

GDPR

Vejledning

GDPR og beskyttelse af persondata

Herunder kan man se Jeres virksomheds Databehandleraftale (DPA) med vores virksomhed, hvis der er behov for at en Databehandler aftale bliver indgået, til beskyttelse af eventuelle følsomme Persondata, som i forvejen ikke allerede er at opfatte som Persondata.

Læs mere om vores arbejde i forhold til den danske Persondata forordning og GDPR her og vores virksomheds persondata politik her for yderligere information omkring disse emner.

VEJLEDNING

Hvis Jeres virksomhed via vores virksomheds tekniske løsninger gør brug af (eller opbevarer) data af følgende type og karakter, bør I som Dataansvarlig svare JA nedenfor, og dermed indgå en Databehandler aftale med vores virksomhed.

Opbevarer I eller gør brug af oplysninger og persondata såsom;

- CPR og eller medlemsnummer kombineret med navne
- Race eller etnisk oprindelse
- Seksuelle forhold og eller seksuel orientering
- Fagforeningsmedlemskab
- Helbredsoplysninger
- Politisk, religiøse eller filosofiske overbevisning

Vær opmærksom på, at det muligvis er nødvendigt at indgå en Databehandler aftale med os, også selvom man måske ikke mener at behandle personfølsomme data. Et eksempel på dette kunne være at har persondata liggende på e-mail eller via et webhotel, hvor visse persondata såsom navn, adresse mv. er opbevaret sammen med en beskrivelse af personen, eller et andet form for tilhørsforhold omkring samme person, der kunne være i et grænsetilfælde af at være personfølsom data.

I disse tilfælde skal man sætte kryds i JA i forhold til at indgå en Databehandler aftale eller ej.

Med andre ord skal du nu læse aftalen her nedenfor igennem, og bagefter tage stilling til om I opbevarer eller gør brug af oplysninger og personfølsomme data hos os, der kræver indgåelse af en Databehandler aftale. Svar JA, hvis det er tilfældet og NEJ, hvis det ikke er tilfældet.

Aftale til godkendelse

DATABEHANDLERAFTALE

Vedrørende Kerteminde Sejlklub hosting af IT løsning placeret hos AzeroCloud ApS.

For at sikre overholdelsen af de til enhver tid gældende regler om behandling af personoplysninger, herunder særligt persondataloven[1] og dertil hørende bekendtgørelser og vejledninger, har

**Kerteminde Sejlklub
Marinavejen 2**

<p>DATAANSVARLIG</p>	<p>5300 Kerteminde</p> <p>Denmark</p> <p>CVR-nummer:</p> <p>Kontaktperson: Kerteminde Sejlklub E-mail: kasserer@kerteminde-sejklub.dk Telefon: 65 32 25 90</p> <p>(herefter <input type="checkbox"/> Dataansvarlig <input type="checkbox"/>)</p>
<p>OG</p>	
<p>DATABEHANDLER</p>	<p>AzeroCloud ApS</p> <p>Herstedvang 8</p> <p>DK-2620 Albertslund Denmark</p> <p>CVR-nummer: DK38706993</p> <p>Kontakt e-mail: support@azero.cloud</p> <p>Telefon: +45-70254505</p> <p>(herefter <input type="checkbox"/> Databehandler eller Hostingpartner <input type="checkbox"/>)</p>

indgået nærværende version 12-04-2018 af Databehandleraftale (herefter Databehandler-aftale eller Databehandleraftalen) som en del af aftalegrundlag af [Dato] om leverance, hvor data fysisk behandles ved brug af Databehandlerens tekniske systemer og Dataansvarliges software/kode løsning, der er placeret hos Databehandleren på dennes tekniske udstyr, placeret i datacenter på adressen adressen Niels Bohrsvej 35, 8660 Skanderborg, og/eller Ejby Industrivej 1, 2600 Glostrup og/eller Herstedvang 8, 2620 Albertslund i Danmark.

1. Dataansvarliges ansvar

Databehandleren handler alene efter instruks fra Dataansvarlige og alene i det omfang, det er nødvendigt for, at Databehandleren kan opfylde sine forpligtelser i henhold til Databehandleraftalen. Databehandleraftalen er således en del af Dataansvarliges instruks til Databehandleren.

Dataansvarlige forpligter sig til, til enhver tid at overholde den danske, såvel som Dataansvarliges nationale lovgivningsmæssige krav vedrørende databehandling og datasikkerhed, samt Databehandlerens informations-sikkerhedspolitikker med tilhørende vejledning og retningslinjer i forbindelse med den databehandling, som udføres for Dataansvarlige.

Dataansvarlige er tillige bekendt med at opbevaring af almindelige og følsomme Persondata på Databehandlers udstyr, er opbevaret på teknisk udstyr, hvor andre virksomheder tillige har adgang, om end data for hver løsning er beskyttet i selvstændige tekniske dataområder. Med dette menes og betyder således, at Dataansvarliges data inden for denne Databehandler aftale ikke er uafhængigt fysisk placeret i forhold til andre virksomheder, hvilket kræver at Dataansvarlige indgår en driftsaftale omkring en dedikeret (fysisk og teknisk afgrænset) service hos Dataansvarlige.

2. Databehandlerens opgave

Formålet med databehandlingen er at:

Opbevare data og programmel på Databehandlerens tekniske systemer, som Dataansvarlige har lejet kapacitet af hos Databehandleren.

3. Tekniske og organisatoriske sikkerhedsforanstaltninger

Dataansvarlige skal træffe de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at oplysninger hædeligt eller ulovligt tilintetgøres, fortabes eller forringes, samt mod, at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med loven.

Dataansvarlige forpligter sig til at overholde de til enhver tid gældende lovgivningsmæssige krav vedrørende behandling af personoplysninger. Databehandlingen skal derfor foregå i overensstemmelse med de til enhver tid gældende regler om behandling af personoplysninger, herunder særligt persondataloven og dertil hørende bekendtgørelser^[2] og vejledninger.

Databehandler behandler oplysninger på Dataansvarliges vegne og handler alene efter instruks fra Dataansvarlige. Minimumskrav til de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger følger den til enhver tid gældende lovgivning om beskyttelse af personfølsomme oplysninger, herunder de til enhver tid gældende retningslinjer fra Datatilsynet.

Databehandleren forpligter sig endvidere til at behandle personoplysningerne i overensstemmelse med den informationssikkerhedspolitik som udspringer fra Datatilsynets retningslinjer, herunder principperne og anbefalingerne i ISO/IEC 27001:2013 Information Security Management System (ISMS) standarden, med senere ændringer vil således på alle relevante områder skulle efterleves som ramme, i det omfang andet ikke fremgår af nærværende Databehandleraftale.

4. Databehandlerens brug af Underdatabehandlere

Databehandleren indgår aftale med Underdatabehandlere efter behov, så længe disse aftaler overholder gældende lovgivning indenfor Danmark og EU, hvorefter disse Underdatabehandlere har Dataansvarliges samtykke som en del af denne Databehandleraftale. Dataansvarlige er således kun berettiget til at stille vilkår for et sådant samtykke, såfremt en aftale om brug af en dedikeret server indgås, hvorpå Dataansvarliges løsning placeres uafhængigt af andre løsninger.

Databehandleren må dog ikke overføre eller tillade overførsel af personoplysninger til lande uden for EU og det Europæiske Økonomiske Samarbejdsområde uden Dataansvarliges forudgående skriftlige samtykke.

Såfremt Dataansvarlige har givet tilladelse til en overførsel af personoplysninger til lande uden for EU og det Europæiske Økonomiske Samarbejdsområde, påhviler det Databehandleren at sikre, at data ikke overføres, før der foreligger et lovligt kontraktgrundlag for overførsel af personoplysninger til de pågældende lande herunder en direkte underdatabehandleraftale mellem Databehandleren og eventuelle underdatabehandler(e) beliggende i tredjelande.

Dataansvarlige skal i sin aftale med Databehandleren sikre sig, at Databehandleren som minimum kan opfylde de forpligtelser, som Databehandleren har påtaget sig ved indgåelse af denne Databehandleraftale, for så vidt angår den behandling af personoplysninger, der skal varetages af Databehandleren.

Dataansvarlige indestår for kontraktmæssigheden og lovligheden af Databehandlerens behandling af personoplysninger. Det forhold, at Databehandler indgår aftale med en eller flere Underdatabehandlere, fritager ikke Databehandleren for pligten til at efterleve nærværende Databehandleraftale.

Ved ophør af en aftale med en Databehandler om behandling af personoplysninger omfattet af denne Databehandleraftale, skal Databehandleren give Dataansvarlige meddelelse herom.

Databehandleren skal i den forbindelse sikre, at den valgte Underdatabehandler sletter data behørigt i overensstemmelse med punkt 9.

Dataansvarlige kan til enhver tid se Databehandlerens brug af Underdatabehandlere her.

5. Ad hoc arbejdspladser

I det omfang, databehandlingen sker fra ad hoc arbejdspladser (fjernarbejdspladser eller hjemmearbejdspladser) skal dette altid ske via en krypteret adgang og brug af teknisk fjernskrivebord til berørt teknisk udstyr og løsninger.

Såfremt Databehandleren foretager databehandling fra ad hoc arbejdspladser, skal Databehandleren tillige sikre, at disse lever op til de sikkerhedsmæssige krav i denne Under- og eventuelle under-underdatabehandleraftale med bilag samt Datatilsynets IT-sikkerhedstekster herom.

Databehandleren skal ved en revision gennemgang til enhver tid blandt andet kunne opfylde og dokumentere følgende:

- Beskrivelse af anvendt krypteret forbindelse mellem ad hoc arbejdspladsen og Underdatabehandlerens /Databehandlerens netværk

- Anvendelse af 2-faktor-autentifikation
- Underdatabehandlers interne instruks til egne medarbejdere vedrørende ad hoc arbejdspladser

6. Tilsynsmyndigheder, audits og revisionserklæringer

Databehandleren skal på Dataansvarliges anmodning give Dataansvarlige tilstrækkelige oplysninger til at denne kan påse, at de nævnte tekniske og organisatoriske sikkerhedsforanstaltninger m.v. er truffet. Endvidere skal Databehandleren kunne dokumentere, at identificerede sårbarheder bliver imødegået ud fra en risikobaseret vurdering.

I tilfælde af, at Dataansvarlige og/eller relevante offentlige myndigheder, særligt Datatilsynet, ønsker at foretage en fysisk inspektion (audit) af de foranstaltninger, som Databehandler foretager i medfør af Databehandleraftalen, forpligter Databehandleren sig til - med et rimeligt varsel - at stille tid og ressourcer til rådighed herfor efter konkret aftale om honorering herom.

Databehandleren forpligter sig på samme måde til at sikre, at sådanne audits også kan gennemføres hos dennes Underdatabehandlere.

Som supplement (eller alternativ) til de ovenfor nævnte audits kan der indgås aftale om, at Dataansvarlige for egen regning sørger for, at en uafhængig ekspert årligt udarbejder en revisionserklæring på grundlag af en anerkendt standard angående Databehandlerens overholdelse af kravene til sikkerhedsforanstaltninger fastsat i Databehandleraftalen.

Dataansvarlige er opmærksom på at Databehandlerens udarbejdelse af en konkret revisionserklæring på grundlag af en anerkendt standard angående Databehandlerens overholdelse af kravene til sikkerhedsforanstaltningerne fastsat i Databehandleraftalen, faktureres af Databehandleren overfor til Dataansvarlige for medgået tid, enten per tilbud eller per time jfr. den allerede indgåede hostingaftale imellem parterne.

7. Underretningspligt og assistance

Databehandleren forpligter sig til straks og skriftligt at orientere Dataansvarlige om enhver afvigelse fra kravene i Databehandleraftalen, f.eks.:

- ved enhver fravigelse fra givne instrukser
- ved enhver afvigelse fra det aftalte om tilgængelighed
- ved planlagte releases, opgraderinger, tests mv.
- ved enhver mistanke om brud på fortroligheden
- ved enhver mistanke om misbrug, fortabelse og forringelse af data
- ved enhver hændelig eller uautoriseret videregivelse af eller adgang til personoplysningerne behandlet efter denne Databehandleraftale

Databehandleren og dennes eventuelle Underdatabehandler(e) skal straks assistere Dataansvarlige med håndteringen af enhver hændelse registreret, herunder anmodning om indsigt, berigtigelse, blokering eller sletning, hvis de relevante personoplysninger behandles af eventuelle Underdatabehandler(e).

Databehandleren og dennes eventuelle Underdatabehandler(e) skal assistere Dataansvarlige med at overholde øvrige forpligtelser, der måtte påhvile Dataansvarlige efter gældende ret, hvor assistance er forudsat, samt hvor assistance er nødvendig for, at Dataansvarlige kan overholde sine forpligtelser.

8. Aftalens ikrafttræden og varighed

Nærværende Databehandleraftale træder i kraft ved underskrift og accept af nærværende aftale.

Nærværende Databehandleraftale ophører, når al behandling af personoplysninger i henhold til parternes indgåede

serviceaftale er ophørt og Dataansvarlige har slettet data, jf. punkt 9.

9. Håndtering af data efter aftalens ophør

Databehandleren og dennes eventuelle Underdatabehandler(e) forpligter sig til at tilbagelevere og/eller slette personoplysninger, når databehandlingen i henhold til aftale med Dataansvarlige ophører.

Dataansvarlige skal oplyse Databehandleren om det præcise tidspunkt, hvor databehandlingen skal ophøre. Det påhviler herefter Databehandleren at tilbagelevere og/eller slette personoplysningerne på det oplyste tidspunkt.

Sletning må ikke ske, før Dataansvarlige skriftligt har godkendt den påtænkte fremgangsmåde for sletning.

Såfremt Dataansvarlige ikke finder metoden tilstrækkelig sikker og i overensstemmelse med gældende regler om behandling af personoplysninger, skal Dataansvarlige meddele Databehandleren om hvilken metode, der kan anvendes i stedet. Der henvises til Datatilsynets it-sikkerhedstekst ST3 fra 2014 med eventuelle opdateringer.

Såfremt Dataansvarlige kræver en særlig metode til sletning af data, der ligger udover gældende lovgivning i Danmark, er Dataansvarlige opmærksom på at Databehandleren vil fakturere Dataansvarlige for medgået tid og følgeomkostninger.

Når sletningen er foretaget, skal Databehandleren fremsende en skriftlig erklæring på, at data er slettet som aftalt, inklusiv en beskrivelse af den anvendte metode.

Såfremt Databehandleren og dennes eventuelle Underdatabehandler(e) i forbindelse med konkurs el.lign. ophører med at behandle personoplysninger for Dataansvarlige, skal alle personoplysningerne straks leveres tilbage til Dataansvarlige på en måde, der gør det muligt for Dataansvarlige at anvende disse fremadrettet. Herefter er Databehandler, dennes konkursbo el.lign. forpligtet til effektivt at slette oplysningerne fra egne systemer i overensstemmelse med ovenstående.

10. Tavshedspligt og fortrolighed

Databehandlerens ansatte, samarbejdspartnere, eksterne konsulenter, vikarer og eventuelle Underdatabehandlere mfl. vil i forbindelse med behandlingen af fortrolige oplysninger være omfattet af de regler om tavshedspligt, som gælder for ansatte i den offentlige forvaltning. Der henvises til forvaltningslovens § 27 og straffelovens §§ 152-152 f.

Det påhviler Databehandleren og dennes eventuelle Underdatabehandler(e) at informere egne ansatte, samarbejdspartnere, eksterne konsulenter og vikarer mfl. om udstrækningen af tavshedspligten og om konsekvenserne ved en eventuel overtrædelse.

Databehandleren skal holde personoplysningerne fortrolige, og er således alene berettiget til at anvende personoplysningerne som led i opfyldelsen af sine forpligtelser i henhold til denne Databehandleraftale og instruks.

Databehandleren påtager sig endvidere at begrænse adgangen til personoplysningerne til de medarbejdere, for hvem det er nødvendigt at behandle personoplysninger for at kunne opfylde Databehandlerens forpligtelser over for Dataansvarlige.

Databehandlerens forpligtelser om tavshedspligt og fortrolighed gælder også efter aftalens ophør.

11. Overdragelse

Databehandleren kan ved eventuelt frasalg af aktiviteter frit overdrage sine rettigheder og forpligtelser i henhold til denne Databehandleraftale uden Dataansvarliges forud indgående samtykke.

12. Misligholdelse

Det betragtes som væsentlig misligholdelse af aftalen, såfremt Databehandler ikke overholder forpligtelserne i Databehandleraftalen, de til enhver tid gældende lovgivningsmæssige krav og kravene i nærværende aftale.

Dataansvarlige er i så fald berettiget til uden varsel at opsige samtlige gældende aftaler om databehandling, som udføres for denne.

Uanset ophævelse/opsigelse af aftalen er Databehandleren dog forpligtet til at levere databehandling i henhold til denne Databehandleraftale indtil Dataansvarliges databehandling er sikret hos anden Databehandler.

Databehandleren er forpligtet til at levere relevant ophørsassistance til Dataansvarlige inden for rimelighedens grænser, hvilket tillige kan indebære udgifter for Dataansvarlige i form af Databehandlers medgået tid og eventuelle omkostninger hermed. Såfremt dette bliver aktuelt vil Databehandleren informere Dataansvarlige herom.

Dette inkluderer, men er ikke begrænset til andre aftaler indgået med samme Databehandler og/eller eventuelle Underdatabehandler(e) vedrørende behandling af samme data.

Databehandleren forpligter sig til at friholde og forsvare Dataansvarlige, medmindre det kan påvises at Dataansvarlige selv er medskyldig, imod alle krav, retskrav og ethvert ansvar, tab, bøder, omkostninger og udgifter forbundet derved som følge af Databehandlerens overtrædelse af Databehandleraftalen eller gældende ret, begået af Databehandleren, Databehandlerens ansatte og/eller eventuelle Underdatabehandler(e) eller repræsentanter i forbindelse med levering af persondatabehandlingen, gennemførelse af aftalen aftalt mellem parterne.

13. Lovvalg og værneting

Denne Databehandleraftale inklusiv ethvert spørgsmål om Databehandleraftalens gyldighed er undergivet dansk ret og værneting i medfør af retsplejelovens regler herom.

14. Øvrige henvisninger

- Lov nr. 429 af 31. maj 2000 om behandling af personoplysninger med senere ændringer
- Bekendtgørelse nr. 528 af 15. juni 2000 vedrørende sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning
- Vejledning til sikkerhedsbekendtgørelsen
- Datatilsynets it-sikkerhedstekst ST3
- ISO/IEC 27001 ISMS - Ledelsessystem for informationssikkerhed

[1] Lov nr. 429 af 31.maj 2000 om behandling af personoplysninger med senere

ændringer § 42, stk. 2 jf. § 41.

[2] Se f.eks. Bekendtgørelse nr. 528 af 15. juni 2000 om sikkerhedsforanstaltninger til

beskyttelse af personoplysninger, der behandles for den offentlige forvaltning

med senere ændringer.