Databehandleraftale

Dataansvarlig: Amatørteateret Charlottentotterne (den "**dataansvarlige**") og

	Databehandleren:
Firma:	One.com Group AB
Registreringsnr.	559205-2400
By:	Malmö
Registreringsland:	Sverige

("**databehandleren**")
(omtales enkeltvis som (en) "**part**" og ved flere som "**parter(ne)**")

har indgået denne:

DATABEHANDLERAFTALE

(herefter benævnt "**aftalen**")
vedrørende databehandlerens behandling af personoplysninger på vegne af den dataansvarlige.

1. De behandlede personoplysninger

1.1 Denne aftale er indgået i forbindelse med den dataansvarliges brug af databehandlerens tjenester som en del af abonnementet og yderligere tjenester som beskrevet i "one.com Vilkår og betingelser" ("**hovedaftalen**").

1.2 Databehandleren behandler typerne af personoplysninger på vegne af den dataansvarlige i forhold til de relevante registrerede som angivet i **Skema 1**. Personoplysningerne vedrører de registrerede anført i **Skema 1**.

1.3 Databehandleren kan påbegynde behandling af personoplysninger på vegne af den dataansvarlige efter aftalens ikrafttræden. Behandlingen har den varighed, der er angivet i instruktionerne i aftalens **Skema 1**.

1.4 Aftalen og hovedaftalen er indbyrdes afhængige og kan ikke opsiges separat. Aftalen kan dog erstattes med en anden gyldig databehandleraftale uden opsigelse af hovedaftalen.

2. Formål

2.1 Databehandleren må kun behandle personoplysninger til formål, der er nødvendige for at opfylde databehandlerens forpligtelser, og i den forbindelse levere de tjenester, der er fastsat i hovedaftalen.

3. Den dataansvarliges forpligtelser

3.1 Den dataansvarlige garanterer, at personoplysningerne behandles med legitime og objektive formål og at databehandleren ikke behandler flere personoplysninger, end det er nødvendigt for at opfylde sådanne formål.

3.2 Den dataansvarlige er ansvarlig for at sikre, at der findes et gyldigt retsgrundlag for behandling på tidspunktet for overførsel af personoplysninger til databehandleren. Efter anmodning fra databehandleren forpligter den dataansvarlige sig skriftligt til at redegøre for og/eller levere dokumentation for grundlaget for behandlingen.

3.3 Den dataansvarlige garanterer desuden, at de registrerede, som personoplysningerne vedrører, er blevet oplyst tilstrækkeligt om behandlingen af deres personoplysninger.

4. Databehandlerens forpligtelser

4.1 Al behandling, som databehandleren foretager af de personoplysninger, der er leveret af den dataansvarlige, skal ske i overensstemmelse med de instruktioner, som den dataansvarlige har udarbejdet, og databehandleren er desuden forpligtet til at overholde al til enhver tid gældende databeskyttelseslovgivning. Hvis EU-retten eller national lovgivning i en EU-medlemsstat, som databehandleren er underlagt, foreskriver, at databehandleren skal behandle personoplysningerne anført i **Skema 1**, skal databehandleren underrette den dataansvarlige om dette juridiske krav, før personoplysningerne behandles. Dette gælder dog ikke, hvis denne lovgivning forbyder sådanne oplysninger af hensyn, der er vigtige for den offentlige interesse. Databehandleren skal straks underrette den dataansvarlige, hvis en instruktion efter databehandlerens opfattelse krænker EU's generelle databeskyttelsesforordning eller databeskyttelsesbestemmelserne i en EU-medlemsstat.

4.2 Databehandleren skal træffe alle nødvendige tekniske og organisatoriske sikkerhedsforanstaltninger, herunder alle yderligere foranstaltninger, der er nødvendige for at sikre, at personoplysningerne ikke utilsigtet eller ulovligt tilintetgøres, mistes eller forringes, eller at de bringes til uautoriserede tredjeparters kendskab, misbruges eller behandles på en måde, der strider mod den til enhver tid gældende databeskyttelseslovgivning. Disse foranstaltninger er nærmere beskrevet i **Skema 2**.

4.3 Databehandleren skal sikre, at medarbejdere, der er autoriseret til at behandle personoplysninger, har underskrevet en fortrolighedserklæring eller er underlagt den relevante lovfæstede tavshedspligt.

4.4 Hvis den dataansvarlige anmoder derom, skal databehandleren erklære og/eller dokumentere, at databehandleren efterlever kravene i gældende databeskyttelseslovgivning, herunder dokumentation vedrørende databehandlerens datastrømme samt procedurer/politikker for behandling af personoplysninger.

4.5 Under hensyntagen til behandlingens art skal databehandleren så vidt muligt bistå den dataansvarlige med passende tekniske og organisatoriske foranstaltninger med henblik på at opfylde den dataansvarliges forpligtelse til at besvare anmodninger om udøvelse af den registreredes rettigheder, som fastsat i kapitel 3 i den generelle databeskyttelsesforordning.

4.6 Databehandleren eller en anden databehandler (underdatabehandler) skal sende anmodninger og indsigelser fra de registrerede til den dataansvarlige med henblik på dennes videre behandling deraf, medmindre databehandleren selv er berettiget til at behandle en sådan anmodning. Hvis den dataansvarlige beder om det, skal databehandleren hjælpe den dataansvarlige med at besvare sådanne anmodninger og/eller indsigelser.

4.7 Hvis databehandleren behandler personoplysninger i et andet EU-land, skal databehandleren overholde det pågældende lands lovgivning om sikkerhedsforanstaltninger.

4.8 Databehandleren skal underrette den dataansvarlige, hvis der sker en driftsafbrydelse, en mistanke om, at databeskyttelsesreglerne er blevet overtrådt, eller der opstår andre uregelmæssigheder i forbindelse med behandlingen af personoplysningerne. Databehandleren har en frist på 24 timer fra det øjeblik, vedkommende bliver opmærksom på et sikkerhedsbrud, til at oplyse den dataansvarlige om et sikkerhedsbrud. Databehandleren skal efter anmodning fra den dataansvarlige bistå den dataansvarlige med henblik på at klarlægge omfanget af sikkerhedsbruddet, herunder udarbejdelse af en notifikation til det relevante databeskyttelsesagentur og/eller de registrerede.

4.9 Databehandleren skal stille alle oplysninger til rådighed for den dataansvarlige, som er nødvendige for at påvise overensstemmelse med artikel 28 i den generelle databeskyttelsesforordning og aftalen. I denne forbindelse giver databehandleren mulighed for og bidrager til revisioner, herunder inspektioner, der udføres af den dataansvarlige eller en anden revisor, som er udpeget af den dataansvarlige.

4.10 Ud over ovennævnte skal databehandleren bistå den dataansvarlige med at sikre, at den dataansvarliges forpligtelser i henhold til artikel 32-36 i den generelle databeskyttelsesforordning overholdes. Denne bistand tager hensyn til arten af behandlingen og de oplysninger, der er tilgængelige for databehandleren.

5. Overførsel af data til underdatabehandlere eller tredjeparter

5.1 Databehandleren skal opfylde betingelserne i artikel 28, stk. 2 og 4, i den generelle databeskyttelsesforordning for at kunne benytte sig af en anden databehandler (underdatabehandler). Dette indebærer, at databehandleren ikke benytter sig af en anden databehandler (underdatabehandler) til udførelse af aftalen uden forudgående specifik eller generel skriftlig godkendelse fra den dataansvarlige.

5.2 Den dataansvarlige giver herved databehandleren en generel fuldmagt til at indgå aftaler med underdatabehandlere. Databehandleren skal underrette den dataansvarlige om eventuelle ændringer vedrørende tilføjelse eller udskiftning af underdatabehandlere senest 30 dage før en ny underdatabehandler påbegynder behandlingen af personoplysningerne. Den dataansvarlige kan fremsætte rimelige og relevante indsigelser mod sådanne ændringer inden for 14 dage fra modtagelsen af meddelelsen. Hvis databehandleren fortsat ønsker at benytte en underdatabehandler, som den dataansvarlige har gjort indsigelse mod, har parterne ret til at opsige aftalen, jf. punkt 7.

5.3 Når den dataansvarlige har godkendt, at databehandleren kan bruge en underdatabehandler, skal databehandleren pålægge underdatabehandleren de samme forpligtelser som fastsat i aftalen. Dette sker gennem en kontrakt eller et andet retsligt dokument i henhold til EU-retten eller en medlemsstats nationale lovgivning. Det skal fx sikres, at underdatabehandleren stiller tilstrækkelige garantier for at kunne gennemføre passende tekniske og organisatoriske foranstaltninger på en sådan måde, at behandlingen opfylder kravene i den generelle databeskyttelsesforordning ("back-to-back"-vilkår).

5.4 Hvis underdatabehandleren ikke opfylder sine forpligtelser vedrørende databeskyttelse, er databehandleren fuldt ud ansvarlig over for den dataansvarlige for udførelsen af underdatabehandlerens forpligtelser.

5.5 Videregivelse, overførsel og intern brug af den dataansvarliges personoplysninger til tredjelande eller internationale organisationer må kun ske i overensstemmelse med dokumenterede instruktioner fra den dataansvarlige - medmindre dette er fastsat i EU-retten eller i den nationale lovgivning i en medlemsstat, som databehandleren er underlagt. I så fald skal databehandleren underrette den dataansvarlige om dette juridiske krav før behandlingen, medmindre loven forbyder en sådan meddelelse af hensyn til vigtige offentlige interesser.

5.6 Hvis de personoplysninger, der er anført i **Skema 1**, overføres til underdatabehandlere uden for EU/EØS, skal det i den nævnte aftale anføres, at databeskyttelseslovgivningen i den dataansvarliges land gælder for underdatabehandlere. Hvis den modtagende underdatabehandler er etableret i EU/EØS, skal det i den nævnte databehandlingsaftale anføres, at det modtagende EU-lands specifikke lovfæstede krav til databehandlere, fx vedrørende krav om notifikation af nationale myndigheder, skal efterleves.

5.7 Databehandleren er forpligtet til at indgå skriftlige aftaler om databehandling med underdatabehandlere i EU/EØS. Hvad angår underdatabehandlere uden for EU/EØS, skal databehandleren sikre de nødvendige overførselsmekanismer og indgå en underdatabehandlingsaftale ved indgåelse af standardaftaler i overensstemmelse med EU-Kommissionens standardkontraktbestemmelser ("**Standardkontrakter**") baseret på 2021/914/EU af 4. juni 2021.

5.8 På tidspunktet for undertegnelsen af denne aftale benytter databehandleren sig af de underdatabehandlere, der er anført i **Skema 3**.

6. Ansvar

6.1 Parternes ansvar er underlagt hovedaftalen.

6.2 Parternes erstatningsansvar i henhold til denne aftale er underlagt hovedaftalen.

7. Ikrafttrædelsesdato og opsigelse

7.1 Denne aftale træder i kraft samtidigt med hovedaftalen. I tilfælde af opsigelse af hovedaftalen opsiges ligeledes denne aftale. Databehandleren er dog fortsat underlagt de forpligtelser, der er fastsat i denne aftale, så længe databehandleren behandler personoplysninger på vegne af den dataansvarlige.

7.2 Efter afslutning af behandlingstjenesterne er databehandleren forpligtet til, efter anmodning fra den dataansvarlige, at slette eller returnere alle personoplysninger til den dataansvarlige samt at slette eksisterende kopier, medmindre opbevaring af personoplysningerne er foreskrevet i EU-retten eller den nationale lovgivning.

8. Gældende lovgivning og anvendt jurisdiktion

8.1 Ethvert krav eller enhver tvist, der opstår som følge af eller i forbindelse med denne aftale, skal afgøres af en kompetent ret i første instans i samme jurisdiktion og med samme lovvalg som fastsat i hovedaftalen.

9. Underskrifter

For den dataansvarlige:

_____

Amatørteateret Charlottentotterne
v. Lars Hansen, Formand
Egenæsvej 4
4571 Grevinge

info@charlottentotterne.dk

Cvr nr: 300 262 25

For databehandleren:

_____

Ronni Engelhardt CEO

Skema 1
Kategorier af registrerede, typer af personoplysninger og instruktioner

1. Kategorier af registrerede:

- Databehandleren vil behandle kontaktoplysninger om den dataansvarliges faktiske, potentielle eller tidligere kunder og/eller medlemmer, medarbejdere, leverandører, forretnings- og samarbejdspartnere samt associerede selskaber.
- Databehandleren har sat sit system til den dataansvarliges disposition som en hostet tjeneste, og databehandleren kan ikke bestemme alle kategorier af registrerede. Hvis den dataansvarlige hoster data om yderligere kategorier af registrerede hos databehandleren, er det den dataansvarliges pligt at registrere disse oplysninger.

2. Typer af personoplysninger:

- Kontakt- og identifikationsoplysninger, herunder e-mail.
- IP-adresser
- Domænenavne
- Brugernavne
- Oplysninger om medlemskab
- Analyser og brugsdata
- Ordrehistorik og -oplysninger
- Kontrakter
- Kommunikation
- Support

- Billeder
- Der kan forekomme andre typer af personoplysninger

3. Instruktioner

Service

Databehandleren kan behandle personoplysninger vedrørende de registrerede med det formål at levere, udvikle, håndtere, administrere og styre tjenesterne i hovedaftalen, herunder sikre stabilitet og oppetid for vores servere og opfylde juridiske krav.

Opbevaringsperiode

De personoplysninger, der er gemt/hostet i vores systemer, slettes eller anonymiseres inden for et rimeligt tidsrum, efter at den dataansvarlige har opsagt hovedaftalen fuldstændigt. Undtagelser er data, hvor der er et lovkrav om, at databehandleren skal gemme dem længere. Denne type data vil typisk blive slettet inden for otte uger, men kan slettes tidligere. Andre typer data, der er gemt i logfiler osv., slettes efter et rimeligt tidsrum, typisk inden for 8 uger, hvorefter de slettes hos databehandleren.

Sted for behandlingen

Behandling af personoplysninger, der er omfattet af aftalen, må ikke uden den dataansvarliges forudgående skriftlige samtykke foretages andre steder end på databehandlerens adresse og adressen på de underdatabehandlere, der er anført i Skema 3.

Inspektion af databehandler

Databehandleren skal for egen regning en gang om året lade en revisions-/inspektionsrapport udarbejde af en tredjepart vedrørende databehandlerens efterlevelse af denne aftale og disse skemaer. Rapporten eller et andet revisionsformat skal sendes til den dataansvarlige eller offentliggøres på den dataansvarliges websted så hurtigt som muligt efter udarbejdelsen.

Skema 2
Sikkerhedsforanstaltninger

Domæne	Fremgangsmåder
Organisering af informationssikkerhed	**Ejerskab af sikkerhed**. one.com har udpeget en sikkerhedsansvarlig, der skal koordinere og overvåge sikkerhedsregler og -procedurer. En ledelse bestående af enkeltpersoner på c-niveau bistår og vejleder den sikkerhedsansvarlige. **Sikkerhedsroller og ansvarsområder**. one.com-personale med adgang til kundedata er underlagt fortrolighedsforpligtelser, som understreges ved ansættelsen, og holdes løbende bevidste herom. **Risikoledelse**. one.com udfører løbende risikovurdering, der er en del af risikoledelsen, før behandling af kundedata eller lancering af services. Risikoledelsessporet gør det muligt at fokusere på relevante trusler ved at prioritere, strukturere og mindske risici ud over det, der kan accepteres. Der er implementeret sikkerhedskopiering.

Domæne	Fremgangsmåder
	Databehandleren opbevarer sine sikkerhedsdokumenter i henhold til vedkommendes opbevaringskrav, efter at de ikke længere er i kraft.
Forvaltning af aktiver	**Aktivfortegnelse**. Databehandleren fører en oversigt over alle medier, som kundedata lagres på. Adgang til fortegnelserne over sådanne medier er begrænset til det af databehandlerens personale, der har skriftlig godkendelse til at have en sådan adgang. **Håndtering af aktiver** - one.com klassificerer kundedata for bedre at kunne identificere dem og for at sikre passende begrænsning af adgangen til dem. - Databehandlerens personale skal indhente databehandlerens godkendelse, før der gemmes kundedata på bærbare enheder, gives fjernadgang til kundedata eller behandles kundedata uden for databehandlingsvirksomhedens faciliteter.
Sikkerhed for menneskelige ressourcer	**Sikkerhedsuddannelse**. one.com oplyser personalet om relevante sikkerhedsprocedurer og deres respektive roller samt om nye trusler osv., hvor medarbejderne spiller en afgørende rolle.
Fysisk og miljømæssig sikkerhed	**Fysisk adgang til faciliteter**. one.com giver kun navngivne godkendte personer adgang til faciliteter, hvor informationssystemer, der behandler kundedata, er placeret. **Fysisk adgang til komponenter**. one.com sikrer tilstrækkelige begrænsninger for medier, der indeholder kundedata. **Beskyttelse mod forstyrrelser**. one.com bruger en række af branchens standardsystemer til at beskytte mod tab af data på grund af strømsvigt, oversvømmelse, brand eller ledningsforstyrrelser. **Bortskaffelse af komponenter**. one.com bruger branchens standardprocesser til at slette kundedata, når der ikke længere er brug for dem.
Kommunikations- og driftsstyring	**Driftspolitik**. one.com har sikkerhedsdokumenter, der beskriver sikkerhedsforanstaltningerne og de relevante procedurer og ansvarsområder for det personale, der har adgang til kundedata. **Procedurer for gendannelse af data** - one.com gemmer kopier af kundedata og procedurer for gendannelse af data et andet sted end det sted, hvor det primære computerudstyr, der behandler kundedata, er placeret. - one.com har specifikke procedurer for adgang til kopier af kundedata. **Skadelig software**. one.com har anti-malware-kontroller for at undgå, at skadelig software får ikke-godkendt adgang til kundedata, herunder skadelig software, der stammer fra offentlige net. Der er også implementeret antivirus. **Hændelseslogning**. one.com logger eller gør det muligt for kunden at logge, tilgå og bruge informationssystemer, der indeholder kundedata, registrere adgangs-id, klokkeslæt, godkendelse givet eller nægtet samt relevant aktivitet.

Domæne	Fremgangsmåder
	Kryptering. Kommunikation via internettet mellem systemer, der håndterer personoplysninger, krypteres.
Adgangskontrol	**Adgangspolitik**. one.com fører en fortegnelse over sikkerhedsrettigheder for personer, der har adgang til kundedata. **Adgangsgodkendelse** - one.com deaktiverer godkendelsesrettigheder, der ikke har været brugt i en periode på højst seks måneder. - one.com identificerer det personale, der kan give, ændre eller annullere godkendt adgang til data og ressourcer. - one.com sikrer, at når mere end én person har adgang til systemer, der indeholder kundedata, har de enkelte personer egne identifikatorer/logins. **Mindste privilegium** - one.com begrænser adgangen til kundedata til kun at omfatte personer, der har brug for en sådan adgang i forbindelse med deres jobfunktion. **Integritet og fortrolighed** - one.com instruerer personalet om at deaktivere den administrative behandling, når de forlader lokalerne, eller når computere på anden måde efterlades uden opsyn. - one.com gemmer adgangskoder på en måde, der gør dem ulæselige, mens de er i kraft. **Godkendelse** - one.com anvender branchens standardprocedurer til at identificere og godkende brugere, der forsøger at få adgang til informationssystemerne. - Hvis godkendelsesmekanismerne er baseret på adgangskoder, kræver databehandleren, at adgangskoderne fornys regelmæssigt. - one.com sikrer, at deaktiverede eller udløbne identifikatorer ikke tildeles andre personer. - one.com overvåger eller gør det muligt for kunden at overvåge gentagne forsøg på at få adgang til informationssystemet ved hjælp af en ugyldig adgangskode. - one.com anvender standardprocedurer for deaktivering af adgangskoder, der er blevet ødelagt eller utilsigtet videregivet. - one.com anvender branchens standardfremgangsmåder for beskyttelse af adgangskoder, herunder fremgangsmåder, der er udviklet til at bevare adgangskodernes fortrolighed og integritet, når de tildeles og distribueres, og under opbevaring. **Netværksdesign**. one.com har kontroller for at undgå, at enkeltpersoner, der antager adgangsrettigheder, som de ikke har fået tildelt, får adgang til kundedata, som de ikke har tilladelse til at få adgang til.
Håndtering af hændelser i forbindelse med informationssikkerhed	**Procedure for hændelsesrespons** - one.com fører en fortegnelse over brud på sikkerheden med en beskrivelse af overtrædelsen, tidsrummet, konsekvenserne af

Domæne	Fremgangsmåder
	bruddet, navnet på indberetteren, og til hvem overtrædelsen blev indberettet, samt proceduren for gendannelse af data. - For hvert sikkerhedsbrud, der er en sikkerhedsrelateret hændelse, vil one.com give meddelelse herom uden unødig forsinkelse og under alle omstændigheder inden for 72 timer. - one.com sporer eller sætter kunden i stand til at spore oplysninger om kundedata, herunder hvilke data der er blevet videregivet til hvem og hvornår.
Styring af forretningskontinuitet	- one.com har nød- og beredskabsplaner for de faciliteter, hvor databehandlingssystemets informationssystemer til behandling af kundedata er placeret. - one.com's redundante lagring og procedurerne for gendannelse af data er designet til at forsøge at rekonstruere kundedata i deres oprindelige eller senest replikerede tilstand fra før det tidspunkt, hvor de gik tabt eller blev ødelagt.

Skema 3
Liste over underdatabehandlere

Leverandør	Sted	Funktion	Opdateret
Global Connect A/S	DK	Datacenter	20.02.2021
Interxion	DK	Datacenter	12.04.2021
Interxion	DK/UK/NL/FR/DE	PoP (Point of presence)	12.04.2021
Equinix	SE	PoP (Point of presence)	12.04.2021