# Sikkerhedsguide til behandlingssikkerhed af personoplysninger

Dette dokument kan bruges som en kort tjekliste til, om de overordnede krav til sikkerhed ved behandling af personoplysninger er opfyldt.

**1. Risikoanalyse af IT-systemer**

- I skal foretages en risikoanalyse af IT-systemerne, inden systemerne tages i brug. Hvis systemet allerede er i brug, skal I foretage en risikoanalyse af IT-systemerne inden 25. maj 2018. Dette kan i vist omfang afklares med IT-leverandøren.

**2. Fortrolighed skal sikres ved behandlingen af personoplysninger**

- Kun autoriseret udstyr og relevante medarbejdere (dvs. med et arbejdsbetinget behov) må have adgang til personoplysninger. Dette kan ske ved at tildele relevante medarbejdere et unikt login/adgangsrettighed til systemet.
- Når medarbejdere fratræder, skal der lukkes for adgangsrettigheder.
- Pseudonymisering og kryptering af personoplysninger.
- Hvis I overfører personoplysninger på det åbne internet, skal I sørge for at overførslen er sikker, evt. vha. kryptering.
- Fysisk sikkerhed (både af adgang til computere og andre enheder samt af printede personoplysninger, såsom notater og journaler mv.)
    - Låse og adgangskontroller på digitale enheder (computere, bærbare, telefoner mv.)
    - Fysisk sikring af bærbare computere (f.eks. låses inde når ikke i brug eller opbevares et sikkert sted)
    - Sørge for at printede personoplysninger opbevares i aflåst skab (nøgle skal ikke være tilgængelig for andre)
    - Sikre kontrol med og sikring af alle flytbare medieenheder (f.eks. USB og eksterne hardware)
    - Fjerne personoplysninger fra medieenheder før udsmidning
    - Fjerne personoplysninger fra harddiske på computere før udsmidning
    - Sikker opbevaring af back-ups
- Logning af adgang til IT-systemet og brugeraktivitet, herunder over fejlslagne loginforsøg og blokering af adgang ved forkert login (kan afstemmes med IT-leverandør).

**3. Integritet og tilgængelighed (afstemmes med IT-leverandør)**

- Det skal være muligt at validere, om personoplysninger på IT-systemerne er korrekte, pålidelige, nøjagtige og fuldstændige.
- Beskyttelse af netværk, systemer, logs og personoplysninger mod manipulation udefra.
- Sikring af gendannelse af personoplysninger ved sikkerhedshændelser.

**4. IT-systemets robusthed (afstemmes med IT-leverandør)**

- Der skal være et program for håndtering af sårbarheder i IT-systemet i forbindelse med behandling af personoplysninger. Programmet skal indeholde (men er ikke begrænset til) følgende tiltag:
    - Undersøgelse af sårbarheden
    - Test af sårbarheden
    - Opfølgning på undersøgelser og test

**5. Sikkerheds- og privatlivsteknologier**

- Anti-virus eller anti-malware software
- Firewall, anti-DDOS og intrusion detection

**6. Træning og sikkerhedstjek i forhold til medarbejdere**

- Baggrundstjek
- Introduktion til medarbejdere omkring informationssikkerhed og persondatareglerne

**7. Reaktion i forbindelse med hændelser og forretningskontinuitet**

- Information om og træning af medarbejdere i forhold til brud på persondatasikkerheden og sikkerhedshændelser (f.eks. information om hvordan og hvornår sikkerhedsbrud skal anmeldes til Datatilsynet, underretning af de personer, som er omfattet af sikkerhedsbruddet, hvordan sikkerhedsbruddet håndteres, konsekvenserne mv. – se Datatilsynets vejledning om håndtering af brud på persondatasikkerheden).
- Plan for at sikre forretningskontinuitet ved alvorlig sikkerhedshændelser, f.eks. ved hacking (dette kan være f.eks. ved brug af backup).

**8. Auditering**

- Auditering (undersøgelse og vurdering) af om jeres behandling af personoplysninger opfylder kravene
- Auditering af om jeres databehandleres behandling af personoplysninger på jeres vegne opfylder kravene
- Regelmæssig afprøvning, vurdering og evaluering af effektiviteten af IT-systemer og jeres egen behandling af personoplysninger
- Auditering skal ske mindst en gang årligt.