Databehandleraftale

Standardkontraktsbestemmelser

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

mellem

Køber

herefter "den dataansvarlige"

og

Auxo ApS
CVR. 3487 7939
Lillebæltsvej 62
6715 Esbjerg N
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

1. Indhold

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 ar-tikel 28, stk. 3, i Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med be-handling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (databeskyttelsesforordningen).

3. I forbindelse med leveringen af udarbejdede hjemmesider, webshopsystem, hosting og support af hjemmeside/webshop (Webløsningen), samt markeds-føringsydelser såsom Google Ads (herunder Google Analytics og Agency Analytics), SoMe annoncer på platforme såsom Facebook og Instagram (herunder Meta Pixel) og LinkedIn, og øvrige markedsføringsprodukter, her-under Search Engine Optimization (SEO) på Google, Bing mv., 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 underdata-behandlere.

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 persono-lysninger 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 person-oplysninger, men instruksen skal altid være dokumenteret og opbevares skriftligt, herunder elektronisk, sammen med disse Bestemmelser.Den dataansvarlige har ret og pligt til at træffe beslutninger om, til hvilke(t) formål og med hvilke hjælpemidler, der må ske behandling af persono-plys-ninger.
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.

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 personoplysnin-gerne 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.

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

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. pseudonymusering 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 nød-vendige 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 idatabeskyttelsesforordningens 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 14 dages varsel og derved give den dataansvarlige mulighed for at gøre indsigelse 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. 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.

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 databeskyttelses-forordningens 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. nderretningspligten 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 behadlingens 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 24 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:

   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. navn og kontaktoplysninger for databeskyttelsesrådgiveren eller et andet kontaktpunkt, hvor yderligere oplysninger kan indhentes
   c.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 tilbagelevere alle personoplysningerne og slette eksisterende kopier, medmindre EU-retten eller medlemsstaternes nationale ret foreskriver opbevaring af personoplysningerne.

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 nærmere 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.

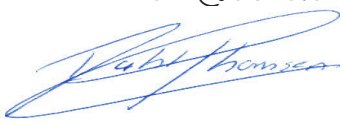
13. Parternes aftale om andre forhold

1. Parterne kan aftale andre bestemmelser vedrørende tjenesten om 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 den dataansvarlige i overensstemmelse med Bestemmelse 11.1 og Bilag C.4, kan Bestemmelserne opsiges med skriftligt varsel af begge parter.
5. Underskrift
   På vegne af den dataansvarlige:
   Ved sin accept af Parternes Aftale om køb af ydelser accepterer den dataansvarlige samtidig nærværende databehandleraftale i sin helhed.
   På vegne af databehandleren:

Navn	Casper Thomsen
Stilling	CFO
Telefonnummer	+45 70 40 40 50
E-mail	cth@auxo.dk
Undersk	



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.

Kontaktperson ved databehandleren:

Navn	Casper Thomsen
Stilling	CFO
Telefonnummer	+45 70 40 40 50
E-mail	cth@auxo.dk

Kontaktperson ved den dataansvarlige:

Navn	Se Købers Intranet-profil
Stilling	Ejer/kontaktperson
Telefonnummer	Se Købers Intranet-profil
E-mail	Se Købers Intranet-profil

Bilag A Oplysninger om behandlingen

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

Formålet med behandlingen er databehandlerens levering af kontraktmæssige ydelser til den dataansvarlige, herunder hosting og support af hjemmeside/webshop, samt markedsføring af den dataansvarlige ved hjælp af Google Ads og Google Analytics, Google My Business inkl. Maps, SoMe annoncer på Facebook/Instagram, Linkedin og Search Engine Opti-mization (SEO) på Google, Bing mv.

A.2. Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige drejer sig primært om opbevaring og organisering/formidling

Databehandlingen indebærer primært, at databehandleren i egenskab af sin rolle som udvikler af hjemmesider/webshops og efterfølgende hosting af samme, opbevarer og har adgang til at se og tilgå de af den dataansvarlige indsamlede personoplysninger om de registrerede/tredjemand, som behandles af den dataansvarlige på dennes hjemmeside/webshop. Databehandleren tilgår og behandler udelukkende hostede personoplysninger i den dataansvarliges systemer og behandler således aldrig personoplysningerne i sine egne systemer.

Databehandlingen omfatter yderligere indsamling og behandling af førstepartscookies og andre cookies, annoncerings-ID'er og regionsoplysninger baseret på IP-adresser, baseret på den besøgendes samtykke, i forbindelse med visse markedsføringsydelser:

1) SEO, herunder Google My Business inkl. Maps og Agency Analytics.

2) Google Ads indsamler førstepartscookies og annoncerings-ID'er der videresendes til Google Analytics med henblik på generering af rapporter til den dataansvarlige ved hjælp af databehandlerens brug af Agency Analytics.

3) Facebook/Instagram annoncering indsamler oplysninger om brugeradfærd, bruger-ID og enhedsoplysninger m.fl. via Meta Pixel som behandles af databehandleren.

Alle personoplysninger behandles i overensstemmelse med den dataansvarliges instrukser herom og vil aldrig blive behandlet med henblik på et andet formål end dét, som oplysningerne blev indsamlet med henblik på.

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

Almindelige personoplysninger om tredjemand, herunder den dataansvarliges kunder, brugere, leverandører, samarbejdspartnere og alle øvrige personoplysninger der indsamles af den dataansvarlige via dennes hjemmeside eller webshop og derved hostes af databehandleren i henhold til Parternes aftale. Dette kan omfatte navn, adresse, arbejdsplads, stillingsbetegnelse, e-mailadresse, telefonnummer, fødselsdato, betalingskortsoplysninger, medlemsnummer og type af medlemskab.

I forbindelse med databehandlerens levering af markedsføringsydelser til den dataansvarlige, herunder SEO, Google My Business og Maps, samt Google Ads, kan der blive indsamlet personoplysninger i form af IP-adresse og cookies (medmindre iubenda eller andet cookie-modul anvendes).

A.4. Behandlingen omfatter følgende kategorier af registrerede

- Kunder/besøgende på den dataansvarliges hjemmeside/webshop, herunder kunder, medlemmer, leverandører, samarbejdspartnere og andre øvrige interessenter såsom besøgende fra annoncering på eksempelvis Google Ads, SoMe annoncer og lignende.
- Ansatte hos den dataansvarlige i det omfang disse fremgår af den dataansvarliges hjemmeside

Bilag B Underdatabehandlere

B.1. Godkendte underdatabehandlere

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af følgende underdatabehandlere

Navn	CVR	ADRESSE	BESKRIVELSE AF BEHANDLING
Curanet A/S (en del af team.blue Denmark A/S)	29412006	Højvangen 4, 8660 Skanderborg, Danmark	a) Hosting af servers via VM's b) Domain Name Services (DNS-server) c) Tivoli Storage Manager (backup) d) Backup af visse af Auxos webhoteller **e)** HostedShop - webshopløsning for visse kundesegmenter
AzeHosting ApS	36974796	Hornevej 7, 2770 Kastrup, Danmark	a) Hosting af hjemmesider for visse kundesegmenter på servere i Tyskland
Amazon Web Services EMEA SARL (AWS)	Intet dansk CVR-nr.	38 Avenue John F. Kennedy, L-1855, Luxembourg	a) **Løbende backups af hjemmesider**
Microsoft Ireland Opera-tions, Ltd.	13612870	One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Ireland	a) Hosting af dataansvarliges Mi-crosoft Outlook mailløsning via Microsoft 365, der kan indeholde personoplysninger om tredjemand
Google Ireland Ltd. og/eller Google International LLC	Intet dansk CVR-nr.	Google Building Gordon House, Barrow St, Grand Canal Dock, Dublin 4, D04 V4X7, Irland + C/O Corporation Service Company, 251 Little Falls Drive, Wilmington, DE 19808, USA	a) Google Analytics behandler førstepartscookies når den dataansvarlige har valgt Google markedsføringsydelser såsom Google Ads og den dataansvarlige ikke benytter iubenda. Der behandles også annoncerings-id´er. b) Google Re-CAPTCHA behandler nødvendige cookies med henblik på at minimere SPAM c) Google My Business (herun-der Google Maps) indsamler oplysninger via cookies, IP-adresser/regioner samt browserrelateret data
Agency Analytics	Intet dansk CVR-nr.	134 Peter Street, Suite 1302, Toronto, Ontario, Canada, M5V 2H2	a) generering af rapporter til den dataansvarlige baseret på oplysninger (cookies) fra Google Analytics
iubenda s.r.l,	Intet dansk CVR-nr.	Via San Raffaele, 1 - 20121 Milan (Italia)	a) Cookie-modul til indhentning af den besøgendes samtykke til cookies

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

Ved databehandlerens planlagte ændringer vedrørende tilføjelse- eller udskiftning af underdatabehandlere underrettes den dataansvarlige skriftligt herom mindst 14 dage før den planlagte ændrings ikrafttræden.

Såfremt den dataansvarlige ikke gør indsigelse mod de planlagte ændringer inden udløb af 14 dages fristen, vil dennes tavshed blive anset for accept af de planlagte ændringer.

Såfremt den dataansvarlige gør indsigelse mod de planlagte ændringer inden udløb af 14 dages fristen, kan den dataansvarlige opsige sin aftale om Ydelsen med virkning fra tidspunktet for de planlagte ændringer. Sådan opsigelse skal være kommet frem til databehandleren inden de planlagte ændringers ikrafttrædelsestidspunkt.

Se i sin helhed Databehandleraftalens Bestemmelse 7 om underdatabehandlere, navnlig Bestemmelse 7.3

Auxo ApS
Lillebæltsvej 62,
6715 Esbjerg N
tlf: +45 82 82 98 98
info@auxo.dk
cvr: 34877939

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:

Databehandleren vil i forbindelse med sin udarbejdelse af hjemmeside og/eller webshop og ved sin efterfølgende hosting og support heraf, behandle personoplysninger på vegne af den dataansvarlige, enten selv eller ved brug af andre databehandlere (underdatabehandlere).

Det drejer sig primært om opbevaring af personoplysninger om tredjemand indsamlet af den dataansvarlige via dennes hjemmeside eller webshop.

I det omfang den dataansvarlige har købt markedsføringsydelser såsom Google Ads og SEO vil der blive indsamlet oplysninger i form af cookies, medmindre iubenda eller tilsvarende cookiemodul anvendes, samt IP-adresse, med henblik på generering af en månedlig rapport via Agency Analytics til brug for den dataansvarlige.

Endelig behandler databehandleren personoplysninger på vegne af den dataansvarlige når sidstnævnte har en Microsoft 365 mailløsning via databehandleren.

C.2. Behandlingssikkerhed

Sikkerhedsniveauet skal afspejle:

Behandlingen omfatter almindelige personoplysninger (i modsætning til særlige kategorier af personoplysninger, jf. forordningens artikel 9) om tredjemand, som databehandleren behandler på vegne af den dataansvarlige, hvorfor der skal etableres et almindeligt 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:

1. Sikring af vedvarende fortrolighed af behandlingssystemer og -tjenester:
    - Databehandleren sikrer, at det kun er relevante medarbejdere, der har adgang til personoplysninger til det aftalte formål (adgang efter behov), og at disse personer er underlagt et krav om fortrolighed og er bekendt med, hvordan personoplysninger behandles på en sikker måde. Databehandleren må og vil aldrig videregive eller offentliggøre nogen af de personoplysninger, som databehandleren bliver be-kendt med i forbindelse med arbejdet for den dataansvarlige.
    - Databehandleren anvender sit eget udviklede system (Kaldet Jytte) til at sikre vedvarende fortrolighed til sine hostede hjemmesi-der/webshops via opdatering af alle hjemmesider/webshops med de seneste sikkerhedsopdateringer, nødvendige plugins og lignende. Alene ansatte der har behov for adgangen til systemet er tildelt bru-gernavn og password dertil. Systemet er ikke tilgængeligt uden for databehandlerens lokaliteter eller via databehandlerens VPN. Udstyr udleveret til medarbejdere må ikke anvendes på offentlige netværk og er ligeledes sikret med brugernavn og password.

2. Sikring af vedvarende fortrolighed af oplysninger under transmission og opbevaring - kryptering af personoplysninger:
    - Databehandleren sikrer, at al transmission af personoplysninger via netværk og internettet som minimum krypteres i transportlaget. Alle websites har et SSL-certifikat hvilket betyder, at data krypteres via TLS.
    - Databehandleren sikrer, at adgang til oplysninger via internettet sker med VPN-forbindelse, individuelle adgangskoder eller elektronisk signatur.
    - Databehandleren sikrer en sikker overførelse af personoplysninger mellem databehandleren og den dataansvarlige samt til tredjeparter, der optræder som underdatabehandlere, ved udelukkende at bruge krypterede overførelsesprotokoller, som eksempelvis HTTPS eller SSL.
3. Sikring af vedvarende integritet af behandlingssystemer og tjenester
    - Databehandleren sikrer via elektronisk signatur, individuelle fortrolige adgangskoder og VPN-forbindelser, samt multifaktor godkendelse eller single sign on hvor det er muligt, at gemte data i systemet forbliver uændret, medmindre det er hensigten at ændre dem.
4. Sikring af vedvarende tilgængelighed af behandlingssystemer og tjenester:
    - Databehandleren har til hver en tid en funktionel backup på op til 6 måneders data afhængig af hvilket kundesegment den dataansvarlige tilhører hos databehandleren.
    - Databehandleren eller dennes underdatabehandler kan lægge backup af en hel server eller af en specifik hjemmeside op på en anden server inden for ca. 30 minutter.
    - Databehandleren kan yderligere lægge den dataansvarliges egne backup(s) op på en server inden for ca. 15 minutter.
    - Databehandleren opbevarer den dataansvarliges data på plesk servere, der muliggør backup af hele serveren på ca. 30 minutter.
5. Sikring af vedvarende robusthed af behandlingssystemer og tjenester:
    - Databehandleren sikrer imod skadelige hændelser blandt andet via aftale med underdatabehandlere der, så vidt muligt, lever op til anerkendte sikkerhedsstandarder eller tilsvarende interne retningslinjer:
        - Curanet A/S som er ISO/IEC 27001-certificeret, herunder i relation til udfald ved dublerede diske, køling, nødstrømsanlæg automatisk brandslukning mv.
        - Google Ireland Limited og Google International LLC er ISO/IEC 27001 certificeret vedrørende deres Google Analy-tics sporing. Certificeret under EU-U.S. Data Privacy Framework til at modtage personoplysninger.
        - Amazon Web Services EMEA SARL er ISO/IEC 27001-certificeret.
        - AzeHosting ApS' datacenter er ISO/IEC 27001-certificeret.
        - Microsoft Ireland Operations, Ltd. er ISO/IEC 27001-certificeret. Certificeret under EU-U.S. Data Privacy Framework til at modtage personoplysninger.
        - AgencyAnalytics er vurderet som havende et passende beskyttelsesniveau, jf. EU Kommissionens tilstrækkelighedsafgørelse for Canada.
        - Iubenda s.r.l. er ISO/IEC 27001:2017 certificeret.

6. Procedure for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerheden:

    - Databehandleren systematiserer gentagne og periodiske procedurer vedrørende scanning, identifikation og afhjælpning af hidtil ukendte sikkerhedsproblemer på servere, arbejdsstationer, netværker, udstyr og applikationer.
    - Der bliver løbende opdateret software, core mv. på serverne af databehandleren og/eller dennes underdatabehandlere.
    - Der opdateres endvidere packages, firewall- og sikkerhedspatches ugentligt. Dette udføres af den IT-ansvarlige hos databehandleren.

7. Procedurer for beskyttelse af oplysninger under opbevaring:

    - Databehandleren opbevarer al data på egen server in house, på virtuelle servere, i et eksternt datacenter eller i et anerkendt cloudmiljø. Al data opbevares indenfor EU og er sikret bag standard firewalls. Databehandleren foretager nødvendig og løbende patching af server og søger at sikre best practice for så vidt angår sikkerhed og adgangsstyring.

8. Procedure for anvendelse af hjemme-/fjernarbejdspladser:

    - Der arbejdes som udgangspunkt fra databehandlerens fysiske lokaliteter, jf. punkt 10 nedenfor. Fjernarbejde er alene tilladt efter aftale og arbejdsbetinget behov. Ved fjernarbejde kan der alene oprettes forbindelse via enten VPN eller anden sikkerheds protokol for netværksforbindelse og alene via dertil udleverede computere.

9. Procedure for logning:

    - Databehandleren giver kun autoriserede personer adgang til personoplysninger via konti, der kan spores ved navn og som ved brug bliver tilstrækkeligt logget. Databehandleren fører altid log over de personer, der har været logget på.

10. Fysisk sikring af lokaliteter:

    - Databehandlerens fysiske lokalitet i 6715 Esbjerg N har elektronisk alarm med tilkaldevagt hos Fog El & Alarm. Der er alene adgang til lokaliteten med udleveret kode, der alene er udleveret til CEO, COO, CFO og øvrige ledende ansatte der til dagligt åbner og lukker for lo-kaliteten. Serverrummet er i samme bygning bag en dør sikret med kodelås. Bærbare computere tages med hjem af den enkelte ansatte og er sikret med brugernavne og passwords. Stationære computere er tilsvarende sikret med brugernavn og password.
    - Databehandlerens fysiske lokalitet i 8000 Aarhus C har sikringsniveau S20 hos Falck/Verisure. Der er alene adgang til lokaliteten med to personligt udleverede nøgler, nøglebrikker eller lignende, hvor brugen logges og hvor brug af den enkelte nøgle kan spærres. Bær-bare computere låses dagligt inde i et særskilt rum med røgkanon, som er aflåst med kodelås og metaldør, hvis de efterlades på kontoret. Alle computere har brugernavn og password.
    - Databehandlerens fysiske lokalitet i 5230 Odense M har elektronisk alarm hos El-Team Sikring. Alarmen aktiveres/deaktiveres via en unik kode som kontoransvarlig besidder. Kontoret befinder sig på 6. sal, hvilket gør at man skal igennem 3 låste døre for at nå lokaliteten. Der er alene adgang til lokaliteten med de ansattes unikke nøglebrikker. Bærbare computere er låst med brugernavn og password.

- Databehandlerens lokalitet i 2860 Søborg er ikke i brug pr. dags dato og medarbejderne arbejder, indtil anden lokalitet er sikret, udelukkende hjemmefra hvor de logger på databehandlerens system via VPN og eget brugernavn og kode.
- Databehandlerens fysiske lokalitet i 9400 Nørresundby har G4S alarmselskab tilknyttet. Alle ansatte har egen nøglebrik med unik kode der skal indtastes for at slå alarmen fra og til. Bærbare computere tages enten med hjem af den enkelte ansatte eller efterlades på dennes plads på kontoret – dette afhænger af hvordan dagens møder er booket. Alle computere har individuelle koder. Når computere efterlades på kontoret natten over (og generelt når kontoret er tomt) er døren dertil låst med kode. På lokaliteten befinder sig også telefoner, iPads mm. til, eksempelvis, fremvisning af referencer til Kunder. Disse er låst med password eller nøglekode.

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:

Hvis den dataansvarlige modtager en anmodning fra en registreret person vedrørende udøvelsen af sine rettigheder som fastlagt i databeskyttelsesforordningens kapitel III, vil databehandleren, under hensyntagen til behandlingens karakter, så vidt muligt, bistå den dataansvarlige med besvarelsen heraf, snarest muligt efter databehandleren oplyses om anmodningen af den dataansvarlige.

Hvis databehandleren modtager en sådan anmodning fra en registreret person direkte, uden om den dataansvarlige, meddeler databehandleren den dataansvarlige herom snarest muligt. Databehandleren vil i den forbindelse oplyse den dataansvarlige om al relevant information om anmodningen. Databehandleren bistår i den forbindelse den dataansvarlige med besvarelsen heraf, men vil ikke på eget initiativ besvare anmodningen medmin-dre skriftlig tilladelse hertil gives af den dataansvarlige.

Databehandleren vil underrette den dataansvarlige om ethvert brud på persondatasikkerheden. Underretning vil uden unødig forsinkelse og uden hensyntagen til databehandlerens egen vurdering af, hvorvidt bruddet usandsynligvis vil indebære en risiko for de registreredes rettigheder eller frihedsrettigheder, eller hvorvidt den dataansvarlige af databehandleren med føje må formodes at være bekendt med bruddet.

Straks efter databehandleren opdager et brud på persondatasikkerheden, træffer denne de nødvendige foranstaltninger for at begrænse de negative konsekvenser heraf og fremtidige identiske brud på persondatasikkerheden.

Databehandleren har ikke den dataansvarliges bemyndigelse til at anmelde brud på persondatasikkerheden til Datatilsynet.

Den dataansvarlige er ansvarlig for at anmelde brud på persondatasikkerheden til Datatilsynet i overensstemmelse med databeskyttelsesforordningens artikel 33.

Det samme gælder for underretning til den registrerede om brud på persondatasikkerheden i overensstemmelse med artikel 34.

C.4 Opbevaringsperiode/sletterutine

Personoplysninger behandles, i det omfang det er muligt, i den dataansvarliges systemer i overensstemmelse med denne aftales Bestemmelser herom. Ved hjemmeside og web-

shop har den dataansvarlige eksempelvis eget login til CMS'et, som databehandleren har adgang til i aftaleperioden for at kunne yde support til den dataansvarlige. Er det ikke muligt at behandle personoplysningerne i den dataansvarliges systemer, foretages behandlingen i databehandlerens systemer.

Ved ophør af Parternes aftale om hjemmeside/webshop, hosting og support og/eller markedsføringsydelser, skal databehandleren tilbagelevere adgangen til den dataansvarliges systemer i overensstemmelse med Bestemmelse 11.

Databehandleren gemmer ikke adgangsoplysninger til den dataansvarliges systemer efter aftalens ophør. Eventuelle personoplysninger der er blevet lagret lokalt hos databehandleren under behandlingen af personoplysninger på vegne af den dataansvarlige slettes så snart formålet med lagringen er udtømt.

Databehandleren har ikke adgang til oplysningerne hostet af databehandlerens underleverandører.

Google Analytics indsamler personoplysninger i form af cookies, medmindre den dataansvarlige benytter et cookiemodul såsom iubenda, hvor der i så fald ikke indsamles personoplysninger med den konsekvens, at der ikke kan genereres månedsrapporter via Agency Analytics. I det omfang den dataansvarlige ikke benytter et cookiemodul, gemmes oplysningerne af Google Analytics som udgangspunkt i 14 måneder – dette kan ændres i indstillingerne for Google Analytics.

Alle personoplysninger i form af cookies opbevares under hele den dataansvarliges SEO-ydelse/aftale med databehandleren, for at kunne dokumentere udviklingen i resultatet af SEO-forløbet. Efter aftalen om SEO er ophørt slettes personoplysningerne straks.

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:

Behandlingen foretages af Auxo ApS som databehandler på følgende adresser:

a. Lillebæltsvej 62, 6715 Esbjerg N, DK
b. ægergårdsgade 118, 8000 Aarhus C, DK
c. Tagholm 15, 9400 Nørresundby, DK
d. Cortex Park 12, 6. sal, 5230 Odense M, DK

Samt af de i Bilag B oplistede underdatabehandlere på disses respektive adresser. Alle underdatabehandlere befinder sig inden for den Europæiske Union (EU), er en del af EØS-samarbejdet eller omfattet af Kommissionens afgørelser om, at de på-gældende underdatabehandlere har sikret et tilstrækkeligt beskyttelsesniveau komparativt til EU's GDPR-beskyttelse, herunder Canada og Amerikanske virksomheder omfattet af EU-U.S. Data Privacy Framework'et.

C.6 Instruks vedrørende overførsel af personoplysninger til tredjelande

Databehandleren eller dennes underdatabehandlere overfører på tidspunktet for udarbejdelsen af nærværende databehandleraftale alene personoplysninger til tredjelandene USA og Canada.

a. Microsoft 365, herunder Microsoft Outlook, anvendes af databehandleren til at tilbyde mailløsning til den dataansvarlige. Den dataansvarliges mails hostes af Microsoft Ireland Operations, Ltd., baseret i Irland, og foretager som udgangspunkt ikke overførsel af personoplysninger til USA. Hvis den dataansvarlige aktiverer funktionerne "Sway" eller "Workplace Analytics" vil der blive overført personoplysninger til Microsoft Corporations servere i USA.

    a. Microsoft Corporation er certificeret under EU-U.S. Data Privacy Framework, jf. forordningens art. 45, stk. 3, jf. stk. 1.

b. Google Ads og Google Analytics anvendes af databehandleren til at indsamle oplysninger om EU-borgere på servers inden for EU, navnlig ved Google Ireland Ltd. Herefter kan oplysningerne blive videresendt til Google International LLC's Google Analytics-servere i USA med henblik på anden behandling.

    a. Google International LLC er certificeret under EU-U.S. Data Privacy Framework, jf. forordningens art. 45, stk. 3, jf. stk. 1.

c. Meta Pixel, ejet af Meta Platforms Ireland Limited, baseret i Irland, anvendes af databehandleren til at indsamle cookies og web-beacons med henblik på optimering af den dataansvarliges Facebook og/eller Instagram annoncering. Oplysningerne kan helt eller delvist blive sendt til Meta Platforms, Inc.' servere i USA.

    a. Meta Platforms, Inc. er certificeret under EU-U.S. Data Privacy Framework, jf. forordningens art. 45, stk. 3, jf. stk. 1.

Certificeringerne for Microsoft Corporation, Google International LLC og Meta Platforms, Inc. kan findes på https://www.dataprivacyframework.gov/list og anses derfor af Kommissionen som havende et tilstrækkeligt beskyttelsesniveau.

d. AgencyAnalytics, baseret i Canada, anvendes af databehandleren til at ge-nerere rapporter til den dataansvarlige om resultaterne af Google Ads baseret på oplysningerne hentet fra Google Analytics. I forbindelse med denne behandling overføres oplysninger til AgencyAnalytics' servere i Canada.

Canada er ved en såkaldt tilstrækkelighedsafgørelse fra Kommissionen blevet klassificeret som et tredjeland, der har et tilstrækkeligt beskyttelsesniveau sammenligneligt med- eller tæt EU's persondatabeskyttelse, herunder databeskyttelsesforordningen m.fl.

Alle øvrige underdatabehandlere oplistet i Bilag B befinder sig inden for EU/EØS.

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

Databehandleren stiller alle oplysninger til rådighed for den dataansvarlige som er nødvendige for at påvise overholdelse af kravene i databehandleraftalen, databeskyttelsesforordningen, databeskyttelsesloven og anden relevant EU- eller national lovgivning.

Databehandleren står til rådighed for den dataansvarlige til at besvare dennes spørgsmål vedrørende databehandlingen.

Databehandleren giver den dataansvarlige mulighed for at bidrage til revisioner, herunder (sikkerheds)revisionserklæringer, der udarbejdes af den dataansvarlige eller en anden revisor, som er bemyndiget hertil af den dataansvarlige. Revisionserklæring kan udarbejdes efter anmodning herom fra den dataansvarlige til databehandleren for den dataansvarliges regning.

Såfremt den dataansvarlige ønsker at få udarbejdet en sikkerhedsrevisionserklæring er parterne enige om, at følgende type kan anvendes:

Uafhængig revisors ISAE 3000-erklæring type 1 – GDPR-erklæring med begrænset sikkerhed.

Revisionserklæringen fremsendes uden unødig forsinkelse til den dataansvarlige til orientering. Baseret på resultaterne af erklæringen, i det omfang disse viser en mangel på sikkerhedsforanstaltninger, er den dataansvarlige berettiget til at anmode om gennemførelse af yderligere foranstaltninger med henblik på at sikre overholdelsen af databeskyttelses-forordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes natio-nale ret og disse Bestemmelser.

Den dataansvarlige har herudover adgang til at foretage inspektioner, herunder fysiske inspektioner, med databehandlerens lokaliteter, herunder fysiske lokaliteter og systemer, der benyttes til eller i forbindelse med behandlingen. Sådanne inspektioner kan gennemføres hvis den dataansvarlige finder det nødvendigt, dog skal databehandleren varsles minimum 30 dage forinden.

Den dataansvarliges eventuelle udgifter i forbindelse med en fysisk inspektion afholdes af den dataansvarlige selv. Databehandleren afsætter de ressourcer (hovedsageligt den tid), der er nødvendig for, at den dataansvarlige kan gennemføre sin inspektion.

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

Databehandleren stiller alle oplysninger til rådighed for den dataansvarlige som er nødven-dige for at påvise overholdelse af kravene i databehandleraftalen, databeskyttelsesforord-ningen, databeskyttelsesloven og anden relevant EU- eller national lovgivning.

På den dataansvarliges anmodning til databehandleren kan denne få udleveret kopi af underdatabehandleres sikkerhedsrevisionserklæring(er), i det omfang underdatabehandler-en har udarbejdet sådan, eller kopi af databehandleraftalen som beskriver sikkerhedsfor-holdene hos underdatabehandlerne som sikrer, at de overholder kravene i databehandler-aftalen, databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.

Databehandleren fører yderligere løbende selvstændigt tilsyn med, hvordan underdatabe-handlerne behandler personoplysninger og om databeskyttelsesforordningen, databeskyt-telsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestem-melser:

a. Revisionserklæringer ISAE 3000 (og ISAE 3402 Type 2) fra Curanet A/S kan findes på www.curanet.dk/om-os/compliance.

b. For Amazon Web Services EMEA SARL ("AWS Europe") vedkommende kan deres pri-vatlivspolitik, herunder behandling af data i henhold til GDPR, findes på https://aws.amazon.com/privacy/#EU-US_Data_Privacy_Framework.2C_UK_Extension.2C_and_Swiss-US_Data_Privacy_Framework ved at klikke på "European Economic Area, UK, and Switzerland".

c. AzeHosting ApS er ISO-27001 certificeret og databehandleraftale kan findes på https://azehosting.net/terms.php

d. For Microsoft Ireland Operations, Ltd.'s vedkommende kan deres databeskyttelse-spolitik og databehandleraftale findes på henholdsvis https://learn.microsoft.com/en-us/compliance/regulatory/gdpr og https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA.

e. For Google Ireland Ltd. og/eller Google International LLC's vedkommende kan deres databeskyttelsespolitik og databehandleraftale for Google Ads m.fl. findes på https://business.safety.google/gdpr/ og https://business.safety.google/adsprocessorterms/

f. For AgencyAnalytics' vedkommende kan deres databehandleraftale findes på https://agencyanalytics.com/company/data-processing-agreement.

g. For Iubenda s.r.l.'s vedkommende kan deres databehandleraftale findes på https://www.iubenda.com/vilkar-og-betingelser/99765740.

Databehandleren vurderer årligt (dog tidligst efter 2 år), om der er behov for et fysisk tilsyn vedrørende overholdelsen af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og af denne databehandleraftale hos underdatabehandlerne.

Bilag D

Parternes regulering af andre forhold

Ikke relevant.