# PERSONUPPGIFTSBITRÄDESAVTAL

Personuppgiftsbiträdesavtal mellan

Föreningens namn
Adress
Postnr Ort
Org. nr. 000000-0000

(nedan kallad ”Personuppgiftsansvarig”)

och

Simply Brf AB
Skeppsgatan 10
211 11 Malmö
Org. nr. 559234-2892

(nedan kallad ”personuppgiftsbiträde”)

(nedan kallade ”parterna” och separat ”part”)

har ingått följande Personuppgiftsbiträdesavtal (”Personuppgiftsbiträdesavtalet”) gällande personuppgiftsbiträdets behandling av personuppgifter på uppdrag av den personuppgiftsansvariga.

## 1 BAKGRUND, SYFTE OCH OMFATTNING

1.1 Som en del av personuppgiftsbiträdets leverans av hostingtjänster (”tjänster”) behandlar personuppgiftsbiträdet personuppgifter för vilka den personuppgiftsansvariga ansvarar.

1.2 Personuppgiftsbiträdet uppfyller gällande lagstadgade krav för personuppgiftsbiträde, inklusive dataskyddsförordningen från den 25 maj 2018;
(Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter) och relaterade rättsakter samt härledd nationell lagstiftning.

1.3 Det är ett krav i dataskyddsförordningen att det mellan parterna ingås ett skriftligt avtal om den behandling som ska utföras, ett så kallat ”personuppgiftsbiträdesavtal”. Detta personuppgiftsbiträdesavtal utgör ett sådant personuppgiftsbiträdesavtal.

1.4 Personuppgiftsbiträdesavtalet omfattar alla tjänster som den personuppgiftsansvariga har hos personuppgiftsbiträdet vid personuppgiftsbiträdesavtalets ikraftträdande och framtida förvärv hos personuppgiftsbiträdet. Om personuppgiftsbiträdets leverans ändras i en sådan utsträckning att den personuppgiftsansvarigas instruktioner ändras, kommer parterna att ingå ett nytt personuppgiftsbiträdesavtal.

## 2 PERSONUPPGIFTER SOM OMFATTAS AV PERSONUPPGIFTSBITRÄDESAVTALET

2.1 Personuppgiftsbiträdesavtalet och tillhörande riktlinjer inkluderar alla typer av personuppgifter som den personuppgiftsansvariga tillhandahåller personuppgiftsbiträdet i förhållande till de tjänster som personuppgiftsbiträdet levererat.

2.2 Kategorier av registrerade personer som personuppgifterna avser kan exempelvis vara användare, anställda, medlemmar, hyresgäster, leverantörer eller liknande.

## 3 GEOGRAFISKA KRAV

3.1 Den behandling av personuppgifter som personuppgiftsbiträdet utför i enlighet med avtalet med den personuppgiftsansvariga får endast utföras av personuppgiftsbiträdet eller underbiträde, jfr punkt 5, inom det europeiska ekonomiska samarbetet (EES). Personuppgiftsbiträdet har inte på något sätt rätt att låta databehandling ske utanför EES utan skriftligt samtycke från den personuppgiftsansvariga, såvida inte detta krävs enligt EU-lagstiftning eller nationell lagstiftning i medlemsländerna, vilken personuppgiftsbiträdet är underställd. I det fallet ska personuppgiftsbiträdet underrätta den personuppgiftsansvariga om detta rättsliga krav innan behandling, såvida aktuell lagstiftning inte förbjuder en sådan underrättelse av hänsyn till viktiga allmänintressen.

## 4 INSTRUKSTIONER

4.1 Den primära databehandling som personuppgiftsbiträdet utför är lagring av de data som den personuppgiftsansvariga tillhandahåller personuppgiftsbiträdet. Om den personuppgiftsansvariga önskar andra former av databehandling som inte är relaterade till de tjänster som personuppgiftsbiträdet levererar, ska den personuppgiftsansvariga ge personuppgiftsbiträdet tydliga dokumenterade instruktioner om detta.

4.2 Personuppgiftsbiträdet handlar endast efter dokumenterade instruktioner från den personuppgiftsansvariga. Personuppgiftsbiträdet ska säkerställa att tillhandahållna personuppgifter inte används för andra ändamål, eller behandlas på ett annat sätt, än vad som framgår av den personuppgiftsansvarigas instruktioner.

4.3 Om en instruktion enligt personuppgiftsbiträdets uppfattning strider mot lagstiftningen ska personuppgiftsbiträdet informera den personuppgiftsansvariga om detta.

4.4 Om behandling av personuppgifter hos personuppgiftsbiträdet sker helt eller delvis med hjälp av fjärranslutning, inklusive hemarbetsplatser, ska personuppgiftsbiträdet fastställa riktlinjer för de anställdas behandling av personuppgifter med hjälp av fjärranslutning, vilket även ska uppfylla de krav som ställts i personuppgiftsbiträdesavtalet.

4.5 Personuppgiftsbiträdet ska så långt det är möjligt bistå den personuppgiftsansvariga med att uppfylla den personuppgiftsansvarigas skyldigheter att svara på begäranden om utövande av de registrerades rättigheter, inklusive insikt, rättelse, begränsning eller radering, om de relevanta personuppgifterna behandlas av personuppgiftsbiträdet. Om personuppgiftsbiträdet mottar sådana begäranden från de registrerade ska personuppgiftsbiträdet informera den personuppgiftsansvariga om detta.

4.6 Den personuppgiftsansvariga ansvarar för personuppgiftsbiträdets alla kostnader vid ett sådant bistånd, jfr punkt 4,5, inklusive till underbiträde. Personuppgiftsbiträdets bistånd faktureras till personuppgiftsbiträdets gällande timtaxa för ett sådant arbete.

## 5 ANVÄNDNING AV UNDERBITRÄDE

5.1 Den personuppgiftsansvariga ger personuppgiftsbiträdet samtycke till användning av underbiträde, förutsatt att de villkor som anges i personuppgiftsbiträdesavtalet är uppfyllda. Den personuppgiftsansvariga kan alltid se personuppgiftsbiträdets underbiträde på personuppgiftsbiträdets webbplats på support.simplybrf.se/gdpr, där personuppgiftsbiträdet informerar om ändringar i valet av underbiträde.

5.2 Underbiträden är underställd personuppgiftsbiträdets instruktioner. Personuppgiftsbiträdet har ingått ett skriftligt personuppgiftsbiträdesavtal med underbiträden, vari det säkerställs att underbiträdet uppfyller krav som motsvarar dem som ställs på personuppgiftsbiträdet av den personuppgiftsansvariga enligt personuppgiftsbiträdesavtalet.

5.3 Kostnader förbundna med upprättandet av avtalsförhållandet med en underbiträde, inklusive kostnader för utarbetandet av personuppgiftsbiträdesavtalet och eventuellt upprättande av grund för överföring till tredje land, bärs av personuppgiftsbiträdet och berör därför inte den personuppgiftsansvariga.

5.4 Om den personuppgiftsansvariga önskar instruera underbiträde direkt bör detta endast ske efter samråd med och via personuppgiftsbiträdet. Om den personuppgiftsansvariga utfärdar instruktioner direkt till underbiträdet ska den personuppgiftsansvariga senast samtidigt underrätta personuppgiftsbiträdet om instruktionen och bakgrunden till denna. Om den personuppgiftsansvariga instruerar underbiträdet direkt a) är personuppgiftsbiträdet befriad från allt ansvar, och alla följder av en sådan instruktion är endast den personuppgiftsansvarigas ansvar, b) ansvarar den personuppgiftsansvariga för alla kostnader som instruktionen kan medföra för personuppgiftsbiträdet, däribland är personuppgiftsbiträdet berättigad att fakturera den personuppgiftsansvariga med sin vanliga timtaxa för all arbetstid som en sådan direkt instruktion kan medföra för personuppgiftsbiträdet, och (c) den personuppgiftsansvariga är själv ansvarig gentemot underbiträdet för alla kostnader, ersättningar eller annan betalning till underbiträdet som den direkta instruktionen kan medföra.

5.5 Den personuppgiftsansvariga accepterar vid ingåendet av detta personuppgiftsbiträdesavtal att personuppgiftsbiträdet är berättigad till att byta underbiträde, förutsatt att a) en eventuell ny underbiträde uppfyller motsvarande villkor som anges i punkt 5 i detta avtal till den nuvarande underbiträdet, och att b) den personuppgiftsansvariga senast vid en eventuell annan underbiträdes påbörjande av behandlingen av personuppgifter, som den personuppgiftsansvariga är personuppgiftsansvarig för, framgår på personuppgiftsbiträdets webbplats.

5.6 Om den personuppgiftsansvariga inte vill att personuppgiftsbiträdet ska använda ett nytt underbiträde som informerats, jfr punkt 5.6, ska den personuppgiftsansvariga lämna en skriftlig invändning till personuppgiftsbiträdet mot användningen av ett sådant nytt underbiträde senast 14 dagar efter mottagandet av informationen eller då den personuppgiftsansvariga fick kännedom om underbiträdet på personuppgiftsbiträdets webbplats. Om personuppgiftsbiträdet inte anser sig vara i stånd att tillmötesgå en eventuell invändning från den personuppgiftsansvariga gentemot ett nytt underbiträde meddelas detta till den personuppgiftsansvariga snarast möjligt, och den personuppgiftsansvariga kan i så fall härefter säga upp sina produkter med en månads upp-

sägning från den 1:e i en månad. För att invändningen ska kunna resultera i detta varsel om uppsägning ska det föreligga en saklig grund för invändningen.

## 6 BEARBETNING OCH UTLÄMNANDE AV PERSONUPPGIFTER

6.1 Den personuppgiftsansvariga garanterar att ha nödvändig rättslig grund för behandling av de personuppgifter som omfattas av detta personuppgiftsbiträdesavtal.

6.2 Personuppgiftsbiträdet får inte utan skriftligt samtycke från den personuppgiftsansvariga lämna ut information till tredje part, såvida inte sådan utlämning av information följer av lagstiftningen eller av en bindande begäran från en rättsinstans eller en dataskyddsmyndighet, eller den framgår av detta personuppgiftsbiträdesavtal.

## 7 SÄKERHET

7.1 Personuppgiftsbiträdet måste vidta lämpliga tekniska och organisatoriska skyddsåtgärder mot oavsiktlig eller olaglig förstörelse, förlust eller försämring av personuppgifter samt mot att obehöriga får kännedom om dem, att de missbrukas eller på annat sätt behandlas i strid med lagstiftningen, jfr punkt 1.2 ovan.

7.2 Personuppgiftsbiträdet ska implementera och upprätthålla de säkerhetsåtgärder som beskrivs i bilaga 1.

7.3 Personuppgiftsbiträdet är alltid berättigad att implementera alternativa säkerhetsåtgärder under förutsättning att sådana säkerhetsåtgärder som ett minimum uppfyller eller ger större säkerhet än de säkerhetsåtgärder som beskrivs i bilaga 1. Personuppgiftsbiträdet kan inte utan den personuppgiftsansvarigas skriftliga förhandsgodkännande företa någon försämring av säkerhetsvillkoren.

7.4 Om personuppgiftsbiträdet är etablerad i ett annan EU-land ska de bestämmelser om säkerhetsåtgärder som är fastställda i lagstiftningen i det EU-land där personuppgiftsbiträdet är etablerad vidare gälla för personuppgiftsbiträdet. Om personuppgiftsbiträdet är etablerad i ett annat EU-land måste personuppgiftsbiträdet uppfylla både de säkerhetskrav som omfattas av gällande lagstiftning i Sverige och säkerhetskraven i personuppgiftsbiträdets hemland. Detsamma gäller för underbiträde.

7.5 Personuppgiftsbiträdet ska enligt särskild överenskommelse med den personuppgiftsansvariga i största möjliga utsträckning bistå den personuppgiftsansvariga med att säkerställa att skyldigheterna i artikel 32 i förordningen uppfylls (genomförande av lämpliga tekniska och organisatoriska åtgärder), 35 (genomförande av konsekvensbedömning av dataskydd) och 36 (föregående samråd). Om den personuppgiftsansvariga kräver ytterligare bistånd än personuppgiftsbiträdets standardförfaranden för att följa ovanstående artiklar, är personuppgiftsbiträdet berättigad till att fakturera den personuppgiftsansvariga med sin vanliga timtaxa för hela personuppgiftsbiträdets arbetstid som ett sådant avtal kan medföra för personuppgiftsbiträdet, och den personuppgiftsansvariga ansvarar även för eventuell betalning till underbiträdet.

## 8 TYSTNADSPLIKT

8.1 Personuppgiftsbiträdet ska på den personuppgiftsansvarigas begäran tillhandahålla den personuppgiftsansvariga tillräcklig information så att denna kan säkerställa att personuppgiftsbiträdet uppfyller dataskyddsförordningens artikel 28 samt personuppgiftsbiträdesavtalet.

8.2 I den utsträckning den personuppgiftsansvariga önskar att detta ska omfatta den behandling som sker hos underbiträde informeras personuppgiftsbiträdet om detta. Personuppgiftsbiträdet inhämtar härefter tillräcklig information från underbiträdet.

8.3 Om den personuppgiftsansvariga vill utföra tillsyn, enligt vad som anges i punkt 8 i detta avtal, ska den personuppgiftsansvariga alltid ge personuppgiftsbiträdet varsel på minst 30 dagar i en sådan förbindelse.

8.4 Den personuppgiftsansvariga ansvarar för alla kostnader som är förknippade med tillsyn av säkerhetsförhållanden hos personuppgiftsbiträdet, samt i förhållande till underbiträdet, däribland är personuppgiftsbiträdet berättigad att fakturera den personuppgiftsansvariga med sin vanliga timtaxa för hela personuppgiftsbiträdets arbetstid som en sådan tillsyn kan medföra för personuppgiftsbiträdet, och den personuppgiftsansvariga ansvarar även för eventuell betalning till underbiträdet.

## 9 ÖVERTRÄDELSE AV PERSONUPPGIFTSSKYDD

9.1 Om personuppgiftsbiträdet får kännedom om en överträdelse av personuppgiftsskyddet, vilken definieras som ett brott mot säkerheten, som leder till oavsiktlig eller olaglig förstörelse, förlust, ändring, obehörigt utlämnande av eller tillgång till personuppgifter som har överförts, lagras eller på annat sätt behandlats, är personuppgiftsbiträdet skyldig att utan onödigt dröjsmål försöka lokalisera en sådan överträdelse och i så stor utsträckning som möjligt försöka begränsa den uppstådda skadan samt i den uträckning det är möjligt återställa eventuella förlorade data.

9.2 Personuppgiftsbiträdet är också skyldig att utan onödigt dröjsmål informera den personuppgiftsansvariga efter kännedom om att det har skett en överträdelse av personuppgiftsskyddet. Personuppgiftsbiträdet ska därefter utan onödigt dröjsmål och i den utsträckning det är möjligt lämna skriftligt besked till den personuppgiftsansvariga, som så långt det är möjligt ska innehålla:
a) En beskrivning av överträdelsens art, inklusive kategorierna och ungefärligt antal berörda registrerade och registreringar av personuppgifter.
b) Namn och kontaktuppgifter för dataskyddskonsulten.
c) En beskrivning av de troliga konsekvenserna av överträdelsen.
d) En beskrivning av de åtgärder som personuppgiftsbiträdet eller underbiträdet har vidtagit eller föreslagit för att hantera överträdelsen, inklusive åtgärder för att begränsa dess möjliga skadeverkningar.

9.3 I den utsträckning det inte är möjligt att ge den information som anges i punkt 9.2 kan informationen meddelas stegvis utan onödigt ytterligare dröjsmål.

9.4 På samma sätt är underbiträdet skyldig att informera personuppgiftsbiträdet utan onödigt dröjsmål i enlighet med punkterna 9.2 och 9.3.

## 10 TYSTNADSPLIKT

10.1 Personuppgiftsbiträdet ska hålla de personuppgifter som behandlas i enlighet med personuppgiftsbiträdesavtalet under sekretess, och är således ensam berättigad att använda personuppgifterna som en del av uppfyllandet av sina skyldigheter och rättigheter enligt personuppgiftsbiträdesavtalet. Personuppgiftsbiträdet ska underställa anställda och eventuella andra, inklusive underbiträde, som är behöriga att behandla de personuppgifter som omfattas i personuppgiftsbiträdesavtalet sekretess gällande uppgifterna. Sådan konfidentialitet gäller även efter det att personuppgiftsbiträdesavtalet upphör.

## 11 FÖRETRÄDE

11.1 Om inget annat anges i personuppgiftsbiträdesavtalet har bestämmelserna i personuppgiftsbiträdesavtalet företräde i förhållande till motsvarande bestämmelser i andra avtal eller villkor mellan parterna.

## 12 VARAKTIGHET OCH UPPHÖRANDE AV PERSONUPPGIFTSBITRÄDESAVTALET

12.1 Personuppgiftsbiträdesavtalet träder i kraft vid parternas underskrift.

12.2 Detta personuppgiftsbiträdesavtal ersätter eventuella tidigare ingångna personuppgiftsbiträdesavtal mellan parterna.

12.3 Personuppgiftsbiträdet är bunden av detta personuppgiftsbiträdesavtal, så länge den personuppgiftsansvariga har en aktiv produkt hos personuppgiftsbiträdet och personuppgiftsbiträdet behandlar personuppgifter på uppdrag av den personuppgiftsansvariga. När den personuppgiftsansvariga raderar sina produkter, eller dessa går ut, är personuppgiftsbiträdet berättigad att radera alla personuppgifter som har behandlats på uppdrag av den personuppgiftsansvariga. Personuppgiftsbiträdet måste dock alltid bevara den behandlade informationen om detta följer av EU-lagstiftning eller nationell lagstiftning i medlemsländerna.

**13 UNDERSKRIFT**

13.1 Ovanstående ingås härmed med verkan genom parternas underskrift.

……

Firmatecknare Simply Brf AB
Personuppgiftsbiträde

……

Personuppgiftsansvarig

……

Personuppgiftsansvarig

# DATA-SÄKERHETSMILJÖ

Databehandlingsavtal -
Bilaga 1

Simply Brf använder Oderland Webbhotell AB tjänster för webbserver och E-post. Den operativa driften styrs därför av Oderland och dess underleverantör. Denna bilaga är en beskrivning av hur säkerhetsåtgärder praktiskt implementeras för driften.

## Fysisk säkerhet

Data och infrastruktur är placerade i flera datacenter belägna i Sverige. Du kan därför vara försäkrad om att dina uppgifter kommer att stanna innanför Sveriges gränser. Datacenterleverantören är ansvarig för den fysiska miljön, exempelvis ström, kylning, brandsläckning och åtkomstkontroll, och för en strikt kontroll över att underleverantörer alltid efterlever de gällande säkerhetsreglerna på området.

Fysisk åtkomst till servrarna tilldelas endast anställda med arbetsrelaterade behov.

## Logiska åtkomster

Rättigheter tilldelas de anställda utifrån arbetsrelaterade behov, och endast särskilt utvalda kan få en privilegierad åtkomst till systemen.

## Nätverk

Höga segmenteringsnivåer används för datanätverk, så att risken för spridning av ett angrepp minimeras. Brandväggar inspekterar trafik till kundernas miljöer, och DDoS-skydd begränsar den påverkan som eventuella angrepp kan ha på servrarna. Avancerad nätverksinspektion upptäcker mönster och angreppsförsök från kända, skadliga ip-adresser och varnar den operativa avdelningen vid behov.

## Loggning

Alla åtkomster till lednings- och kundmiljöer loggas, och loggningen används bl.a. till felsökning och utredning av eventuella händelser.

## Sårbarhetshantering

Oderland ansvarar för att löpande övervaka huruvida nya sårbarheter kan uppstå i de system som drivs. En process finns för att bedöma och hantera nya sårbarheter, och det installeras korrigeringsfiler så fort som möjligt efter att de har publicerats.
Simply Brf ansvarar för att utföra sårbarhetshantering och uppdatering av den programvara/kod som vi installerar för att erbjuda dig tjänster.

## Övervakning

Övervakning sker av infrastruktur och relevanta tjänster dygnet runt. Till övervakningen finns det anslutet ett 24/7-vaktschema.

# Backup

Backupdata speglas mellan två fysiskt skilda platser i Sverige, så att det alltid finns en tillgänglig kopia i händelse av en kritisk krasch. Säkerhetskopior sparas i 12 månader.

**Backup av webbhotell inkl. e-post**
Backup genomförs dagligen, och denna lagras i allmänhet i 12 månader.

# Kryptering

Åtkomst till administrativa system / kontrollpaneler sker via krypterade TLS-anslutningar.

**Kryptering på webbhotell**

Hemsidor är generellt konfigurerade så att överföring sker krypterat till besökare via HTTPS.

**Kryptering av e-post**

Du måste aktivt välja att använda ett krypterat protokoll till överföring av e-post, eftersom e-postsystemen, för att stödja gamla e-post-program, också tillåter användning av icke-krypterade anslutningar.

**Kryptering av data**

Om nedladdad data (filer, dokument, osv.) ska lagras i krypterad form, ska du själv göra detta med hjälp av applikationer. Simply Brf lagrar data i krypterad form på sina arbets-stationer och exempelvis vid mellanlagring för flytt av e-post åt kund. Om du hanterar känsliga uppgifter på e-post, bör du åtminstone säkerställa att du använder en krypterad anslutning, när du får åtkomst till e-postsystemen.

# Underleverantörer

Om underleverantörerna kan påverka säker-hetsmiljön ansvara Oderland för att de upp-fyller uppställda krav. Detta görs via avtal, databehandlingsavtal, revisions- berättelser, egenkontroller och sekretessavtal. Löpande kontroller sker att underleverantörer uppfyller kraven.

# Beredskap

Beredskap handlar om att vara förberedd på händelser som kan ha en kritisk eller katastrofal påverkan på driften. Därför finns beredskapsplaner som fastställer förfaranden, rutiner och roller i händelse av en katastrof. Underleverantörernas anställda utbildas i beredskap flera gånger om året.

En del av beredskapen är också att vara förberedda om det skulle inträffa ett dataintrång. I det avseendet finns rutiner för att ge råd till kunder och relevanta myndigheter, i enlighet med vad som krävs enligt den nya Dataskyddsförordningen.

# Kundens ansvar

Simply Brf säkerställer säkerheten i sin del av leve-ransen, dvs. de it-system som används för webbho-tell- och e-posttjänster. Du som kund ansvarar själv för konfigurationer du gör på eget initiativ samt egna installationer, såvida inte Simply Brf uttryckligen bett dig göra
detta. Vi ansvara för att våra instruktioner är korrekta till dig som kund