



LANDSORGANISATIONEN  
DANSKE DAGINSTITUTIONER

PERSONDATAFORORDNINGEN

# IT SIKKERHED OG IMPLEMENTATION

## Datasikkerhed

### Artikel 5F (Principper for behandling af personoplysninger)

Emne: Integritet og fortrolighed

- Personoplysninger skal behandles på en måde, der sikrer tilstrækkelig sikkerhed for de pågældende personoplysninger, herunder beskyttelse mod uautoriseret eller ulovlig behandling og mod hændeligt tab, tilintetgørelse eller beskadigelse, under anvendelse af passende tekniske eller organisatoriske foranstaltninger (»integritet og fortrolighed«).

Hvad betyder alt dette?

# IT SIKKERHED OG IMPLEMENTATION



## Citat:

"Sikrer tilstrækkelig sikkerhed"

## IT teknologi:

- ▶ Ikke rigtig nogen specifikation

## Graden af sikkerhed:

- ▶ 'Tilstrækkelig sikkerhed' i forhold til hvad?
- ▶ Hvordan skal denne sikkerhed vurderes? Målestok?
- ▶ Dataforordningen kan virke ret diffus mht. hvilke værktøj eller software der skal bruges
- ▶ Kom med et bud???

## Citat

"Beskyttelse mod uautoriseret eller ulovlig behandling"

## Områder f.eks.:

- ▶ Dokumenthåndtering systemer f.eks. Dropbox, OneDrive, Google drive...
- ▶ Dokumenter f.eks. Word, Excel, PDF...
- ▶ E-mail med følsomme data

## Beskyttelse:

- ▶ Login brugernavn/ adgangskode
- ▶ Adgangskode til Word, Excel, PDF...
- ▶ Kryptering af sendte/ modtaget e-mail
- ▶ Bog med koder i aflåste skab

## Citat

"Hændeligt tab, tilintetgørelse eller beskadigelse"

## Områder f.eks.:

- ▶ Operativ Systemer f.eks. Windows, MAC, Linux, Android...
- ▶ Interne/ ekstern HDD, USB-nøgler...

## Beskyttelse:

- ▶ Login brugernavn og adgangskode på alle OS brugerkontoer
- ▶ Kryptering og backup af data, harddisk og usb-nøgle
- ▶ Minimer fysisk transport og lagring af følsomme data i ubeskyttede systemer

PERSONDATAFORORDNINGEN

# IT SIKKERHED OG IMPLEMENTATION



## Tekniske foranstaltninger:

- ▶ Opdatering af operativ system, firewall, sikkerhedsprogrammer
- ▶ Perodeskift af login kode i anvendte IT-systemer
- ▶ Løbende backup af følsomme data
- ▶ Dokumentation og procedure for udformningskrav for de overnævnte

## Organisatoriske foranstaltninger:

- ▶ Begrænset uautoriseret personale (f.eks. begrænsede adgang til en login-konto)
- ▶ Løbende afholdelse af kurser/ info til personale omkring sikkerhedspolitik
- ▶ Clean Desk Policy
- ▶ Efterlevelse af kravene i forhold til beskyttelse/ behandling af personoplysninger (Compliance)

PERSONDATAFORORDNINGEN

# IT SIKKERHED OG IMPLEMENTATION



## Ansvarlighed:

Den ansvarlige skal være i stand til at dokumentere, at systemer og processer fungerer konsekvent og som tilsigtet !

**Vi siger, hvad vi gør – og kan forklare hvorfor !**

**Vi gør, hvad vi siger – og vi kan bevise det !**

# IT SIKKERHED OG IMPLEMENTATION



## Samlede overblik (IT):

- ▶ Bevidst omkring persondatahåndtering\*
- ▶ Øget sikkerhed mht. databeskyttelse\*\*
- ▶ Konkrete procedure/ dokumentation håndteringsprocesser

*\* f.eks. i forhold Cloud-tjenester og leverandører af disse services (dataansvarlig aftale)*

*\* Fokuspunkt for LDD i forhold til alle institutioner*

## Bevidst omkring datahåndtering:

- ▶ Hvem er ansvarlige for disse data?
- ▶ Hvem har tilgang til dem?
- ▶ Hvad er graden af sikkerheden (beskyttelse, logning, adgangskode, genskabelse, tab?)
- ▶ Gennemsigtighed og gennemskuelse?
- ▶ Risikovurdering/ konsekvensanalyse?
- ▶ Handling for tab af data inden for 72 timer?
- ▶ Procedure for datakontrol og sletning?

## Hvad skal der laves:

Behov/ vurdering af flere OS brugerkonto:

- ▶ Opret flere brugerkonto

Aktiver periodekodeskift:

- ▶ Sæt OS til at spørge efter ny kode hver 90 dage

Aktivering af BitLocker:

- ▶ Ændre BitLocker kryptering fra AES-128 til AES-256 bit

| Key size | Time to Crack                |
|----------|------------------------------|
| 56-bit   | 399 seconds                  |
| 128-bit  | $1.02 \times 10^{18}$ years  |
| 192-bit  | $1.872 \times 10^{37}$ years |
| 256-bit  | $3.31 \times 10^{56}$ years  |

Kryptering af intern OS harddisk:

- ▶ Krypter OS harddisk f.eks. C-drevet

Kryptering af eksterne harddisk/ usb-nøgler:

- ▶ Krypter eksterne HDD/usb-nøgle BitLocker AES-256

Installation af sikkerhedsprogrammer:

- ▶ Vurder nuværende sikkerhedsprogram/ evt. installere ny sikkerhedsprogrammer f.eks. Kaspersky Internet Security, Bitdefender, Symantic Norton Security eller andre
- ▶ Aktiver periodisk scanning af hele computeren

PERSONDATAFORORDNINGEN

# IT SIKKERHED OG IMPLEMENTATION



## Hvad skal der laves:

### Bekæmpelse af spyware og orme:

- ▶ Vurder nuværende spyware og orme bekæmpelse/ evt. installere nye software f.eks. Malwarebytes (anbefaling)
- ▶ Aktiver periodisk scanning af hele computeren

### Office 2016 eller 365 & sikker mail:

- ▶ Installation af Microsoft Office 2016 eller 365
- ▶ Installation af medarbejdersignatur
- ▶ Opsætning af Outlook i forhold Gmail, Yahoo-mail, Hotmail eller Domæne-mail
- ▶ Konfiguration af Outlook til at sende/modtage sikker mail

### Adgangskode på dokumenter:

- ▶ Undervis i at sætte koder på Word, Excel, PDF dokumenter
- ▶ Få udleveret en manual til det overnævnte

### Opdatering af/ tjek op på alle software:

- ▶ Microsoft Windows 10 Pro og MAC OS
- ▶ Sikkerhedsprogrammer f.eks. Kaspersky Internet Security 2018 og Malwarebytes
- ▶ Microsoft Office 2016 eller 365
- ▶ Aktiver genoprettelsesfunktion i Windows 10
- ▶ Fjern software, der potentiel kan skade computeren
- ▶ Fjernelse af Java

# IT SIKKERHED OG IMPLEMENTATION



## Kravspecifikation:

- ▶ En pc eller MAC, der understøtter AES-256 bit
- ▶ Sikkerhedsprogram
- ▶ Software til bekæmpelse af spyware
- ▶ Microsoft Windows 10 Pro eller MAC OS
- ▶ Microsoft Office 2016 eller 365
- ▶ Medarbejdersignatur (nøglefil)
- ▶ Gmail, Yahoo-mail, Hotmail (ingen garanti for sikkerhed/ data genskabelse) eller andet
- ▶ BitLocker AES-256 bit software

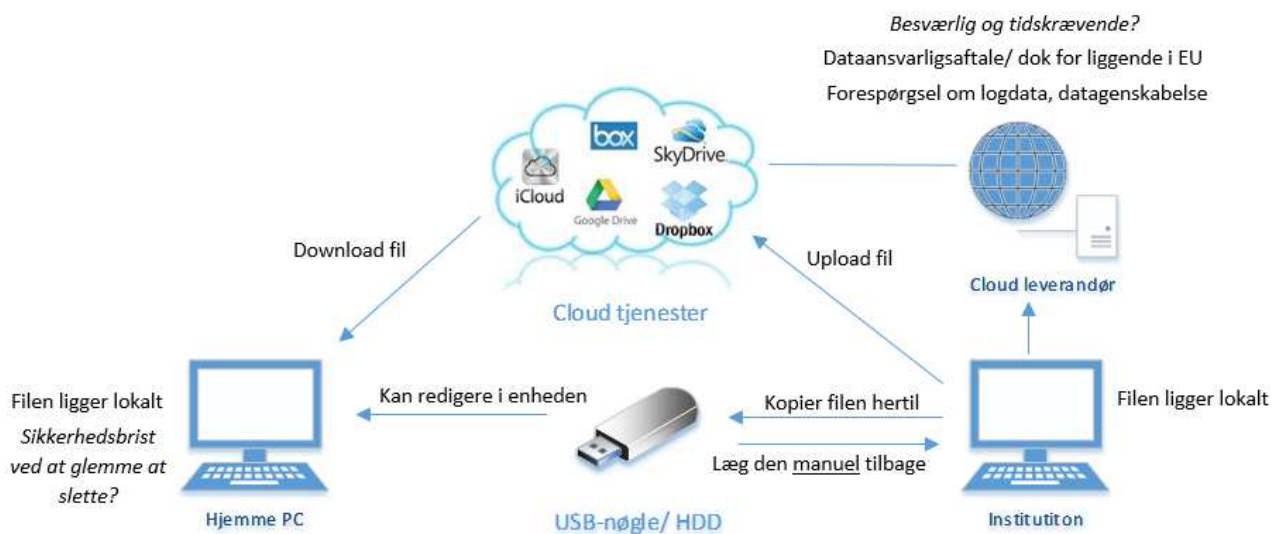
## Mulige geninstallation/ opgradering:

- ▶ Microsoft Windows 10 Pro\*
- ▶ Microsoft Office 2016 eller 365\*

\* Disse produkter understøtter AES-256 bit kryptering

## Overvejelse omkring Cloud-tjenester:

Google drive – OneDrive – Dropbox – Box – Amazondrive – iCloud ....m.m.



## Hvem skal vi kontakte???

Følgende skal være afklaret ved benyttelse af Cloud-tjenester:

- ▶ Elektronisk/ fysisk dokumentation for en dataansvarlig aftale med underskrift
- ▶ Elektronisk/ fysisk dokumentation for at tjenesten ligger inden for EU
- ▶ Genskabelse af tabte data
- ▶ Adgangs til eller forespørgsel på aktivitetslogging (ved kontrol)

# IT SIKKERHED OG IMPLEMENTATION



## Godt at vide:

- ▶ Bog med login kode skal ligge i et låst skab
- ▶ Følsomme data skal ligge struktureres af hensyn til overskuelighed og sletning
- ▶ Følsomme data skal opbevares krypteret i Outlook, men det er ikke forsvarlig at opbevare dem lang tid i Outlook (f.eks. af hensyn til sletning)
- ▶ Forældede data skal slettes via påmindelse. Der skal forelægge en validering for at disse data faktisk bliver slettet til tiden
- ▶ At kopiere følsomme dokumenter over til ens hjemme-pc er ikke anbefalet af hensyn til sikkerhed

## Godt at vide:

- ▶ At have følsomme oplysninger på en ikke-krypteret harddisk/ USB nøgler er ikke anbefalet eller forsvarligt
- ▶ Log altid ud af Windows eller MAC, hvis du ikke er tilstede eller i nærheden
- ▶ Husk altid at have en backup af følsomme dokumenter, hvis uheldet er ude (mulighed for genskabelse og kontakte de relaterede)

PERSONDATAFORORDNINGEN

# IT SIKKERHED OG IMPLEMENTATION



## Demo - Et fiktivt eksempel på hackning:

- ▶ Der har været indbrud på en institution, hvor tyven havde fået fat på en bærbar med følsomme oplysninger!
- ▶ Bærbaren havde adgangskode på, og tyven forsøger ihærdig for at logge ind, men den er godt beskyttet!
- ▶ Tyven havde også forsøgt at trykke på alle mulige knappe for at se, om han kan komme ind via andre veje, men nej !
- ▶ Hvad gør tyven for at komme ind til disse dokumenter???

PERSONDATAFORORDNINGEN

# IT SIKKERHED OG IMPLEMENTATION



## Demo - Et fiktivt eksempel på hackning:

Her er hvad han kan gøre:

- ▶ Hent et backup software:  
<https://www.acronis.com/en-us/personal/computer-backup/>
- ▶ Tag et backup af hele C-drevet på computeren over på en ekstern HDD
- ▶ Åbne backuppen på sin egen computer med samme program
- ▶ Naviger til dokument mappen/ skrivebord og kopier dem ud

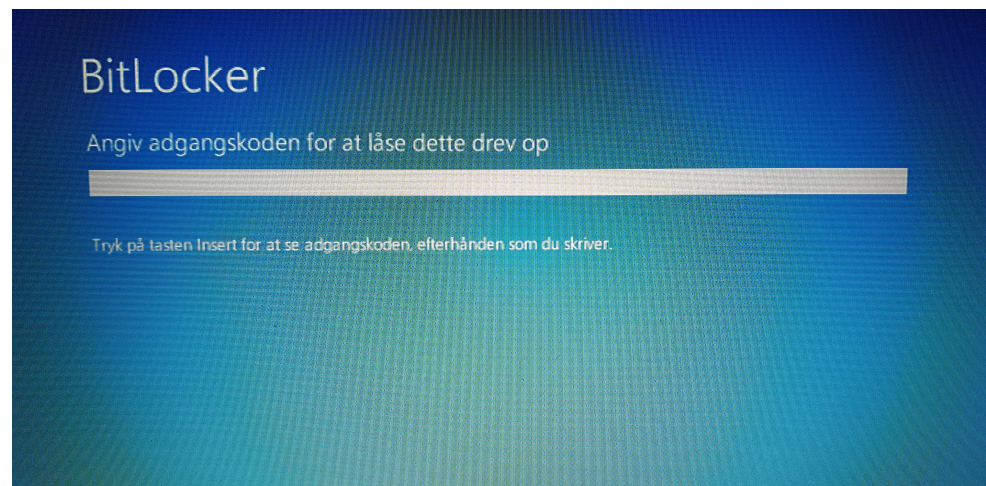
PERSONDATAFORORDNINGEN

# IT SIKKERHED OG IMPLEMENTATION



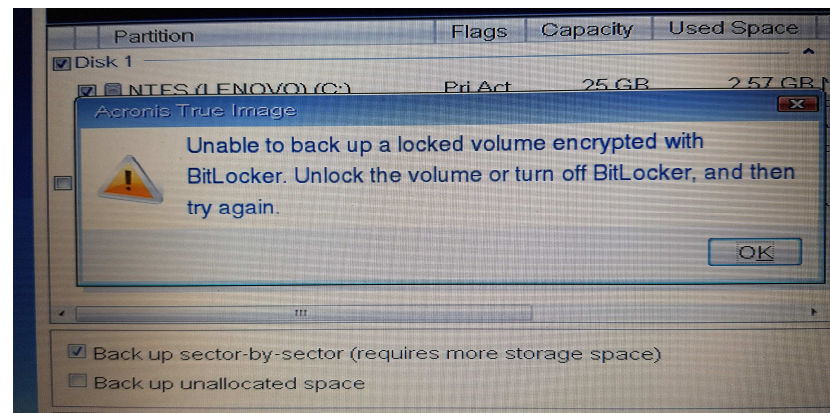
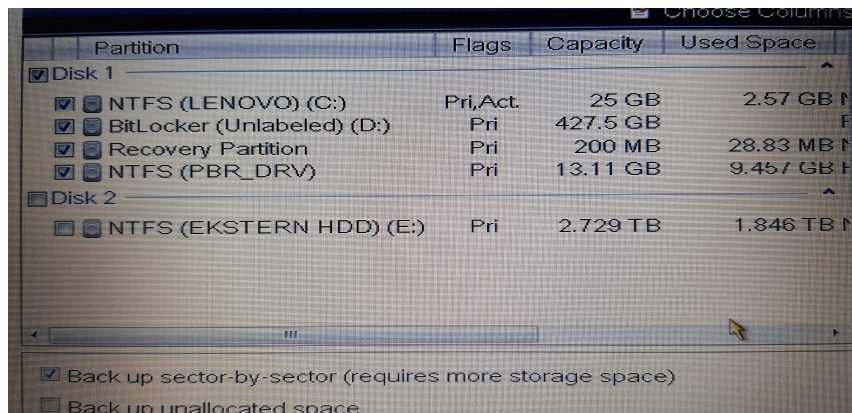
## Et krypteret OS harddisk:

Ingen adgang uden kode, og der kan IKKE laves en backup af disken !!!



## Et krypteret OS harddisk:

Ingen adgang uden kode, og der kan IKKE laves en backup af disken !!!



PERSONDATAFORORDNINGEN

# IT SIKKERHED OG IMPLEMENTATION



## Spørgsmål?

