Databehandleraftale

Changelog standardkontraksbestemmelser

VERSION	ÆNDRINGER
1.1	Ændringer i Bestemmelserne 7.7., 9.2., 10.4. og Bilag C.8. *(Tastefejl og opdaterede krydshenvisninger).*
1.2	Ændringer i Bestemmelse 7.6 *(Bestemmelsen er gjort valgfri og ordlyden er blevet modificeret)*

OCTOPUS PMS ApS • +45 73 700 100
info@octopuspms.com • octopuspms.com

Standardkontraktsbestemmelser

i henhold til artikel 28, stk. 3, i forordning 2016/679 (databeskyttelsesforordningen) med henblik på databehandlerens behandling af personoplysninger

mellem

Kunde
(herefter "den dataansvarlige")

og

OCTOPUS PMS
CVR 38296418
Gerlachsgade 4,4
6400 Sønderborg
Danmark

(herefter "databehandleren"),

der hver især er en "part" og sammen udgør "parterne"

HAR AFTALT følgende standardkontraktsbestemmelser (Bestemmelserne) med henblik på at overholde databeskyttelsesforordningen og sikre beskyttelse af privatlivets fred og fysiske personers grundlæggende rettigheder og frihedsrettigheder

OCTOPUS PMS ApS • +45 73 700 100
info@octopuspms.com • octopuspms.com

1. Indhold

OCTOPUS PMS ApS • +45 73 700 100
info@octopuspms.com • octopuspms.com

2. Præambel

1. Disse Bestemmelser fastsætter databehandlerens rettigheder og forpligtelser, når denne foretager behandling af personoplysninger på vegne af den dataansvarlige.

2. Disse bestemmelser er udformet med henblik på parternes efterlevelse af artikel 28, stk. 3, i Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (databeskyttelsesforordningen).

3. I forbindelse med leveringen af Octopus PMS herunder hosting og support behandler databehandleren personoplysninger på vegne af den dataansvarlige i overensstemmelse med disse Bestemmelser.

4. Bestemmelserne har forrang i forhold til eventuelle tilsvarende bestemmelser i andre aftaler mellem parterne.

5. Der hører fire bilag til disse Bestemmelser, og bilagene udgør en integreret del af Bestemmelserne.

6. Bilag A indeholder nærmere oplysninger om behandlingen af personoplysninger, herunder om behandlingens formål og karakter, typen af personoplysninger, kategorierne af registrerede og varighed af behandlingen.

7. Bilag B indeholder den dataansvarliges betingelser for databehandlerens brug af underdatabehandlere og en liste af underdatabehandlere, som den dataansvarlige har godkendt brugen af.

8. Bilag C indeholder den dataansvarliges instruks for så vidt angår databehandlerens behandling af personoplysninger, en beskrivelse af de sikkerhedsforanstaltninger, som databehandleren som minimum skal gennemføre, og hvordan der føres tilsyn med databehandleren og eventuelle underdatabehandlere.

9. Bilag D indeholder bestemmelser vedrørende andre aktiviteter, som ikke af omfattet af Bestemmelserne.

10. Bestemmelserne med tilhørende bilag skal opbevares skriftligt, herunder elektronisk, af begge parter.

11. Disse Bestemmelser frigør ikke databehandleren fra forpligtelser, som databehandleren er pålagt efter databeskyttelsesforordningen eller enhver anden lovgivning.

3. Den dataansvarliges rettigheder og forpligtelser

1. Den dataansvarlige er ansvarlig for at sikre, at behandlingen af personoplysninger sker i overensstemmelse med databeskyttelsesforordningen (se forordningens artikel 24), databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes[1] nationale ret og disse Bestemmelser.

2. Den dataansvarlige har ret og pligt til at træffe beslutninger om, til hvilke(t) formål og med hvilke hjælpemidler, der må ske behandling af personoplysninger.

3. Den dataansvarlige er ansvarlig for, blandt andet, at sikre, at der er et behandlingsgrundlag for behandlingen af personoplysninger, som databehandleren instrueres i at foretage.

4. Databehandleren handler efter instruks

1. Databehandleren må kun behandle personoplysninger efter dokumenteret instruks fra den dataansvarlige, medmindre det kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som databehandleren er underlagt. Denne instruks skal være specificeret i bilag A og C. Efterfølgende instruks kan også gives af den dataansvarlige, mens der sker behandling af personoplysninger, men instruksen skal altid være dokumenteret og opbevares skriftligt, herunder elektronisk, sammen med disse Bestemmelser.

2. Databehandleren underretter omgående den dataansvarlige, hvis en instruks efter vedkommendes mening er i strid med denne forordning eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.

1 Henvisninger til "medlemsstat" i disse bestemmelse skal forstås som en henvisning til "EØS medlemsstater".

OCTOPUS PMS ApS • +45 73 700 100
info@octopuspms.com • octopuspms.com

5. Fortrolighed

1. Databehandleren må kun give adgang til personoplysninger, som behandles på den dataansvarliges vegne, til personer, som er underlagt databehandlerens instruktionsbeføjelser, som har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt, og kun i det nødvendige omfang. Listen af personer, som har fået tildelt adgang, skal løbende gennemgås. På baggrund af denne gennemgang kan adgangen til personoplysninger lukkes, hvis adgangen ikke længere er nødvendig, og personoplysningerne skal herefter ikke længere være tilgængelige for disse personer.

2. Databehandleren skal efter anmodning fra den dataansvarlige kunne påvise, at de pågældende personer, som er underlagt databehandlerens instruktionsbeføjelser, er underlagt ovennævnte tavshedspligt.

6. Behandlingssikkerhed

1. Databeskyttelsesforordningens artikel 32 fastslår, at den dataansvarlige og databehandleren, under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder, gennemfører passende tekniske og organisatoriske foranstaltninger for at sikre et beskyttelsesniveau, der passer til disse risici.

Den dataansvarlige skal vurdere risiciene for fysiske personers rettigheder og frihedsrettigheder som behandlingen udgør og gennemføre foranstaltninger for at imødegå disse risici. Afhængig af deres relevans kan det omfatte:

a. Pseudonymisering og kryptering af personoplysninger

b. evne til at sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og -tjenester

c. evne til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse

d. en procedure for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed.

2. Efter forordningens artikel 32 skal databehandleren – uafhængigt af den dataansvarlige – også vurdere risiciene for fysiske personers rettigheder som behandlingen udgør og gennemføre foranstaltninger for at imødegå disse risici. Med henblik på denne vurdering skal den dataansvarlige stille den nødvendige information til rådighed for databehandleren som gør vedkommende i stand til at identificere og vurdere sådanne risici.

3. Derudover skal databehandleren bistå den dataansvarlige med vedkommendes overholdelse af den dataansvarliges forpligtelse efter forordningens artikel 32, ved bl.a. at stille den nødvendige information til rådighed for den dataansvarlige vedrørende de tekniske og organisatoriske sikkerhedsforanstaltninger, som databehandleren allerede har gennemført i henhold til forordningens artikel 32, og al anden information, der er nødvendig for den dataansvarliges overholdelse af sin forpligtelse efter forordningens artikel 32.

Hvis imødegåelse af de identificerede risici – efter den dataansvarliges vurdering – kræver gennemførelse af yderligere foranstaltninger end de foranstaltninger, som databehandleren allerede har gennemført, skal den dataansvarlige angive de yderligere foranstaltninger, der skal gennemføres, i bilag C.

7. Anvendelse af underdatabehandlere

1. Databehandleren skal opfylde de betingelser, der er omhandlet i databeskyttelsesforordningens artikel 28, stk. 2, og stk. 4, for at gøre brug af en anden databehandler (en underdatabehandler).

2. Databehandleren må således ikke gøre brug af en underdatabehandler til opfyldelse af disse Bestemmelser uden forudgående generel skriftlig godkendelse fra den dataansvarlige.

3. Databehandleren har den dataansvarliges generelle godkendelse til brug af underdatabehandlere. Databehandleren skal skriftligt underrette den dataansvarlige om eventuelle planlagte ændringer vedrørende tilføjelse eller udskiftning af underdatabehandlere med mindst 30 dages varsel og derved give den dataansvarlige mulighed for at gøre indsigelse

OCTOPUS PMS ApS • +45 73 700 100
info@octopuspms.com • octopuspms.com

mod sådanne ændringer inden brugen af de(n) omhandlede underdatabehandler(e). Længere varsel for underretning i forbindelse med specifikke behandlingsaktiviteter kan angives i bilag B. Listen over underdatabehandlere, som den dataansvarlige allerede har godkendt, fremgår af bilag B.

4. Når databehandleren gør brug af en underdatabehandler i forbindelse med udførelse af specifikke behandlingsaktiviteter på vegne af den dataansvarlige, skal databehandleren, gennem en kontrakt eller andet retligt dokument i henhold til EU-retten eller medlemsstaternes nationale ret, pålægge underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der fremgår af disse Bestemmelser, hvorved der navnlig stilles de fornødne garantier for, at underdatabehandleren vil gennemføre de tekniske og organisatoriske foranstaltninger på en sådan måde, at behandlingen overholder kravene i disse Bestemmelser og databeskyttelsesforordningen.

   Databehandleren er derfor ansvarlig for at kræve, at underdatabehandleren som minimum overholder databehandlerens forpligtelser efter disse Bestemmelser og databeskyttelsesforordningen.

5. Underdatabehandleraftale(r) og eventuelle senere ændringer hertil sendes – efter den dataansvarliges anmodning herom – i kopi til den dataansvarlige, som herigennem har mulighed for at sikre sig, at tilsvarende databeskyttelsesforpligtelser som følger af disse Bestemmelser er pålagt underdatabehandleren. Bestemmelser om kommercielle vilkår, som ikke påvirker det databeskyttelsesretlige indhold af underdatabehandleraftalen, skal ikke sendes til den dataansvarlige.

6. Databehandleren skal i sin aftale med underdatabehandleren indføje den dataansvarlige som begunstiget tredjemand, således at den dataansvarlige i tilfælde af at databehandleren faktisk eller retligt set er ophørt med at eksistere eller i tilfælde af databehandlerens konkurs, har ret til at opsige underdatabehandleraftalen og instruere underdatabehandleren i at slette eller tilbagelevere personoplysningerne.

7. Hvis underdatabehandleren ikke opfylder sine databeskyttelsesforpligtelser, forbliver databehandleren fuldt ansvarlig over for den dataansvarlige for opfyldelsen af underdatabehandlerens forpligtelser. Dette påvirker ikke de registreredes rettigheder, der følger af databeskyttelsesforordningen, herunder særligt forordningens artikel 79 og 82, over for den dataansvarlige og databehandleren, herunder underdatabehandleren.

8. Overførsel til tredjelande eller internationale organisationer

1. Enhver overførsel af personoplysninger til tredjelande eller internationale organisationer må kun foretages af databehandleren på baggrund af dokumenteret instruks herom fra den dataansvarlige og skal altid ske i overensstemmelse med databeskyttelsesforordningens kapitel V.

2. Hvis overførsel af personoplysninger til tredjelande eller internationale organisationer, som databehandleren ikke er blevet instrueret i at foretage af den dataansvarlige, kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som databehandleren er underlagt, skal databehandleren underrette den dataansvarlige om dette retlige krav inden behandling, medmindre den pågældende ret forbyder en sådan underretning af hensyn til vigtige samfundsmæssige interesser.

3. Uden dokumenteret instruks fra den dataansvarlige kan databehandleren således ikke inden for rammerne af disse Bestemmelser:

   a. overføre personoplysninger til en dataansvarlig eller databehandler i et tredjeland eller en international organisation
   b. overlade behandling af personoplysninger til en underdatabehandler i et tredjeland
   c. behandle personoplysningerne i et tredjeland

4. Den dataansvarliges instruks vedrørende overførsel af personoplysninger til et tredjeland, herunder det eventuelle overførselsgrundlag i databeskyttelsesforordningens kapitel V, som overførslen er baseret på, skal angives i bilag C.6.

5. Disse Bestemmelser skal ikke forveksles med standardkontraktsbestemmelser som omhandlet i databeskyttelsesforordningens artikel 46, stk. 2, litra c og d, og disse Bestemmelser kan ikke udgøre et grundlag for overførsel af personoplysninger som omhandlet i databeskyttelsesforordningens kapitel V.

OCTOPUS PMS ApS • +45 73 700 100
info@octopuspms.com • octopuspms.com

9. Bistand til den dataansvarlige

1. Databehandleren bistår, under hensyntagen til behandlingens karakter, så vidt muligt den dataansvarlige ved hjælp af passende tekniske og organisatoriske foranstaltninger med opfyldelse af den dataansvarliges forpligtelse til at besvare anmodninger om udøvelsen af de registreredes rettigheder som fastlagt i databeskyttelsesforordningens kapitel III.

Dette indebærer, at databehandleren så vidt muligt skal bistå den dataansvarlige i forbindelse med, at den dataansvarlige skal sikre overholdelsen af:

a. oplysningspligten ved indsamling af personoplysninger hos den registrerede
b. oplysningspligten, hvis personoplysninger ikke er indsamlet hos den registrerede
c. indsigtsretten
d. retten til berigtigelse
e. retten til sletning ("retten til at blive glemt")
f. retten til begrænsning af behandling
g. underretningspligten i forbindelse med berigtigelse eller sletning af personoplysninger eller begrænsning af behandling
h. retten til dataportabilitet
i. retten til indsigelse
j. retten til ikke at være genstand for en afgørelse, der alene er baseret på automatisk behandling, herunder profilering

2. I tillæg til databehandlerens forpligtelse til at bistå den dataansvarlige i henhold til Bestemmelse 6.3., bistår databehandleren endvidere, under hensyntagen til behandlingens karakter og de oplysninger, der er tilgængelige for databehandleren, den dataansvarlige med:

a. den dataansvarliges forpligtelse til uden unødig forsinkelse og om muligt senest 72 timer, efter at denne er blevet bekendt med det, at anmelde brud på persondatasikkerheden til den kompetente tilsynsmyndighed, Datatilsynet, medmindre at det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder

b. den dataansvarliges forpligtelse til uden unødig forsinkelse at underrette den registrerede om brud på persondatasikkerheden, når bruddet sandsynligvis vil medføre en høj risiko for fysiske personers rettigheder og frihedsrettigheder

c. den dataansvarliges forpligtelse til forud for behandlingen at foretage en analyse af de påtænkte behandlingsaktiviteters konsekvenser for beskyttelse af personoplysninger (en konsekvensanalyse)

d. den dataansvarliges forpligtelse til at høre den kompetente tilsynsmyndighed, Datatilsynet, inden behandling, såfremt en konsekvensanalyse vedrørende databeskyttelse viser, at behandlingen vil føre til høj risiko i mangel af foranstaltninger truffet af den dataansvarlige for at begrænse risikoen.

3. Parterne skal i bilag C angive de fornødne tekniske og organisatoriske foranstaltninger, hvormed databehandleren skal bistå den dataansvarlige samt i hvilket omfang og udstrækning. Det gælder for de forpligtelser, der følger af Bestemmelse 9.1. og 9.2.

10. Underretning om brud på persondatasikkerheden

1. Databehandleren underretter uden unødig forsinkelse den dataansvarlige efter at være blevet opmærksom på, at der er sket et brud på persondatasikkerheden.

2. Databehandlerens underretning til den dataansvarlige skal om muligt ske senest 36 timer efter, at denne er blevet bekendt med bruddet, sådan at den dataansvarlige kan overholde sin forpligtelse til at anmelde bruddet på persondatasikkerheden til den kompetente tilsynsmyndighed, jf. databeskyttelsesforordningens artikel 33.

3. I overensstemmelse med Bestemmelse 9.2.a skal databehandleren bistå den dataansvarlige med at foretage anmeldelse af bruddet til den kompetente tilsynsmyndighed. Det betyder, at databehandleren skal bistå med at tilvejebringe nedenstående information, som ifølge artikel 33, stk. 3, skal fremgå af den dataansvarliges anmeldelse af bruddet til den kompetente tilsynsmyndighed:

OCTOPUS PMS ApS • +45 73 700 100
info@octopuspms.com • octopuspms.com

a. karakteren af bruddet på persondatasikkerheden, herunder, hvis det er muligt, kategorierne og det omtrentlige antal berørte registrerede samt kategorierne og det omtrentlige antal berørte registreringer af personoplysninger

b. de sandsynlige konsekvenser af bruddet på persondatasikkerheden

c. de foranstaltninger, som den dataansvarlige har truffet eller foreslår truffet for at håndtere bruddet på persondatasikkerheden, herunder, hvis det er relevant, foranstaltninger for at begrænse dets mulige skadevirkninger.

4. Parterne skal i bilag C angive den information, som databehandleren skal tilvejebringe i forbindelse med sin bistand til den dataansvarlige i dennes forpligtelse til at anmelde brud på persondatasikkerheden til den kompetente tilsynsmyndighed.

11. Sletning og returnering af oplysninger

1. Ved ophør af tjenesterne vedrørende behandling af personoplysninger, er databehandleren forpligtet til at slette alle personoplysninger, der er blevet behandlet på vegne af den dataansvarlige og på opfordring bekræfte over for den dataansvarlig, at oplysningerne er slettet, medmindre EU-retten eller medlemsstaternes nationale ret foreskriver opbevaring af personoplysningerne.
2. Dataansvarlige kan, via selskabets GDPR opsætning i OCTOPUS PMS, yderligere bestemme hvornår data udelukkende skal foreligge i en anonymiseret form. Dataansvarlige kan selv tilpasse "opbevaringsperioden". Det er den Dataansvarliges ansvar. OCTOPUS PMS forbeholder sig ret til at slette dataansvarliges data 90 dage efter abonnementets ophør, uanset årsagen hertil, og OC har ingen forpligtelse til at opbevare data efter dette tidspunkt.

Databehandleren forpligter sig til alene at behandle personoplysningerne til de(t) formål, i den periode og under de betingelser, som disse regler foreskriver.

12. Revision, herunder inspektion

1. Databehandleren stiller alle oplysninger, der er nødvendige for at påvise overholdelsen af databeskyttelsesforordningens artikel 28 og disse Bestemmelser, til rådighed for den dataansvarlige og giver mulighed for og bidrager til revisioner, herunder inspektioner, der foretages af den dataansvarlige eller en anden revisor, som er bemyndiget af den dataansvarlige.

2. Procedurerne for den dataansvarliges revisioner, herunder inspektioner, med databehandleren og underdatabehandlere er nærmeret angivet i Bilag C.7. og C.8.

3. Databehandleren er forpligtet til at give tilsynsmyndigheder, som efter gældende lovgivningen har adgang til den dataansvarliges eller databehandlerens faciliteter, eller repræsentanter, der optræder på tilsynsmyndighedens vegne, adgang til databehandlerens fysiske faciliteter mod behørig legitimation.

13. Parternes aftale om andre forhold

1. Parterne kan aftale andre bestemmelser vedrørende tjenesten vedrørende behandling af personoplysninger om f.eks. erstatningsansvar, så længe disse andre bestemmelser ikke direkte eller indirekte strider imod Bestemmelserne eller forringer den registreredes grundlæggende rettigheder og frihedsrettigheder, som følger af databeskyttelsesforordningen.

14. Ikrafttræden og ophør

1. Bestemmelserne træder i kraft på datoen for begge parters underskrift heraf eller ved e-mail accept ved indgåelse af aftalen om brug af OCTOPUS PMS.

2. Begge parter kan kræve Bestemmelserne genforhandlet, hvis lovændringer eller uhensigtsmæssigheder i Bestemmelserne giver anledning hertil.

OCTOPUS PMS ApS • +45 73 700 100
info@octopuspms.com • octopuspms.com

3. Bestemmelserne er gældende, så længe tjenesten vedrørende behandling af personoplysninger varer. I denne periode kan Bestemmelserne ikke opsiges, medmindre andre bestemmelser, der regulerer levering af tjenesten vedrørende behandling af personoplysninger, aftales mellem parterne.

4. Hvis levering af tjenesterne vedrørende behandling af personoplysninger ophører, og personoplysningerne er slettet eller returneret til den dataansvarlige i overensstemmelse med Bestemmelse 11.1 og Bilag C.4, kan Bestemmelserne opsiges med skriftlig varsel af begge parter.

5. Underskrift
Databehandleren er bundet af Bestemmelserne uden Parternes underskrift. Bestemmelserne indgås således uden fysiske/digitale underskrifter, idet Bestemmelserne er bindende i overensstemmelse med kravet i GDPR, artikel 28. 3,1 pkt. på vegne af den dataansvarlige.

15. Kontaktpersoner hos den dataansvarlige og databehandleren

1. Parterne kan kontakte hinanden via nedenstående kontaktpersoner.

2. Parterne er forpligtet til løbende at orientere hinanden om ændringer vedrørende kontaktpersoner.

Kontaktoplysninger for den Dataansvarlige:

Jf. hovedaftale

Kontaktoplysninger for Databehandlinger:

Jf. hovedaftale

OCTOPUS PMS ApS • +45 73 700 100
info@octopuspms.com • octopuspms.com

16. Bilag A Oplysninger om behandlingen

A.1. Formålet med databehandlerens behandling af personoplysninger på vegne af den dataansvarlige

Levere OCTOPUS PMS

A.2. Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige drejer sig primært om (karakteren af behandlingen)

Drift, hosting og support af systemet.

A.3. Behandlingen omfatter følgende typer af personoplysninger om de registrerede

Navn, e-mailadresse, telefonnummer, adresse, firmanavn. Derudover kan kunden skrive noter i forbindelse med bookinger. Omhandler almindelige persondata.

A.4. Behandlingen omfatter følgende kategorier af registrerede

Kundens kunder og gæster samt kunden medarbejdere (kommende, nuværende, tidligere).

A.5. Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige kan påbegyndes efter disse Bestemmelsers ikrafttræden. Behandlingen har følgende varighed

Varigheden af behandlingen er til opsigelse eller kunden ønsker behandlingen stoppet.

OCTOPUS PMS ApS • +45 73 700 100
info@octopuspms.com • octopuspms.com

17. Bilag B Underdatabehandlere

B.1. Godkendte underdatabehandlere

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af følgende underdatabehandlere

NAVN	CVR	ADRESSE	BESKRIVELSE AF BEHANDLING
ipnordic	33577591	Nygade 17 6300 Gråsten	Hosting, (Netværk, IT drift, support mv.)

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af ovennævnte underdatabehandlere for den beskrevne behandlingsaktivitet. Databehandleren må ikke – uden den dataansvarliges skriftlige godkendelse – gøre brug af en underdatabehandler til en anden behandlingsaktivitet end den beskrevne og aftalte eller gøre brug af en anden underdatabehandler til denne behandlingsaktivitet.

B.2. Varsel for godkendelse af underdatabehandlere

Se pkt. 7.3.

OCTOPUS PMS ApS • +45 73 700 100
info@octopuspms.com • octopuspms.com

18. Bilag C Instruks vedrørende behandling af personoplysninger

C.1. Behandlingens genstand/instruks
Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige sker ved, at databehandleren udfører følgende: Levering af OCTOPUS PMS, drift, hosting og support.

C.2. Behandlingssikkerhed
Sikkerhedsniveauet skal afspejle:

Behandlingen omfatter en større mængde personoplysninger omfattet af databeskyttelsesforordningens artikel 6 om "almindelige kategorier af personoplysninger", hvorfor der skal etableres et "medium" sikkerhedsniveau.

Databehandleren er herefter berettiget og forpligtet til at træffe beslutninger om, hvilke tekniske og organisatoriske sikkerhedsforanstaltninger, der skal gennemføres for at etableret det nødvendige (og aftalte) sikkerhedsniveau.

Databehandleren skal dog – under alle omstændigheder og som minimum – gennemføre følgende foranstaltninger, som er aftalt med den dataansvarlige:

Risikovurdering
Databehandleren skal kunne dokumentere en regelmæssigt opdateret risikovurdering i forhold til den databehandling, som foretages for den dataansvarlige.
Databehandler skal minimum én gang årligt gennemgå risikovurderingen og vurdere og evaluere effekten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerheden.
Risikovurderingen skal som minimum opdateres i forbindelse med forestående ændringer af egne organisatoriske forhold, forestående ændringer af en eventuel underleverandørs forhold eller forestående ændringer af anvendt teknologi og infrastruktur herunder udstyr.

Organisatoriske
Alle medarbejdere hos databehandler har underskrevet en fortrolighedserklæring.

Awareness
Databehandleren skal sørge for, at dennes medarbejdere modtager den tilstrækkelige uddannelse og instruktioner for at sikre, at personoplysninger behandles i overensstemmelse med relevant lovgivning samt Databehandlerens politikker og procedurer herfor. Den enkelte medarbejder har modtaget instruks på ikke bare at måtte downloade elementer og specielt ikke arbejdsrelaterede elementer.
Computeren låses når den forlades. Ingen uvedkommen må "kigge" med på skærmen. Adgang til bygninger er styret med individuelle nøglekort/ elektroniske koder eller nøgler.

Databehandleren må til varetagelse af sine opgaver i henhold til denne aftale alene benytte personer, der er underlagt en fortrolighedsforpligtelse.
Databehandlerne skal ved medarbejderes fratrædelse have en procedure, der sikrer, systemrettigheder ophører, herunder at it-udstyr inddrages. Fratrådte medarbejdere er fortsat underlagt fortrolighed

Databehandleren skal sikre, at kun de personer, som autoriseres hertil, må have adgang til de personoplysninger, der behandles på vegne af den dataansvarlige.
Databehandleren må kun autorisere personer, der er beskæftiget med de formål, hvortil oplysningerne behandles jf. punkt C.1. De enkelte brugere må ikke autoriseres til anvendelser, som de ikke har specifikt behov for i forbindelse med aftalens opfyldelse. Leverandøren skal løbende sikre og dokumentere, at de autoriserede brugere fortsat opfylder dette krav. Kontrol heraf skal foretages mindst én gang hvert halve år.

Udover ovennævnte må databehandleren endvidere autorisere brugere, for hvem adgang til personoplysningerne er nødvendig med henblik på revision eller drifts- og systemtekniske opgaver i forbindelse med aftalens opfyldelse.

Beredskabsplaner
Databehandleren forpligter sig til at have et beredskab, der sikrer, at konsekvenserne af driftsafbrydelser som følge af eksempelvis et angreb eller nedbrud på forsyningsnetværket begrænses mest muligt.

Tekniske
Databehandleren har antivirus på alle arbejdsstationer.
E-mail anvendes udelukkende erhvervsmæssigt samt er der fokus på phishing og smishing mails og SMS'er. osv.

OCTOPUS PMS ApS • +45 73 700 100
info@octopuspms.com • octopuspms.com

Databehandler benytter underdatabehandler til lagring af data og håndtering af servere som oplyser.

Vi sikrer passende backup af data, der behandles på den dataansvarliges vegne, så risikoen for tab minimeres. Det skal regelmæssigt sikres, at backups kan genindlæses.

Beskyttelse af oplysninger under transmission
Databehandleren må kun anvende eksterne kommunikationsforbindelser til behandling af personoplysninger for den dataansvarlige, hvis der træffes tilstrækkelige foranstaltninger for at sikre, at uvedkommende ikke gennem disse forbindelser kan få adgang til oplysningerne.
Forsendelser af følsomme og fortrolige personoplysninger skal altid foregå med kryptering, end-to-end kryptering eller en alternativ sikker overførsel, som skal godkendes af den dataansvarlige. Ved krav om forsendelse af store datasæt med følsomme og fortrolige personoplysninger stilles der krav om end-to-end kryptering.

Beskyttelse af oplysninger under opbevaring
Vi anvender firewalls, VPN opkobling m.m. samt ligger vores data i datacentre med høj sikkerhed, begrænset adgange.
Der skal være etableret antivirus og firewall på databehandlerens udstyr og disse skal løbende holdes opdaterede gennem fastlagte procedurer.
Harddiske skal være krypterede med f.eks. bitlocker. Operativsystemet bør være opsat til at kryptere harddisken på den enkelte pc.
Databehandleren bør som udgangspunkt ikke benytte bærbare medier herunder USB-nøgler eller eksterne harddiske. Såfremt det ikke kan undgås, skal databehandleren sikre, at det bærbare medie er passende krypteret.

Opdateringer og ændringer
For databehandlerens eget udstyr, som indgår i eller anvendes ved levering af ydelserne, bør der være en dokumenteret proces for ændringshåndtering af hardware, software, og netværkskomponenter, herunder applikationer, services, operativsystemer, servere, databaser, firmware og netværksudstyr.

C.3 Bistand til den dataansvarlige
Databehandleren skal så vidt muligt – inden for det nedenstående omfang og udstrækning – bistå den dataansvarlige i overensstemmelse med Bestemmelse 9.1 og 9.2 ved at gennemføre følgende tekniske og organisatoriske foranstaltninger.

Databehandleren skal være behjælpelig i forhold til udøvelsen af de registreredes rettigheder, herunder:

- Indsigtsanmodninger
- Sletteanmodninger
- Anmodning om berigtigelse
- Anmodning om overførsel af data til anden dataansvarlig
- Anmodning om begrænsning af behandling

Databehandleren assisterer den dataansvarlige i fornødent omfang med henblik på at overholde pkt. 9.1 og 9.2.
Databehandleren er berettiget til, efter forudgående aftale, at fakturere for medgået tid og omkostninger.

C.4 Opbevaringsperiode/sletterutine
Personoplysninger opbevares i henhold til den dataansvarliges instruks.

Dataansvarlig kan via indstillinger i OCTOPUS PMS bestemme, hvornår gæstedetaljer skal anonymiseres samt hvornår fakturadokumentation skal anonymiseres. Dette er en enkelt og simpel opsætning hvorefter at data automatisk anonymiseres.

Dataansvarlig kan, via OCTOPUS PMS, dagligt hente alle data (fremtidige reservationer og bookinger) ud i en fil, der er læsbar i de fleste systemer. Databehandler henter dagligt og automatisk en sikkerhedsfil, der er læsbar i de fleste systemer. Vi opbevarer disse i 1 måned.

Dataansvarlig beslutter, via opsætningen i OC, selv hvem der skal have adgang til at hente filen samt hvordan denne opbevares.

Ved ophør af tjenesten vedrørende behandling af personoplysninger, skal databehandleren slette eller anonymiseres personoplysningerne i overensstemmelse med bestemmelse 11.1, medmindre den dataansvarlige – efter underskriften af disse

OCTOPUS PMS ApS • +45 73 700 100
info@octopuspms.com • octopuspms.com

bestemmelser – har ændret den dataansvarlige oprindelige valg. Sådanne ændringer skal være dokumenteret og opbevares skriftligt, herunder elektronisk, i tilknytning til bestemmelserne.

C.5 Lokalitet for behandling
Behandling af de af Bestemmelserne omfattede personoplysninger kan ikke uden den dataansvarliges forudgående skriftlige godkendelse ske på andre lokaliteter end de på enhver tid gældende adresser for selskabet som pt. er:

OCTOPUS PMS, Gerlachsgade 4, 4. sal, 6400 Sønderborg

Der arbejdes lejlighedsvis på hjemmearbejdsplads. Der arbejdes efter de samme retningslinjer som ved arbejde på virksomhedsadressen.

Ipnordic, Nygade 17, 6300 Gråsten eller til enhver tid gældende adresser for selskabet eller deres datacenter.

C.6 Instruks vedrørende overførsel af personoplysninger til tredjelande

Hvis den dataansvarlige ikke i disse Bestemmelser eller efterfølgende giver en dokumenteret instruks vedrørende overførsels af personoplysninger til et tredjeland, er databehandleren ikke berettiget til inden for rammerne af disse Bestemmelser at foretage sådanne overførsler.

C.7 Procedurer for den dataansvarliges revisioner, herunder inspektioner, med behandlingen af personoplysninger, som er overladt til databehandleren

Databehandleren kan én gang årligt for egen regning, men på den dataansvarliges foranledning, bekræfte skriftligt databehandlerens overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.

Bekræftelsen fremsendes uden unødig forsinkelse til den dataansvarlige til orientering.
Baseret på resultaterne af bekræftelsen, er den dataansvarlige berettiget til at anmode om gennemførelse af yderligere foranstaltninger med henblik på at sikre overholdelsen af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.

Den dataansvarlige eller en repræsentant for den dataansvarlige har herudover adgang til at foretage inspektioner, herunder fysiske inspektioner, af lokaliteterne hvorfra databehandleren foretager behandling af personoplysninger, herunder fysiske lokaliteter og systemer, der benyttes til eller i forbindelse med behandlingen. Sådanne inspektioner kan gennemføres, når den dataansvarlige finder det nødvendig, Vurderingen skal bero på fakta og ikke fornemmelse. Fysisk inspektion kræver forudgående aftale med databehandleren, og med et forudgående varsel på 3 uger, så databehandleren er forberedt på at kunne afsætte de nødvendige ressourcer til det.

Den dataansvarliges eventuelle udgifter i forbindelse med en fysisk inspektion afholdes af den dataansvarlige selv. Databehandleren er dog forpligtet til at afsætte de ressourcer (hovedsageligt den tid), der er nødvendig(e) for, at den dataansvarlige kan gennemføre sin inspektion og er berettiget til at fakturere for medgået tid og omkostninger.

C.8 Procedurer for revisioner, herunder inspektioner, med behandling af personoplysninger, som er overladt til underdatabehandlere

Den dataansvarlige fører tilsyn med underdatabehandleres overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser samt i henhold til Datatilsynets vejledninger.

Databehandleren eller en repræsentant for databehandleren har herudover adgang til at foretage inspektioner, herunder fysiske inspektioner, med lokaliteterne hvorfra underdatabehandleren foretager behandling af personoplysninger, herunder fysiske lokaliteter og systemer, der benyttes til eller i forbindelse med behandlingen. Sådanne inspektioner kan gennemføres, når databehandleren (eller den dataansvarlige) finder det nødvendigt.

OCTOPUS PMS ApS • +45 73 700 100
info@octopuspms.com • octopuspms.com

Dokumentation for sådanne inspektioner kan fremsendes uden unødig forsinkelse til den dataansvarlige til orientering. Den dataansvarlige kan anfægte rammerne for og/eller metoden af inspektionen og kan i sådanne tilfælde anmode om gennemførelsen af en ny inspektion under andre rammer og/eller under anvendelse af anden metode. Det skal være baseret på fakta og ikke fornemmelse.

19. Bilag D Parternes regulering af andre forhold

Følgende erstatter pkt. 7.6:
Databehandleren skal i sin aftale med underdatabehandleren indføje den dataansvarlige som begunstiget tredjemand, såfremt det er muligt, således at den dataansvarlige i tilfælde af at databehandleren faktisk eller retligt set er ophørt med at eksistere eller i tilfælde af databehandlerens konkurs, har ret til at opsige underdatabehandleraftalen og instruere underdatabehandleren i at slette eller tilbagelevere personoplysningerne.

OCTOPUS PMS ApS • +45 73 700 100
info@octopuspms.com • octopuspms.com