyder ikke, at krypteringen ikke kan brydes, men at det mere besværligt at komme til oplysningerne, for dem, der ikke har reelle hensigter.

DST kræver derfor f.eks. også at pnr-numre behandles som cpr-numre!

Du kan også overveje om det er nødvenligt, at du kende f.eks. den præcis adresse på en person - måske er en kode for en kommune eller en region nok til, at du kan lave din undersøgelse?

Tænk hele tiden på: Hvad er det mindste, som du behøves at vide – og kan du omkode eller krypterer?

2.3 Hvem skal vide hvad?

Når du har gjort dine data mest mulig uinteressante og uanvendelige for udeforstående, ved dataerne kun indeholder den mindst mulige mængde information, som du har brug for, så skal du overveje; hvordan du mindsker spredningen af dine fortrolige data – og ikke mindst i hvilken form du evt. spreder dem.

Tænk på: Behøves det næste led i kæden at vide lige så meget, som dig?

Behøves dine samarbejdspartnere, at have alle data om enkelt personer – eller er det nok, at de f.eks.:

- *Kun har aggregerede data, med mindst 5 personer i en gruppering?*
- *Er det nok, at de f.eks. kun kender gennemsnitsværdierne for f.eks. en kommune?*
- *Kan navne, adresser etc. være erstattet med en kode?*
- *Kan værdier være erstattet med et interval?*
- *Behøves datatabeller - eller er f.eks. et histogram nok?*
- *Er alle variable i en f.eks. tabel nødvendige?*

Dette princip er kendt, som ”Need to Know Security Policy” og det er meget effektivt, når data skal forlade kilden. Dette skyldes, at informationerne bliver mere og mere ubrugelige, for udenforstående, når de komme væk fra kilden, fordi informationsindholdet gøres mindre, hver gang et nyt led eller et nyt spor kommer til.

2.4 Hvordan mindskes spredning?

Kopier er generelt noget skidt, da du oftest kun har fokus på en af kopierne af gangen – de andre ”ligger bare og flyder - til fri afbenyttelse for andre!”

Tænk på: Færrest mulige kopi er mere sikkert mod spredning!

Nå du giver en kopi til nogen, hvor mange kopier bliver de data, som du har ansvaret for så til?

- *Behøves du at give en kopi?*
- *Kan andre nøjes med at se data hos dig?*
- *Kan data bevares central med adgangskontrol?*

Ved at tænke på denne måde, så mindsker du spredningspotentialet meget mere effektivt.

Danmarks Statistiks forskermaskiner benytte f.eks. dette princip, hvor data ligger central og sikkert – og alle der har lov til at se dem skal igennem en overvåget adgangskontrol. Der er samme princip som bruges f.eks. til en bankboks, hvor der er flere led af kontroller inden nogle kommer frem til indholdet.

2.5 Hvem har adgang til data?

Allerede når du ansøger om at opbevare personfølsomme data, så skal du redegøre for, hvem der skal have adgang til disse data. Det betyder kort og godt, at ingen andre skal kunne få adgang til disse data – og at du ikke må videregive disse data til nogen uden for denne sluttede kreds, som er omfattet af tilladelsen.

Her skal du tænke på:

- *Kan nogen komme ind på dit kontor og tilegne sig dine informationer?*
  (Kommer der nogen f.eks. og gør rent, når du er gået hjem?)
- *Er adgangen til opbevaringsstedet aflåst?*
  (Hvem har en nøgle?)
- *Er informationerne låst inde i f.eks. skab, når du er på toilettet eller til kaffe?*
  (Låser du din computer, når du går fra den?)
- *Har du en kopi der hjemme til godnat læsning?*
  (Hvem holder øje med den kopi, når du er på arbejde?)
- *Hvad sker der, hvis nogen stjæler din PC eller du glemmer den toget?*
  (Er din harddisk krypteret?)
- *Hvor ligger du dine nøgler?*

Ved at tænke sig lidt om, så kan man hurtigt øge sikkerheden ved, at gøre adgangen mere besværlig for udenforstående.

Tænk på: Flere låse er bedre!

Husk: Selv om man er paranoid – så bliver man helt sikkert forfulgt!

2.6 Hvordan ser dine data ud for andre?

Vores data indeholder typisk ordnede koloner og rækker, som er fyldt med vigtige informationer.

For at gøre forståelsen nemmere for os selv, så bruger vi f.eks. gerne bekvemme variable navne, etiketter med forklaringer, fysiske enheder, standardkoder etc.

Men, det gør det også let for uvedkommende hurtigt, at skabe sig et overblik over om informationerne har en værdi for dem. Hvis disse forklaringer ikke er tilstede, så har vi kun en bunke intetsigende tal og koder i rækker og koloner. Hvem kan bruge dem til noget?

Variable	**Værdi**	**Enhed**
Vægt	72	Kg
Højde	174	cm
Køn	K	K/M
Alder	41	År

	72	
	174	
	0	
	41	

Derfor kan man overveje om ”intetsigende data” er en mulighed, for at beskytte sig. Eller om disse ”ekstra oplysninger” kan opbevares et andet sted og bruges som en slags ”nøgle” til informationerne.

2.7 Jamen, er der virkelig nogen, der gider at stjæle mine data?

Som svar på dette, så er her et eksempel på, hvad der er sket:

”En kommunen fik indbrud, fik brækket et brandsikkert skab op og fik stjålet få cpr-numre, navne, adresser etc. fra de personer, som havde bestilt et nyt kørekort i den forgangene uge”

Ja, oplysningerne har en værdi for andre, der ikke har reelle hensigter, da oplysningerne kan misbruges til kriminalitet eller kan videresælges. Typisk til net svindel og identitetstyveri.

Dette er frygteligt for dem der går ud over - og derfor har vi en ekstra moralsk forpligtigelse til at beskytte dem, der har stillet deres data til rådighed for vores forskning.

2.8 Hvem har egentlig ansvaret?

Når du arbejder med personfølsom data, så gælder loven:

Individdata er fortrolige, jf. Forvaltningslovens § 27, stk. 3 og straffelovens §152.

Så det er **dig**, der arbejder med data, som har ansvaret – under straffeansvar!

3 Opbevaring af digitale data

Indtil videre var vi kun talt om at minimere spredningen af informationer og i at begrænse værdien af informationernes værdi overfor udeforstående. Vi har ikke engang være inde på emnet "Edb-systemer" endnu.

Digitalisering gør det både nemmere for os – og for dem, der uretmæssigt vil tilegne sig vores data!

Det har aldrig været nemmere at lave et indbrud, for at skaffe sig data, end efter digitalisering. I de fleste tilfælde så opdager vi faktisk aldrig, at vi er blevet bestjålet – eller mere præcist kopieret!

Det er derfor, at gode gamle metoder fra oldtiden, som der er nævnt flere af overfor, stadig er brugbare: skjul, minimer, nøgler, krypter, besværliggøre etc. etc.

3.1 Sikkerhedszoner

Når vi taler om digitale sikkerhed, så er der som udgangspunkt forskellige sikkerhedszoner, som vi kan befinde os i:

1. **Lukkede netværk**
   Dette er netværk, som er 100% lukkede for omverden.
   Det er f.eks. sådan nogen som PET eller Forsvaret bruger.

2. **Lukkede netværk, med tunnel adgang**
   Her kan man komme ind igennem kryperede tunneler, hvis man er en godkendt bruger.
   Når du logger på, så sender serveren dig en brugerflade, som er uafhængig af din computer.
   Dette kan f.eks. være Danmarks Statistiks Forskermaskiner.

3. **Beskyttede netværk**
   Dette prøver man typisk at have i firmaer, det offentlige og på AU.
   Her er alle brugere kendte og har et login.
   Du har f.eks. direkte adgang til et netværksdrev, en printer etc., når du logget i på nettet værket.
   Når du er uden for det fysiske netværket har du ingen adgang, med mindre man acceptere VPN.

4. **Hjemme netværk**
   Her har man et udefineret sikkerhedsniveau.
   Typisk kan man komme på uden adgangskontrol.
   Folk på gaden kan komme på via f.eks. dit trådløse netværk.
   Selv om du bruget kryptering etc. så er det nemt at bryde ind.

5. **Internettet / Hotspots**
   Hvad der er her – det har alle, hvis de vil havde det!
   Typisk kan man komme på uden reel adgangskontrol.
   Dette kan være biblioteker, tog, hoteller, lufthavne etc.

Som du sikkert kan fornemme, så er det nemmere at være datatyv, nogle steder end andre. Der hvor det er nemmeste er der selvfølgelig også flest. Men de bedste møder du, hvor du mindst venter det.

Så lad være med at tage fortrolig data med hjem på dit hjemmenetværk, hvis du vil sidde derhjemme og arbejde med data. Brug som minimum en VPN adgang og Fjernskrivebord til din PC på AU. Her er der i det mindste nogle IT medarbejder på AU, som forsøger deres bedste for at hjælp dig med sikkerheden.

Du skal nøje overveje, hvor du befinder dig - og hvor du bevæger dig hen med dine handlinger!

Der er her i "Sikkerhedszonerne", at du ubevist kan komme meget galt af sted og f.eks. overtræde sikkerhedsbestemmelser, retningslinjer, lovgivningen m.m.

Downloader du f.eks. et datasæt fra Danmarks Statistiks Forskermaskiner, som du har adgang til via en tunnel, fra en PC på AU. **Så har du overtrådt reglerne og brudt loven!**

Eksemplet her får bl.a. de konsekvenser at hele instituttets adgang til Danmarks Statistik bliver lukket ned for samtlige medarbejdere, på ubestemt tid, hvis bare én medarbejder gør noget galt. Man, risikerer desuden at blive politianmeldt for at bryde loven!

Når du får tilladelser til at opbevare, indsamle eller se på data, så er der altid krav til hvor, hvem og hvordan du må bruge informationerne.

3.2 Opbevaring af data

Du skal her gøre dig helt klat, hvilken sikkerhedszone du er i og gør dig bevist om, at du ikke ubevist kommer til at skifte til en på et laverer niveau.

Der er mange typer at medier, som du kan gemme dine data på, men de er heller ikke lige sikre at anvende.

Lokale medier. Du skal her være opmærksom på at slettede data ofte kan gendannes af eksperter. Dette kan f.eks. gøres med data på USB-stick, harddiske, memory-cards, re-writeble cd'er og dvd'er etc. Efter brug skal disse fysisk ødelægges for at det ikke fortsat vil være data på dem.

Smid aldrig selve harddisken ud fra en gammel PC, som du har haft fortrolig data på. En ny harddisk kost få hunderede kr. Destruer den gamle harddisk inden du smider PC'en ud, sælger den eller giver den væk. Dette punkt har ofte været kilden til skandaler! Det samme gælder for de andre lokale medier.

Netværksdrev er oftest beskyttede og adgangsbegrænsede til nogle bestemte brugere. Men, det er ikke altid gennemskueligt, hvem disse brugere er. Her bliver der typisk også taget backups – men, hvor bliver den backup af og hvem har adgang til den?

Skydrev. Skydrev eller internet drev som de også kaldes, f.eks. DropBox er meget populære – men, hele verden har en "ledning" til dem og du har ingen kontrol over, hvad der sker med data på disse drev. Google f.eks. på et tidspunkt, at de havde ret til at tilgå og bruge data, som var lagret hos dem!

Windows 8 har nu f.eks. som standard "internet profiler" og "OneDrive", hvilket vil sige at dine data etc. bliver gemt på en server ude i verden, så kun kan få adgang til dem, når du logger ind på en anden maskine!

Alt hvad der er smart og har en forbindelse til **internettet** er meget sårbart og det er umuligt at gennemskue, hvad der ske med data disse steder og når de løber rundt i netværkskablerne et sted i mellem din PC og et ukendt sted i verden. DropBox ligger f.eks. data på servere i US. Endnu være er det, hvis der er trådløse forbindelser involveret, så bliver alt sendt i alle retninger!

For at give et eksempel på, hvad der sker, som de fleste ikke tænker over – er logninger!

- Alle teleselvskaber er pålagt at logge netværkstrafik ved lov!
  (Dvs. at der er kopier derude af alle dine emails, downloads etc.)

- Som eksempel på, hvor meget det logges, så kan vi bruge et tal fra NSA i US.
  I 2008 rundede NSA, alene, logning af data svarende til alle informationer, der er i kongressens bibliotek (det største bibliotek i verden). Det var så ikke i løbet af 2008 – men, i minuttet i 2008!

Dette er kun eksempler på hvad "the good guys" gør – men, "the bad guys" de kan mindst lige så meget.

Derfor tænk dig meget grundigt om inden du bruger internettet til at gemme eller flytte dine fortrolige data – og endnu bedre lad være!

3.3 Min egen PC

Man kan forstille sig, at man udelukkende har sine data på sin egen PC og kun arbejder med data her direkte fra en DVD, som man tager ud og låser inde når man er færdig.

Det kunne man fristes til at tro at dette absolut må være det sikreste.

Men, her er der igen mange forholde som gør sig gældende:

1. Din PC kan være på nettet:
   a) Så er døren åben for hackning, loggers, trackers etc.
   b) Dine data bliver måske, uden du ved det, kopieret til nettet af "backup" programmer etc.

2. Din programmer kopiere dine data til f.eks.:
   a) Undo-data for at du kan lave "fortryd". Disse data ligger f.eks. skjult i Word-filer.
   b) Gennemer kopier data i lokale file, der er optimeret for hurtig databehandling.
   c) Gemmer kopier i Windows "swap" fil.

3. Din PC bliver stjålet!

4. Din PC går i stykker og bliver sendt til reparation!

Hvis du har personfølsom data på din PC – så bør den som minimum have en krypteret harddisk!

Der findes værktøjer som kan kryptere en hel harddisk, så ikke en gang Windows kan startes før et password er indtastet. Men andre ord, så er det første du ser på skærmen, når du tænder PC'en en besked om at indtaste dit password eller identificerer dig med f.eks. fingeraftryk. Her er ALT på harddisken krypteret.

Vi kan kun opfordre til, at har du personfølsom data eller skal have det, så kontakt Datamanagement, som kan hjælpe dig - eller Datamanagement kan få AUs IT-sikkerhedsfolk til rådgive i de konkrete tilfælde, når der skabt et overblik over problemstillingen.

4 Flytning af data

Ofte kommer vi i den situation, at vi bliver nydt til at flytte vores data eller at vi skal dele informationer med andre i vores arbejdsgruppe, som vi vil sende informationerne til.

De største risikoer for at du får kopieret dine data er, når du flytter dem!

Her er det nøjagtig som i de gamle film, hvor guldet skal transporteres fra Tower of London (A) til Fort Knox (B) – røveriet sket 95% af gangene under transporten, hvor guldet er ud for porten til fæstningen.

Det samme gør sig gældende for digitale data – forskellen er bare at vi ofte ikke ved, hvornår vi er inden og uden for fæstningen - og hvad vi faktisk gjorde for at komme fra A til B. Eller om vi blev "røvet" under vejs!

4.1 E-mails

Det er meget almindelig at vedhæfte og sende en fil med en e-mail. Det er nemt og der er hurtigt.

MEN, dette er ligesom i "Hans og Grete", så ligger du brødkrummer hele vejen ud igennem skoven, som kragerne gladelig spiser!

Her er det bare kopier af din e-mail og vedhæftede filer, der ligger kopier af på hver eneste server, som e-mail er kommet forbi fra A til B. Det kan bliver til mange kopier, som du ingen kontrol har over.

4.2 Dropbox og lign.

En anden almindelig mulighed er en aftale om, at filen bliver lagt i en delt Dropbox.

Her skal man for det først være opmærksom på at Dropbox betragtes af Datatilsynet som en tredjeparts databehandler – dette kræver, at Datatilsynet har givet tilladelse til dette. Her er det også vigtigt at man er klar over at Dropbox befinder sig uden for EU, hvilket i sig selv giver et andet juridisk grundlag.

Dropbox er blevet hacket flere gange – og oplysninger er blevet spredt herfra. Så lad være!

4.3 Streaming, FTP, delte mapper etc.

Her er der typisk ingen kryptering eller standard krypteringer - og det er meget nemt at tappe informationerne tusindevis af steder på ruten fra A til B.

Når banditterne har en kopi – så betyder det ikke noget for dem, at det tager et par dage at knække koden.

4.4 Gammeldags Post (snail-mail)

Dette er trodsalt i dag mere sikkert end elektronisk distribuering – men, dette går også galt.

Statistikken viser at mange pakker i "CD/DVD-æsker" forsvinder i postsystemet, da de formodes at indeholde let omsættelige musik, spil eller film.

Det er derfor ikke sikkert at dine data var det primære mål – men, nu er de havnet derude!

Vi har f.eks. selv oplevet at data sendt fra SSI til DST på DVD forsvandt under!

4.5 Sikker transport – hvad gør jeg?

Her gælder først alt, hvad der stod i afsnitet "2. Sikkerhed i praksis", for både elektronisk data og papir data, og det der stod i afsnit "3. Opbevaring af digitale data". Altså:

- Minimer værdien af indholdet for udenforstående

- Gør tilgangen besværlig
- Fjern nøgleinformationer
- Krypter det hele

Herefter kan man overveje hvordan informationerne sendes mest sikkert.

En god gammel metode fra oldtiden er at dele sine informationer op i et antal pakker, som sendes af forskellige ruter med forskellige kurere. Ideen er her, at har man ikke alle pakkerne, så kan informationerne ikke genskabes.

Send derfor oplysningerne af flere omgange:

1. Delvise data i pakke 1, pakke 2… pakke N
2. Nøgledata i pakke N+1 (variable navne, enheder etc.)
3. Koder i pakke N+2 (koder til afkryptering)
4. Send gerne til forskellige adresser, e-mails etc.
5. Send pakkerne forskudt i tid.

Dermed bliver det yderst besværligt for udeforstående at opsnappe informationerne.

Dette princip bruges f.eks. i "Torrents", som er en metode som ofte bruges til at dele piratkopierede film, musik, software etc. Her kommer f.eks. en film som meget små krypterede bidder fra tusindvis af computere, der er fordelt ud over hele kloden. Til sidst ligges "puslespillet" hos modtageren og filmen er genskabt.

I vores tilfælde har vi ikke vores data liggende på tusindvis af computere, men forhåbentlig kun på en. Derfor kan vi ikke direkte bruge "Torrent" metoden. Men, vi kan gøre noget lignende ved at splitte vores data op i mange små krypterede bidder og sende dem forskudt i tid.

Der findes mange programmer, der kan hjælpe med dette. Her er bare et simpelt forslag:

1. "Splitting Zip Files", www.7-zip.org
   Programmer som 7-zip/winzip kan ligge en kryptering med kodeord på en pakket fil.
   Samt, de kan splitte en pakket fil op i et antal delpakker.

2. Send skjulte krypteringsnøgler

   

   Her over ses to billeder, af AU's logo.
   Men er de nu helt ens?
   Billedet til venstre indeholder en krypteret indlejring af krypteringsnøglen til de opsplittede zip-filer ovenfor, som endvidere er beskyttet med yderligere et password.
   Der gør billedet til højre ikke!
   Her er servicen http://mozaiq.org brugt.
   Denne service kan skjule tekst-informationer i billeder – og er gratis!

Vi kan så brænde de krypterede delfiler ned på DVD'er og sende dem af flere omgange med posten.

Eller nogle med email, andre med posten, et par stykker på et delt drev og de sidste med GLS.

Billedet så f.eks. i en email signatur – og password et givet mundligt i telefonen.

Hvem kan bruge en del af en krypteret fil – og hvor nøglen er skjult i f.eks. billede et sted på nettet?

På denne simple måde er det pludseligt ikke længere så nemt at være bandit, selv om det kun er gjort en meget lille indsats for at gøre en data-kapring særdeles besværlig.

5 Opsamling

Når du arbejder med personfølsomme data, så over vej altid mulighederne for:

- Loven og datatilsynets regler gælder
- Minimer informationerne i data til et minimum.
- Omkodning af variable til ikke identificerbar data, hvor det er muligt.
- Krypter dine opbevarede data og din computer.
- Undgår spredning af kopier og unødvendig information.
- Destruer medier, papirer etc. efter brug.
- Bliv i sikreste netværkszoner (f.eks. DST) og lås dine ting inde.
- Lav sikre forsendelser og overførsler af data
- Tænk over din adfærd!

Husk, at ansvaret er dit!