

Checkliste til Tjenesteydere

	Emne:	Ja	Nej
1	Er tjenesteyderen ISO-certificeret		
2	Er data og programmer beskyttet opdaterede, anerkendte og dækkende anti-virus programmer?		
3	Har tjenesteyderen registreret hvilke medarbejdere, der har adgang til AKU-data?		
4	Følges det regelmæssigt op på, hvem der har adgang til AKU-data		
5	Er der etableret sikkerhedsforanstaltninger således, at uvedkommende ikke kan få adgang til oplysningerne?		
6	Er der taget forholdsregler imod at materiale og/eller programmel går tabt eller kan blive beskadiget?		
7	Bliver data og øvrigt materiale slettet makismalt et kvartal efter deltagelse i 4 panel?		
8	Foregår der SSL-kryptering af data/medie så længe de ikke er i DST's varetægt, og foregår intern datatransmission som sikker kommunikation med SSL-krypering eller tilsvarende standard?		
9	Sker al datatransmission fra tjenesteyderen til DST via en sikret FTP-platform?		
10	Leveres data i et record-layout, der overholder OIOXML standarden eller en tilsvarende standard?		
11	Er der taget forholdsregler imod at data går tabt eller kan blive beskadiget ifbm. transmissionen fra tjenesteyderen til DST?		
12	Er transmissionsforbindelsen mellem tjenesteyderen og DST sikret via stærk kryptering via IPSEC VPN og Checkpoint Firewall-1?		
13	Hvilke grupper hos tjenesteyderen underskriver fortrolighedserklaringen:		
	A) alle interviewere tilknyttet AKU?		
	B) andre der har adgang til data vedrørende AKU?		
14	Indgår information af overholdelse af sikkerhedsbestemmelserne i uddannelsen af interviewerne?		
15	Er der installeret logon-procedure med unik adgangskode eller lignende adgangskontrol i hver enkelt PC eller lignende medie, der anvendes til interview?		
16	Er interviewprogrammer sikret via en adgangskode?		
17	Anvendes PC eller andre anvendte medier til private formål?		

Hvis ja - Yderligere dokumentation
Hvilken certificering er der tale om?
Hvilke programmer, og hvornår blev de opdateret sidst
Hvor ofte?
Hvilke sikkerhedsforanstaltninger?
Hvilke forholdsregler
Hvordan bortskaffes data?
Hvis tilsvarende standard hvilken?
Hvis tilsvarende standard hvilken?
Hvilke forholdsregler
Hvordan sikres stærk kryptering?
Opbevares der et underskrevet eksemplar for alle medarbejdere?
Hvilken logon-procedure?