Vejledning til fastlæggelse og gennemførelse af ledelseskontrol

Generelt
Formålet med ledelseskontrol er at gennemføre kontroller, der påviser og dokumenterer,

- at institutionens retningslinjer for GDPR overholdes (retningslinjer skal være afstemt institutionens forhold og GDPR-regler i øvrigt – se trin 1 og 2 herunder)
- at retningslinjer hvis retningslinjer ikke overholdes eller fungere i praksis, at der foretages forbedringer.

Trin 1
Ledelseskontrol skal foretages med en fornuftig frekvens og dybde.
Kontrolpunkter bør tilrettelægges i forhold til hvad der er væsentligst / eller kan påvirke den registrerede mest, hvis noget går galt.

Eksempelvis kan det overvejes, hvor stor en risiko der er for, at personoplysninger kommer til uvedkommendes kendskab, fx hvis papirer ligger fremme. Det kunne også være risikoen for, at personoplysninger anvendes til andet end formålet, der indhentes for mange oplysninger, oplysninger gemmes for længe osv.

Trin 2
Ledelseskontrollens praktiske indhold planlægges. Her anbefales det, at den skabelon, der er stillet til rådighed, gennemgås og justeres, så den passer til de faktiske forhold i institutionen.
I skabelonen er de foreslåede kontrolpunkter opdelt i forhold til praktisk gennemførelse fx er alle kontroller vedrørende en fysisk gennemgang af lokaler samlet under et.

Trin 3
Når kontroller gennemføres, dokumenteres dette ved følgende

- en kort beskrivelse af, hvad der konkret er påset og resultatet af kontrollen
- hvornår kontrollen er gennemført
- hvilken forbedringer der evt. skal iværksættes
- hvornår forbedringer skal være gennemført

Trin 4
Der følges op på, om evt. forbedringer er gennemført
Det sikres at forbedringer om nødvendigt inkluderes i kommende kontroller.