Standardkontraktsbestemmelser/Underdatabehandleraftale

i henhold til artikel 28, stk. 3 og 4, i forordning 2016/679 (databeskyttelsesforordningen) med henblik på underdatabehandlerens behandling af personoplysninger

mellem

FirstAgenda
CVR 37098922
Mariane Thomsens Gade 4
8000 Aarhus C
Danmark

herefter ”databehandleren”

og

Ubivox Technologies ApS
CVR 27379494
Østre Stationsvej 43, 3. sal
5000 Odense C
Danmark

herefter ”underdatabehandleren”

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

1. Indhold

2. Præambel

1. Disse Bestemmelser fastsætter underdatabehandlerens rettigheder og forpligtelser, når denne foretager behandling af personoplysninger på vegne af databehandleren.

2. Disse bestemmelser er udformet med henblik på parternes efterlevelse af artikel 28, stk. 3, jf. artikel 28 stk. 4, 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 licens til underdatabehandlerens e-mail marketings- og automationsplatform behandler underdatabehandleren personoplysninger på vegne af databehandleren 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 databehandlerens betingelser for underdatabehandlerens brug af andre underdatabehandlere og en liste af andre underdatabehandlere, som databehandleren har godkendt brugen af.

8. Bilag C indeholder databehandlerens instruks for så vidt angår underdatabehandlerens behandling af personoplysninger, en beskrivelse af de sikkerhedsforanstaltninger, som underdatabehandleren som minimum skal gennemføre, og hvordan der føres tilsyn med underdatabehandleren og andre 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 underdatabehandleren fra forpligtelser, som underdatabehandleren er pålagt efter databeskyttelsesforordningen eller enhver anden lovgivning.

3. Databehandlerens rettigheder og forpligtelser

1. Databehandleren er ansvarlig for at sikre, at underdatabehandleren er pålagt samme databehandlingsforpligtigelser som databehandleren selv er pålagt i medfør af databehandleraftale indgået mellem den dataansvarlige og databehandleren, som regulere databehandlerens behandling af persondata på vegne af den dataansvarlige, jf. databeskyttelsesforordningens art. 28 stk. 3, samt databeskyttelsesforordningen (se

forordningens artikel 28), databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes[1] nationale ret og disse Bestemmelser.

2. Databehandleren skal sikre at underdatabehandleren har passende tekniske og organisatoriske foranstaltninger på en sådan måde, at behandlingen opfylder kravene i denne forordning og databehandleraftale indgået mellem den dataansvarlige og databehandleren.

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

4. Underdatabehandleren handler efter instruks

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

2. Som følge af at det er den dataansvarlige, der bestemmer til hvilke formål og med hvilke hjælpemidler, der må foretages behandling af de personoplysninger denne er dataansvarlig for, jf. databeskyttelsesforordningens art. 4, nr. 7, afspejler databehandlerens instruks den instruks databehandleren har fået i medfør af databehandleraftalen mellem den dataansvarlige og databehandleren, som regulere databehandlerens behandling af persondata på vegne af den dataansvarlige, jf. databeskyttelsesforordningens art. 28 stk. 3. Det er netop formålet med underdatabehandleraftalen, at underdatabehandleren pålægges samme forpligtigelser som databehandleren er pålagt efter databeskyttelsesforordningens art. 28, jf. databeskyttelsesforordningens art. 28 stk. 4.

3. Underdatabehandleren underretter omgående databehandleren, hvis en instruks efter vedkommendes mening er i strid med denne forordning eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.

5. Fortrolighed

1. Underdatabehandleren må kun give adgang til personoplysninger, som behandles på databehandlerens vegne, til personer, som er underlagt underdatabehandlerens 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.

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

2. Underdatabehandleren skal efter anmodning fra databehandleren kunne påvise, at de pågældende personer, som er underlagt underdatabehandlerens 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. Denne forpligtigelse pålægges underdatabehandleren i samme omfang som databehandleren selv i medfør af denne underdatabehandleraftale, som forskrevet i databeskyttelsesforordningens art. 28 stk. 4.

   Databehandleren 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. Underdatabehandleren skal på samme vis implementere passende foranstaltninger for at imødegå disse risici. Disse foranstaltninger er specificeret i Bilag C.

3. Derudover skal underdatabehandleren bistå databehandleren med vedkommendes bistand til den dataansvarliges overholdelse af den dataansvarliges forpligtelse efter forordningens artikel 32, ved bl.a. at stille den nødvendige information til rådighed for databehandleren vedrørende de tekniske og organisatoriske sikkerhedsforanstaltninger, som underdatabehandleren 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. Disse informationer stilles til rådighed for databehandleren, således at denne kan overbringe sådan til den dataansvarlige.

   Hvis imødegåelse af de identificerede risici kræver gennemførelse af yderligere foranstaltninger end de foranstaltninger, som underdatabehandleren allerede har gennemført, skal databehandleren angive de yderligere foranstaltninger, der skal gennemføres, i bilag C.

7. Anvendelse af andre underdatabehandlere

1. Underdatabehandleren 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 anden underdatabehandler).

2. Underdatabehandleren må således ikke gøre brug af en anden underdatabehandler til opfyldelse af disse Bestemmelser uden forudgående specifik skriftlig godkendelse fra databehandleren.

3. Underdatabehandleren må kun gøre brug af andre underdatabehandlere med databehandlerens forudgående specifikke skriftlige godkendelse. Underdatabehandleren skal indgive anmodningen om en specifik godkendelse 45 dage inden anvendelsen af den pågældende anden underdatabehandler. Listen over andre underdatabehandlere, som databehandlere allerede har godkendt, fremgår af bilag B.

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

   Underdatabehandleren er derfor ansvarlig for at kræve, at den anden underdatabehandler som minimum overholder underdatabehandlerens forpligtelser efter disse Bestemmelser og databeskyttelsesforordningen.

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

6. Underdatabehandleren skal i sin aftale med den anden underdatabehandler indføje databehandleren som begunstiget tredjemand i tilfælde af underdatabehandlerens konkurs, således at databehandleren kan indtræde i underdatabehandlerens rettigheder og gøre dem gældende over for de andre underdatabehandlere, som f.eks. gør databehandleren i stand til at instruere den anden underdatabehandler i at slette eller tilbagelevere personoplysningerne.

7. Hvis den anden underdatabehandler ikke opfylder sine databeskyttelsesforpligtelser, forbliver underdatabehandleren fuldt ansvarlig over for databehandleren for opfyldelsen af den anden underdatabehandlers 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 underdatabehandleren på baggrund af dokumenteret instruks herom fra databehandleren og skal altid ske i overensstemmelse med databeskyttelsesforordningens kapitel V.

2. Hvis overførsel af personoplysninger til tredjelande eller internationale organisationer, som underdatabehandleren ikke er blevet instrueret i at foretage af databehandleren, kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som underdatabehandleren er underlagt, skal underdatabehandleren underrette databehandleren 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 databehandleren kan underdatabehandleren 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 anden underdatabehandler i et tredjeland
    c. behandle personoplysningerne i et tredjeland

4. Databehandlerens 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.

9. Bistand til den dataansvarlige

1. Underdatabehandleren bistår, under hensyntagen til behandlingens karakter, så vidt muligt databehandleren 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 underdatabehandleren så vidt muligt skal bistå databehandleren i dennes bistand til 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 underdatabehandlerens forpligtelse til at bistå databehandlernes i dennes bistand til den dataansvarlige i henhold til Bestemmelse 6.3., bistår underdatabehandleren endvidere, under hensyntagen til behandlingens karakter og de oplysninger, der er tilgængelige for underdatabehandleren, databehandleren i dennes bistand til 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 underdatabehandleren skal bistå databehandleren 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. Underdatabehandleren underretter uden unødig forsinkelse databehandleren efter at være blevet opmærksom på, at der er sket et brud på persondatasikkerheden.

2. Underdatabehandlerens underretning til databehandleren skal om muligt ske senest 24 timer efter, at denne er blevet bekendt med bruddet, sådan at databehandleren kan underrette den dataansvarlige i tids nok til at denne 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 underdatabehandleren bistå databehandleren i dennes bistand til den dataansvarlige med at foretage anmeldelse af bruddet til den kompetente tilsynsmyndighed. Det betyder, at underdatabehandleren 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:

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 underdatabehandleren skal tilvejebringe i forbindelse med sin bistand til databehandleren som led i dennes 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 underdatabehandleren forpligtet til at tilbagelevere alle personoplysningerne og slette eksisterende kopier, medmindre EU-retten eller medlemsstaternes nationale ret foreskriver opbevaring af personoplysningerne.

12. Revision, herunder inspektion

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

2. Procedurerne for databehandlerens revisioner, herunder inspektioner, med underdatabehandleren og andre underdatabehandlere er nærmeret angivet i Bilag C.7. og C.8.

3. Underdatabehandleren 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 underdatabehandlerens 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.

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

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 databehandleren i overensstemmelse med Bestemmelse 11.1 og Bilag C.4, kan Bestemmelserne opsiges med skriftligt varsel af begge parter.

5. Underskrift

   På vegne af databehandleren

Navn	Kasper Lyhr
Stilling	CEO
Telefonnummer	
E-mail	
Underskrift	

   På vegne af underdatabehandleren

Navn	David McNally
Stilling	Administrerende direktør
Telefonnummer	+45 2594 4282
E-mail	dm@ubivox.com
Underskrift	

15. Kontaktpersoner hos den databehandleren og underdatabehandleren

1. Parterne kan kontakte hinanden via nedenstående kontaktpersoner.

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

   For databehandleren

Navn	Søren Skou
Stilling	Data Compliance Specialist
Telefonnummer	+45 29365164
E-mail	dataprivacy@firstagenda.com

   For underdatabehandleren

Navn	David McNally
Stilling	Administrerende direktør
Telefonnummer	+45 2594 4282
E-mail	dm@ubivox.com

Bilag A Oplysninger om behandlingen

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

Underdatabehandleren stiller en e-mail marketings- og automationsplatform til rådighed for databehandleren, som denne bl.a. kan benytte til udsendelse af nyhedsbreve og øvrige markedsføringshenvendelser og tiltag over for dennes kunder eller potentielle leads.

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

Underdatabehandlerens behandling af personoplysninger på vegne af databehandleren omfatter at underdatabehandleren stiller systemet Ubivox til rådighed for databehandleren og herigennem opbevarer stamdata for databehandleren på virksomhedens server.

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

Almindelige personoplysninger, jf. databeskyttelsesforordningens art. 6, herunder, men ikke begrænset til, navn, e-mailadresse, telefonnummer og oplysninger om permissions.

A.4. Behandlingen omfatter følgende kategorier af registrerede

- Administratorer
- brugere af Platformen FirstAgenda der er tilmeldt nyhedsbreve med produktopdateringer, feature releases mv.

”Person, som har eller har haft samhandel med databehandleren og/eller person, der har givet samtykke til modtagelse af e-mails fra databehandleren”

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

Behandlingen er ikke tidsbegrænset og varer indtil Underdatabehandleraftalen opsiges eller ophæves af en af Parterne.

Uanset Underdatabehandleraftalens formelle aftaleperiode, skal Underdatabehandleraftalen vedblive at gælde, så længe underdatabehandleren behandler personoplysninger for databehandleren.

Bilag B Andre underdatabehandlere

B.1. Godkendte underdatabehandlere

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af følgende underdatabehandlere

NAVN	CVR	ADRESSE	BESKRIVELSE AF BEHANDLING
LeaseWeb Netherlands B.V	NL812426939B01	Hessenbergweg 95 1101 CX Amsterdam	Hostingudbyder Ubivox oplyser, at selskabets hostingmiljø (fysiske hardware) befinder sig i Amsterdam hos hostingleverandøreren, LeaseWeb Netherlands B.V. Ubivox står inde for, at behandlingen hos LeaseWeb Netherlands B.V. sker i overensstemmelse med ovennævnte persondataretlige forskrifter. Ubivox' aftale med LeaseWeb Netherlands B.V. sikrer desuden, at data udelukkende opbevares og behandles indenfor grænserne af EU og det Europæiske Økonomiske Samarbejdsområde, samt at LeaseWeb Netherlands B.V. lever op til Databehandleraftalen.

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

Jf. 7.3

Bilag C Instruks vedrørende behandling af personoplysninger

C.1. Behandlingens genstand/instruks

Underdatabehandlerens behandling af personoplysninger på vegne af databehandleren sker ved, at databehandleren udfører følgende:

Ved tilmelding til nyhedsbrevet påbegynder Ubivox opbevaring af e-mailadresse, IP-adresse og eventuelle andre informationer Modtageren opgiver ved tilmelding. En bekræftelsesmail sendes til Modtageren, og når denne bekræftes, må Ubivox gemme dato, tid og IP-adresse som dokumentation af samtykke fra Modtageren. Disse oplysninger må gemmes indtil samtykket trækkes tilbage, hvorefter disse oplysninger samt andre informationer opgivet ved tilmeldingen skal slettes.

Ved modtagelse af nyhedsbreve påbegynder Ubivox opbevaring af statistiske data for modtageren, herunder åbning af nyhedsbrevet, klik på links, region hvor åbningen er sket, samt fysisk enhed hvorpå åbningen er sket. Disse data kan ikke knyttes til den enkelte modtager, men opbevares udelukkende statistisk, og slettes ikke hvis modtageren framelder sig.

Ved udsendelse af e-mails via Ubivox' SMTP-løsning påbegynder Ubivox opbevaring af Modtagerens e-mailadresse samt emnefeltet for e-mailen. Disse data slettes idet retten til at blive glemt bliver effektueret for Modtageren.

C.2. Behandlingssikkerhed

Sikkerhedsniveauet skal afspejle:

Eftersom underdatabehandlerens levering af e-mail marketings- og automationsplatformen muliggør, at underdatabehandleren kan uploade og på anden vis tilføje generelt personoplysninger, vil underdatabehandleren potentielt behandle en ukendt mængde af personoplysninger og ukendte kategorier af personoplysninger og datasubjekter.

Derfor har underdatabehandleren valgt at implementere et generelt sikkerhedsniveau afspejlende, at der kan ske behandling af en ukendt mængde personoplysninger og af alle former for kategorier af personoplysninger og datasubjekter.

Underdatabehandleren 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.

Underdatabehandleren skal dog – under alle omstændigheder og som minimum – gennemføre følgende foranstaltninger, som er aftalt med databehandleren:

Fysisk sikring og miljøsikring

Underdatabehandlerenen skal opretholde fysiske sikringsforanstaltninger til sikring af lokaliteter, som anvendes til behandling af personoplysninger, herunder opbevaring af personoplysninger omfattet af underdatabehandleraftalen mod uvedkommendes adgang og manipulation.

> Skal have passende tekniske foranstaltninger til at begrænse risikoen for enhver uautoriseret adgang til lokaler, hvor der behandles persondata. Underatabehandleren skal desuden, hvor det er nødvendigt, evaluere og forbedre effektiviteten af sådanne forholdsregler
>
> Sikrer at niveauet for den fysiske sikkerhed til enhver tid være er afstemt med det aktuelle

trusselbillede samt den følsomhed og mængde af persondata som underdatabehandleraftalen omfatter

Kommunikationsforbindelser og kryptering
Underdatabehandleren har passende tekniske foranstaltninger til at beskytte systemer og netværk, herunder beskytte data under transmission og adgang via internettet, samt til at begrænse risikoen for uautoriseret adgang og/eller installering af skadelig kode.

Underdatabehandleren anvender passende krypteringsteknologier og andre tilsvarende foranstaltninger i overensstemmelse med kravene i lovgivningen, godkendte standarder for kryptering af klassificeret information samt god databehandlingsskik.

I det omfang det er et krav i medfør af gældende national og international lovgivning, standarder vedrørende kryptering af klassificeret information eller god databehandlingsskik anvender databehandler krypteringsteknologier og andre tilsvarende foranstaltninger.

Transmission af følsomme og fortrolige oplysninger over internettet er beskyttet af kryptering. Teknologiske løsninger til kryptering er tilgængelige og aktiveret. Firewall tillader kun krypteret datatrafik. Der foreligger formaliserede procedurer, der sikrer, at transmission af følsomme og fortrolige oplysninger over internettet er beskyttet af stærk kryptering baseret på en anerkendt algoritme.

Firewall eller lignende tekniske foranstaltninger
Ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, alene sker gennem en VPN. Der skal foreligge administrativ adgang til at vedligeholde firewall-konfiguration og -regelsæt.

Antivirus
Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, installeret antivirus, som løbende opdateres

Sikkerhedskopiering
Underdatabehandler skal have interne beredskabsprocedurer, der sikrer genetablering af services uden ugrundet ophold i tilfælde af driftsafbrydelser i henhold til hovedaftalen. Underdatabehandleren sikrer daglig backup.

Sikkerhedskopiering af konfigurationsfiler og data skal finde sted hyppigt og som minimum fire gange ugentligt, således at relevant data kan reetableres. Sikkerhedskopierne opbevares således, at de ikke hændeligt eller ulovligt (eks. ved brand, oversvømmelse, uheld, tyveri eller lignende) tilintetgøres, fortabes, forringes, kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med de til enhver tid gældende regler og forskrifter for behandling af personoplysninger.
Sikkerhedskopierne skal opbevares fysisk adskilt fra primære data og i et sikkerhedsgodkendt datacenter.

Underdatabehandleren anvender redundant miljø til sikring af adgang og kontinuerlig drift af softwareløsningen. Sikrer at backup gemmes i sin fulde længde.

Anvendelse af hjemme/fjernarbejdspladser
Såfremt der foretages databehandling fra ad hoc og/eller hjemmearbejdspladser, sikrer underdatabehandleren at disse lever op til de sikkerhedsmæssige krav i denne underdatabehandleraftale med bilag og lovgivning i øvrigt.

Underdatabehandler skal blandt andet opfylde følgende:

- At deres anvendes krypteret forbindelse mellem ad hoc arbejdspladsen og underdatabehandlerens netværk
- Underdatabehandlerens har en intern instruks til egne medarbejdere vedrørende ad hoc og hjemmearbejdspladser

Derudover skal Underdatabehandleren, hvis det er teknisk muligt anvende 2-faktor-autentifikation.

Instruktion af medarbejdere

Underdatabehandleren sikrer at ansatte til stadighed er bekendt med og har tilstrækkelig uddannelse og instruktion om databehandlingens formål, politikker, arbejdsgange og om deres tavshedspligt.

Der foreligger en informationssikkerhedspolitik, som ledelsen har behandlet og godkendt inden for det seneste år. Informationssikkerhedspolitikken er kommunikeret til relevante interessenter, herunder databehandlerens medarbejdere.

Informationssikkerhedspolitikken generelt lever op til kravene om sikringsforanstaltninger og behandlingssikkerheden i indgåede databehandleraftaler.

Der foreligger formaliserede procedurer, der sikrer efterprøvning af underdatabehandlerens medarbejdere i forbindelse med ansættelse.

Nyansatte medarbejdere har underskrevet en fortrolighedsaftale. Nyansatte medarbejdere er blevet introduceret til:
- Informationssikkerhedspolitikken.
- Procedurer vedrørende databehandling, samt anden relevant information

Der foreligger procedurer, der sikrer, at fratrådte medarbejderes rettigheder inaktiveres eller ophører ved fratrædelse, og at aktiver som adgangskort, pc, mobiltelefon osv. Inddrages. Fratrådte medarbejderes rettigheder er inaktiveret eller ophørt, samt at aktiver er inddraget.

Der foreligger formaliserede procedurer, der sikrer, at fratrådte medarbejdere gøres opmærksom på opretholdelse af fortrolighedsaftalen og generel tavshedspligt. Ansættelseskontrakten indeholder retningslinjer for, at medarbejdere er underlagt tavshedspligt efter ophørt samarbejde.

Underdatabehandleren udbyder awareness-træning til medarbejderne omfattende generel it-sikkerhed og behandlingssikkerhed i relation til personoplysninger. Der foreligger dokumentation for, at alle medarbejdere, som enten har adgang til eller behandler personoplysninger, har gennemført den udbudte awareness-træning.

Logning

1. Sikrer logning på alle miljøer, hvor personoplysninger behandles.
2. Sikrer, at loggene som minimum skal indeholde oplysninger om
    a. Tidspunkt for adgang
    b. IP-adresse ved adgang
    c. Brugernavn
    d. Handlinger udført ved adgang

3. Sikrer, at sikkerhedsloggens omfang er defineret ud fra en af underdatabehandleren udført risikovurdering
4. Sikrer, at der er plads nok til at sikkerhedsloggene kan gemmes for perioden
5. Sikrer, at der gennemføres løbende stikprøvekontroller, af, at sikkerhedsloggene indeholder det forventede
6. Sikrer, at brugernes adgang blokeres for yderligere forsøg login, såfremt der inden for en fastsat periode er registreret højst 3 på hinanden følgende afviste adgangsforsøg fra samme arbejdsstation eller med samme brugeridentifikation.
7. Afvejer sikkerhedsloggens slettefrister imellem muligheden for at analysere cyberangreb, understøtte efterforskning og hensynet til beskyttelses af fysiske personers rettigheder og frihedsrettigheder.

Sikrer opsamlede oplysninger om brugeraktivitet i logs er beskyttet mod sletning og manipulation.

Bortskaffelse af udstyr
Underdatabehandleren skal have formelle processer med henblik på at sikre, at der sker en effektiv sletning af personoplysninger inden bortskaffelse af elektronisk udstyr.

Underdatabehandler sikrer herunder:

- benytter sikre forbindelser (HTTPS, SSH, VPN o.l.) til al online kommunikation så vidt muligt
- sikrer arbejdsstationer og enheder med adgangskoder og kryptering
- indfører log-in- og adgangskodeprocedurer for adgang til computere, platform m.v. sikrer, at alene medarbejdere med arbejdsrelaterede formål hertil har adgang til personoplysningerne
- sikrer, at bygninger og systemer, der anvendes i forbindelse med databehandlingen, er sikre, samt at der alene anvendes hardware og software af høj kvalitet, som opdateres løbende
- sikrer, at medarbejdere modtager passende uddannelse, fyldestgørende instruktioner i og retningslinjer for behandlingen af personoplysningerne. Ubivox er forpligtet til at sikre, at de medarbejdere, som er involveret i behandlingen af personoplysningerne, er bekendte med sikkerhedskravene.
- udformer nødvendig dokumentation og instruktion, herunder medarbejderhåndbog og beredskabsplan
- generelt bestræber sig på at indrette sikkerheden overensstemmelse med ISO27001 og ISO27002 (ligesom hos underdatabehandler)

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

Registreredes rettigheder, jf. pkt. 9.1.
• Databehandleren skal bistå med at iagttage de registreredes rettigheder ved bl.a. at kunne give indsigt i, slette, begrænse og berigtige oplysninger, og sørge for at dette også sker hos underdatabehandlerne.
• Databehandleren skal bistå med at opfylde de registreredes rettigheder uden unødig forsinkelse
• Databehandleren skal have udarbejdet en procedure for, hvordan de behandler anmodninger fra en registreret om deres rettigheder.

Brud og hændelser, jf. pkt. 9.2.
En underretning om brud og hændelser skal udfyldes mest muligt inden for fristen på 24 timer uden ekstra omkostninger. Efterfølgende informationer sendes straks.
Informationer som skal sendes:
• Fakta om det konstaterede brud (tid, sted, årsag)
• Hvornår bruddet startede, hvornår det blev opdaget og hvornår bruddet er standset
• Karakteren af bruddet på persondatasikkerheden, herunder om der er sket brud på fortrolighed, integritet og tilgængelighed
• Kategorierne og det omtrentlige antal berørte registrerede, hvis det er muligt
• Kategorierne af personoplysninger, hvis det er muligt.
• Navn og kontaktoplysninger til kontaktpunkt, hvor yderligere oplysninger kan indhentes
• Beskrivelse af de sandsynlige konsekvenser af bruddet
• Beskrivelse af foranstaltninger der er truffet, eller foreslås truffet som led i håndteringen af bruddet og dets mulige skadevirkninger

Databehandleren og dennes underdatabehandlere må hverken offentligt eller til tredjeparter kommunikere om sikkerhedsbrud uden forudgående skriftlig aftale med den Dataansvarlige om indholdet af en sådan kommunikation, medmindre Databehandleren er retligt forpligtet til sådan kommunikation.

C.4 Opbevaringsperiode/sletterutine
Personoplysninger opbevares i perioden for parternes aftale om underdatabehandlerens levering af e-mail marketings- og automationsplatform til databehandleren, eller i henhold til særskilt skriftlig aftale, hvorefter de slettes hos underdatabehandleren.

Ved ophør skal underdatabehandleren således enten slette eller tilbagelevere personoplysningerne i overensstemmelse med bestemmelse 11.1, medmindre databehandleren – efter underskriften af disse bestemmelser – har ændret databehandlerens 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 følgende:

Underdatabehandlerens hjemsted eller indenfor EU/EØS. Disse lokaliteter skal oplyses på bilag B.

C.6 Instruks vedrørende overførsel af personoplysninger til tredjelande
Hverken databehandleren eller underdatabehandlere må overføre personoplysninger til tredjelande. Dette inkluderer også at databehandleren og underdatabehandleren ikke må lade en af deres afdelinger, som er placeret i et tredjeland behandle personoplysninger.

Såfremt underdatabehandleren ønsker at overføre personoplysninger til tredjelande, så skal underdatabehandleren kontakte FirstAgenda dataprivacy@firstagenda.com.

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

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

Underdatabehandleren udfører årligt en intern revision af forhold defineret i underdatabehandleraftalen, herunder kontrol af intern dokumentation, kontrol af logging og sikkerhedsopdateringer i softwaren leveret af underdatabehandleren, kontrol af firewall, backups m.v., kontrol af fysiske lokationer, kontrol af medarbejderdokumentation m.v. Denne revision fremsendes efter ønske til Databehandleren.

Baseret på resultaterne af den interne revision er databehandleren 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.

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, men dog minimum med 28 dages varsel.

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

Underdatabehandleren skal årligt for egen regning indhente en revisorerklæring fra en uafhængig tredjepart eller en kontrolrapport vedrørende de anvendte underdatabehandlers overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.

Dokumentation for sådanne inspektioner fremsendes efter ønske til databehandleren til orientering.

Bilag D Parternes regulering af andre forhold

D.1. Misligholdelse og tvistigheder

Misligholdelse og tvistigheder er reguleret i Hovedaftalen. I tilfælde af, at Hovedaftalen ikke tager stilling hertil, skal gældende rets almindelige misligholdelsesbeføjelser finde anvendelse på Aftalen.

Regulering af tvistløsning, inklusive lovvalg og værneting, i Hovedaftalen finder også anvendelse for Aftalen, som om Aftalen var en integreret del heraf. I tilfælde af at Hovedaftalen ikke tager stilling hertil skal nedenstående bestemmelser finde anvendelse på Aftalen.

Aftalen er underlagt dansk ret med undtagelse af:

a) Regler der fører til anvendelse af anden lov end dansk lov samt
b) FN-Konventionen om internationale løsørekøb (CISG)

Opstår der uoverensstemmelser i forbindelse med Aftalen eller dens gennemførelse, skal parterne med en positiv, samarbejdende og ansvarlig holdning søge at indlede forhandlinger med en mediator med henblik på at løse tvisten. Om nødvendigt skal forhandlingerne søges løftet op på direktionsniveau i parternes organisationer.

Kan parterne ikke opnå en løsning ved forhandling, er parterne berettiget til at kræve tvisten afgjort endeligt ved retssag ved de almindelige domstole. Retten i Esbjerg er valgt som værneting. Retsplejelovens henvisningsregler til Landsret og Sø- og Handelsret skal dog fortsat finde anvendelse.

Såfremt den Dataansvarlige ikke mener, at en af Databehandleren udpeget Underdatabehandler lever op til et eller flere af de ovennævnte krav under punkt (7), vil det blive betragtet som væsentlig misligholdelse. Inden væsentlig misligholdelse gøres gældende skal den Dataansvarlige underrette sin Databehandler om forholdet og give en passende frist til at udbedre misligholdelsen.

Som udgangspunkt betragtes det som væsentlig misligholdelse, såfremt Databehandleren ikke overholder forpligtelserne i Databehandleraftalen, den til enhver tid gældende lovgivning vedrørende databeskyttelse samt kravene i de dokumenter, der udgør bilag til Databehandleraftalen.

D.2. Erstatning og forsikring

Erstatnings- og forsikringsspørgsmål er reguleret i Hovedaftalen. I tilfælde, at Hovedaftalen ikke tager stilling hertil, er Databehandleren erstatningsansvarlig i overensstemmelse med dansk rets almindelige regler i tilfælde af misligholdelse af Databehandleraftalen. Såfremt den Dataansvarlige af tredjemand gøres erstatningsansvarlig for Databehandlerens og/eller eventuelle Underdatabehandleres manglende overholdelse af Databehandleraftalen, herunder Databehandleraftalens bilag, og/eller overtrædelse af gældende lovgivning vedrørende databeskyttelse, skal Databehandleren holde den Dataansvarlige skadesløs for alle omkostninger, gebyrer, erstatningsbeløb, udgifter eller tab, som den Dataansvarlige har afholdt eller pådraget sig som følge heraf.