

# Svar på databehandlerperspektiv

---

Bemærk: Vi optræder som databehandler og ikke dataansvarlig i aftaleforholdet med kunden.

Spørgsmål / Udtalelse	Svar / Kommentar
Som databehandler anvender vi kun personoplysningerne til det formål, der er aftalt med den dataansvarlige.	JA
Vi har udpeget en leder/medarbejder, der er GDPR-ansvarlig.	JA
Efter udfyldt besvarelse vurderes det, at der ikke er behov for at opdatere den indgåede databehandleraftale.	JA
Vi har en konkret procedure for, hvordan vi håndterer eventuelle brud og underretter den dataansvarlige herom indenfor den aftalte tidsfrist.	JA
Vi har kortlagt, hvor, og hvordan vi behandler persondata (fortegnelseskravet).	JA
Vi har en konkret procedure for, hvor og hvordan personoplysninger skal opbevares.	JA
Vi har en konkret sletteprocedure, som vores medarbejdere følger.	JA
Vi har en indført en procedure for, hvordan vi kan opfylde de registreredes rettigheder, hvis den dataansvarlige anmodes herom.	JA
Vi sørger løbende for, at opdaterer vores politikker og procedurer, hvis der er behov herfor, samt løbende at uddanne vores ansatte i, hvordan de behandler personoplysninger ansvarligt.	JA
Som databehandler, efterlever vi det sikkerhedsniveau, vi har oplyst til den dataansvarlige.	JA
Vi bekræfter, at vi har tegnet en IT-produktansvarsforsikring	JA
Som dataansvarlig har vi vedtaget en IT-sikkerhedspolitik, som alle vores medarbejdere følger.	JA, revideres tilbagevendende senest 3 måneder efter indgangen til vores eget regnskabsår, senest d. 31/3.
Vi har vedtaget en IT-beredskabsplan.	JA, revideres tilbagevendende senest 3 måneder efter indgangen til vores eget regnskabsår, senest d. 31/3.
Vi har afprøvet vores IT-beredskabsplan	JA, revideres tilbagevendende senest 6 måneder efter indgangen til vores eget regnskabsår, senest d. 15/5.

Hvad gør I for at beskytte jeres systemer mod uønsket adgang?	Vi anvender anerkendte sikkerhedsforanstaltninger for at beskytte vores systemer mod uautoriseret adgang. Dette inkluderer blandt andet adgangskontrol, regelmæssig opdatering af software og implementering af passende netværkssikkerhedsprotokoller. Derudover foretager vi løbende vurderinger og opdateringer af vores sikkerhedspraksis for at imødekomme relevante trusler.
Hvad gør I for at sikre høj tilgængelighed og opetid?	Vi stræber efter at opretholde en stabil drift ved hjælp af overvågning af systemernes ydeevne, redundante løsninger og løbende vedligeholdelse. Vi har implementeret procedurer til hurtig genopretning i tilfælde af uforudsete hændelser for at minimere nedetid.
Hvad gør I for at dokumentere egen sikkerhed?	Vi opretholder interne procedurer og retningslinjer for sikkerhed, som løbende evalueres og opdateres. Dokumentationen inkluderer relevante rapporter om sikkerhedsopdateringer, risikovurderinger og gennemførte interne audits, som bruges til at sikre, at vi overholder gældende standarder og krav.
Hvad gør I for at passe godt på persondata?	Vi følger gældende databeskyttelsesregler og anvender passende tekniske og organisatoriske foranstaltninger til at beskytte persondata mod uautoriseret adgang, tab eller misbrug. Vores procedurer evalueres og justeres løbende i takt med udviklingen af relevante krav og risici.
Hvordan aftales den konkrete ansvarsfordeling mellem virksomheden og leverandøren?	Den konkrete ansvarsfordeling mellem virksomheden og leverandøren er klart defineret i vores databehandleraftale. Aftalen specificerer roller og ansvar i overensstemmelse med gældende databeskyttelseslovgivning og sikrer en fælles forståelse af forpligtelserne i forhold til behandling og beskyttelse af persondata.
Hvordan holder I jer opdateret indenfor de nyeste krav til digital sikkerhed?	Vi overvåger løbende udviklingen inden for digital sikkerhed gennem relevante kilder, herunder brancheanbefalinger, standarder og tilgængelige vejledninger. Derudover foretager vi periodiske vurderinger af vores sikkerhedsprocedurer for at sikre overensstemmelse med gældende krav.
Vi anvender alene de underdatabehandlere,	JA

som er angivet i databehandleraftalen.	
Vi fører årligt tilsyn med vores anvendte underdatabehandlere, således at vi sikrer, at de overholder den indgåede databehandleraftale.	JA, revideres tilbagevendende senest 3 måneder efter indgangen til vores eget regnskabsår, senest d. 31/3.
Vores anvendte underdatabehandlere overfører personoplysninger til et usikkert tredjeland.	NEJ
Vi har indført en procedure for, hvordan vi underretter den dataansvarlige, hvis påtænker at anvende en anden underdatabehandler end angivet i databehandleraftalen.	JA
Vi har indført en procedure for, hvordan vi sikrer, at vores anvendte underdatabehandlere sletter de personoplysninger, som tilhører den dataansvarlige, ved ophørt anvendelse.	JA