Bilag 3 - Behandlingssikkerhed

inpadi indfører følgende særlige foranstaltninger:

- Mulighed for stærk kryptering af alle data, der opbevares hos inpadi.
- Mulighed for stærk kryptering af alle data, der sendes mellem inpadi og Kunden.
- Logning af alle behandlinger af Kundens data, herunder logning af, hvem der har foretaget behandlingen, formålet med behandlingen, hvad der præcis blev foretaget af behandlinger, tidspunktet for behandlingens påbegyndelse og afslutning.
- Indretning af alle de relevante af inpadis rutiner, så behov for adgang til Kundens data reduceres til tilfælde, hvor det er tvingende nødvendigt for at kunne løse opgaver for Kunden.
- Udførelse af løbende risikoanalyser, herunder ved opdatering til ny teknologi eller ændringer i arbejdsrutiner og sikkerheds-setup.
- Gennemførelse af mindst en årlig sikkerhedstest, der dokumenterer sikkerhedsniveauet.
- Sikre, at de af inpadis medarbejdere, der kan få adgang til Kundens data, er ansat efter en procedure, der sikrer, at medarbejderne ikke er tidligere straffet eller på anden måde udgør en sikkerhedsrisiko.
- I sine interne retningslinjer fastsætte regler, der sikrer, at inpadis medarbejdere kun har adgang til de af Kundens data, som er nødvendige for medarbejdernes udførelse af deres arbejdsopgaver.
- Sikre, at alle medarbejdere, der behandler Kundens data, er underlagt en tavshedspligt.
- Føre en ajourført liste over de medarbejdere, der kan få adgang til Kundens data.
- Skriftlige retningslinjer for medarbejdernes anvendelse af hjemmearbejdspladser og mobile enheder uden for inpadis kontor.

Leverer inpadi tillige egen/egne applikation(er) til Kunden, forpligter inpadi sig at designe sin/sine applikation(er) sådan, at de understøtter databeskyttelse bedst muligt, og sådan at brugerne via standardindstilling kan begrænse adgangen til data, så applikationen(erne) ikke uden udtrykkelig stillingtagen fra en administrator giver ubegrænset adgang til Kundens data.

Leverer inpadi tillige tredjemandsapplikation(er) til Kunden, forpligter inpadi sig til at sætte applikationen(erne) sådan op, at brugerne via standardindstilling kan begrænse adgangen til data, så applikationen(erne) ikke uden udtrykkelig stillingtagen fra en administrator giver ubegrænset adgang til personlig information.