Sjekkliste for databehandleravtale (GDPR)

Sjekkliste for når databehandleravtalen tilfredsstiller ny personopplysningslov 2018

Nr.	Sjekkpunkter	ja/nei
1	Hva databehandler faktisk skal gjøre med personopplysningene	
2	Hva som er formålet med behandlingen	
3	Hvor lenge avtalen skal gjelde (trenger ikke å være dato)	
4	Hva slags personopplysninger som er registrert	
5	Hvilke kategorier personer som er registrert (medlemmer, ansatte, kunder, pasienter, elever og lignende)	
6	At din virksomhet (behandlingsansvarlig) er ansvarlig at behandlingen skjer i samsvar med personopplysningsloven	
7	At din virksomhet bestemmer hvordan personopplysningene blir behandlet. Dette skal dokumenteres i en skriftlig instruks som legges eller innarbeides i databehandleravtalen. Databehandler skal gi beskjed dersom instruksen er i strid med regelverket	
8	At din virksomhet kan si opp avtalen dersom databehandler ikke følger regelverket	
9	I noen tilfeller pålegger norsk lov en bestemt behandling av personopplysninger. Databehandler skal underrette din virksomhet dersom dette gjelder personopplysninger fra din virksomhet	
10	At databehandler godkjenner alle som skal ha tilgang til personopplysningene, slik at bare autoriserte personer har tilgang. Disse personene er forpliktet til å behandle personopplysningene fortrolig eller er underlagt taushetsplikt. Dette skal kunne dokumenteres. Kun personer som har tjenestlig behov for det skal autoriseres	
11	Hvilke sikkerhetstiltak som skal gjennomføres for å sikre personopplysningene. Kravene til sikkerhetstiltak følger av den risikovurderingen din virksomhet har gjennomført	

Nr.	Sjekkpunkter	ja/nei
12	Når databehandleren ønsker å bruke underleverandører skal dette være godkjent av din virksomhet. Databehandleren skal inngå egne databehandleravtaler med underleverandørene. Disse avtalene skal minimum inneholde de samme forpliktelsene som avtalen din virksomhet har inngått med databehandleren. Det bør framgå at databehandleren er ansvarlig dersom en underleverandør ikke oppfyller sine forpliktelser	
13	At databehandler legger til rette for at registrerte får utøvd sin rett til innsyn, retting, sletting og innsigelse av personopplysninger	
14	At databehandleravtalen beskriver hva som skal skje med personopplysningene når oppdraget er fullført. Databehandleren skal kunne påvise at personopplysningene inklusive kopier faktisk er slettet eller tilbakelevert etter at oppdraget er avsluttet	
15	At databehandleren gjør det mulig å gjennomføre revisjoner, enten av din virksomhet eller av en uavhengig tredjepart. Din virksomhet skal også få tilgang til nødvendig dokumentasjon	
16	At databehandler treffer alle tiltak som er nødvendig for at personopplysningssikkerheten er i tråd med reglene, og at brudd varsles til databehandlingsansvarlig uten opphold	
17	At databehandleren garanterer at lagring og behandling innenfor EØS-området. Canada, Australia, Sveits er også godkjent av EU som trygge mottakerstater. Databehandlere i USA som er med i sertifiseringsordningen EU-US Privacy shield er også godkjente for behandling og lagring av personopplysninger	