Changelog

VERSION	ÆNDRINGER
1.1	Ændringer i Bestemmelserne 7.7., 9.2., 10.4. og Bilag C.8. *(Tastefejl og opdaterede krydshenvisninger).*
1.2	Tilpasset MCB kunder
1.3	Præcisering af B2 - varsling via e-mail
1.4	Opdatering af Bilag B - opdelt efter leverance platform. Raptor Services er tilføjer som underdatabehandler til platformen MCB.Cloud.
1.5	Opdatering til Bilag B - Heroku er indført som UDB for Hubspot og Shopify - CloudFactory indført som UDB for Umbraco og MCB.Cloud
1.6	Opdatering til Bilag B - ActiveCampaign indført som Underdatabehandler - Redigerbare felter indført i Bilag A til indførelse af systemer, som aftalen er gældende for.
1.7	Fjernet dublet data og stavefejl
1.8	Opdateret Bilag C med flere præciseringer - C2 - C3 - C6 - C7
1.9	Ændring til databehandler - MCB.Cloud hosting overgår 100% til DLX A/S fra Lynero. Se bilag B.

Standardkontraktsbestemmelser

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

mellem

Navn:	Navn: MCB A/S
CVR-nr:	CVR-nr: 29150966
Adresse:	Adresse: Lægaardsvej 86B
Postnr.: By:	Postnr.: 7500 By: Holstebro
Land:	Land: Danmark
"Dataansvarlige"	**"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.

Indhold

1. Præambel

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

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

3. I forbindelse med leveringen af drift, udvikling og rådgivning af webløsninger og relaterede produkter, behandler databehandleren personoplysninger på vegne af den dataansvarlige i overensstemmelse med disse Bestemmelser.

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

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

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

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

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

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

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

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

2. Den dataansvarliges rettigheder og forpligtelser

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

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

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

3. Databehandleren handler efter instruks

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

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

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

4. Fortrolighed

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

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

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

5. Behandlingssikkerhed

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

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

   a. Pseudonymisering og kryptering af personoplysninger.

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

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

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

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

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

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

6. Anvendelse af underdatabehandlere

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

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

3. Databehandleren har den dataansvarliges generelle godkendelse til brug af underdatabehandlere. Databehandleren skal skriftligt underrette den dataansvarlige om eventuelle planlagte ændringer vedrørende tilføjelse eller udskiftning af underdatabehandlere med mindst 1 måneds 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. Databehandleren skal i sin aftale med underdatabehandleren indføje den dataansvarlige som begunstiget tredjemand i tilfælde af databehandlerens konkurs, således at den dataansvarlige kan indtræde i databehandlerens rettigheder og gøre dem gældende over for underdatabehandlere, som f.eks. gør den dataansvarlige i stand til at instruere underdatabehandleren i at slette eller tilbagelevere personoplysningerne.

7. Hvis underdatabehandleren ikke opfylder sine databeskyttelsesforpligtelser, forbliver databehandleren fuldt ansvarlig over for den dataansvarlige for opfyldelsen af underdatabehandlerens forpligtelser. Dette påvirker ikke de registreredes rettigheder, der følger

   af databeskyttelsesforordningen, herunder særligt forordningens artikel 79 og 82, over for den dataansvarlige og databehandleren, herunder underdatabehandleren.

7. 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.

8. Bistand til den dataansvarlige

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

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

    a. oplysningspligten ved indsamling af personoplysninger hos den registrerede
    b. oplysningspligten, hvis personoplysninger ikke er indsamlet hos den registrerede
    c. indsigtsretten
    d. retten til berigtigelse
    e. retten til sletning ("retten til at blive glemt")
    f. retten til begrænsning af behandling

g. underretningspligten i forbindelse med berigtigelse eller sletning af personoplysninger eller begrænsning af behandling
h. retten til dataportabilitet
i. retten til indsigelse
j. retten til ikke at være genstand for en afgørelse, der alene er baseret på automatisk behandling, herunder profilering

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

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

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

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

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

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

9. 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 60 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. 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.

10. Sletning og returnering af oplysninger

1. Ved ophør af tjenesterne vedrørende behandling af personoplysninger, er databehandleren forpligtet til at enten at slette alle personoplysninger, der er blevet behandlet på vegne af den dataansvarlige og bekræfte over for den dataansvarlig, at oplysningerne er slettet. Eller alternativt at tilbagelevere alle personoplysningerne og slette eksisterende kopier, medmindre EU-retten eller medlemsstaternes nationale ret foreskriver opbevaring af personoplysningerne.

11. Revision, herunder inspektion

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

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

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

12. 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.

13. 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 skriftlig varsel af begge parter.

5. Underskrift

På vegne af den dataansvarlige	**På vegne af databehandleren**
Navn:	Navn: Bo Hedegaard Rasmussen
Stilling:	Stilling: Direktør
Telefon:	Telefon: 4082 5863
Email:	E-mail: bhk@mcb.dk
_____	_____
Underskrift	Underskrift

14. 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.

Navn:	Navn: Jesper Navntoft Pedersen
Stilling:	Stilling: Afdelingsleder
Telefon:	Telefon: 2222 0432
Email:	E-mail: jnp@mcb.dk

Bilag A: Oplysninger om behandlingen

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

Dataansvarlig modtager assistance til drift, hosting og udvikling af web relaterede services og digital marketing.

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

Databehandler vil have adgang til personoplysninger i de systemer som der er givet adgange til af dataansvarlig

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

A.4. Behandlingen omfatter følgende kategorier af registrerede

A.5 Behandlinger er begrænset til følgende systemer

A.6. Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige kan påbegyndes efter disse Bestemmelsers ikrafttræden. Behandlingen har følgende varighed

Behandlingen sker så længe den Dataansvarlige har samarbejde med Databehandleren, dvs. indtil den Dataansvarlige opsiger aftalen med Databehandleren.

Bilag B: Underdatabehandlere

B.1. Godkendte underdatabehandlere

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af følgende underdatabehandlere

MCB.Cloud og Education

NAVN	CVR	ADRESSE	BESKRIVELSE AF BEHANDLING
DLX A/S	28692986	Hammerhusvej 16C 7400 Herning +45 7025 2728 Support@dlx.dk	For MCB.Cloud kunder Underdatabehandler leverer og drifter den fysiske infrastruktur for det virtuelle hostingmiljø på, hvor den Dataansvarliges it-system afvikles, herunder servere, netværk, storagesystem, firewall, internetforbindelse, strømforsyninger, brandslukningsudstyr og køling. Endvidere leveres backup af data.
John Nielsen		Calle Sierra Guadalupe 14 30163 Esparragal, Murcia. Spanien	Bistår med udvikling og serverdrift.
MCB LT		Laisvės g. 14, 89223 Mažeikiai, Lithuania	MCB LT bistår med udvikling
Raptor	DK35055975	Åboulevarden 37, 4. 8000 Aarhus C	Profilering og anbefaling af produkter. For MCB.Cloud kunder, som benyttet personalisering i platformen, er opfattet af at MCB benytter Raptor som underdatabehandler til denne ydelse.
CloudFactory	DK35393692	Vestergade 4 6800 Varde	Håndterer forbindelse til MS Azure. Services benyttes til generativ AI af artikler og produkter.

Magento, Wordpress, WooCommerce (PHP)

NAVN	CVR	ADRESSE	BESKRIVELSE AF BEHANDLING
MCB Vietnam		5th floor, No. 58, Alley 221 Ton Duc Thang Str., Dong Da Hanoi, Vietnam contact@mcb.vn	MCB Vietnam bistår med udvikling jf. SCC – se pkt. C6.
Powerhosting ApS	33055048	Dalgasgade 11 7400 Herning	For Magento platform kunder Underdatabehandler leverer og drifter den fysiske infrastruktur for det virtuelle hostingmiljø på, hvor den Dataansvarliges it-system afvikles, herunder servere, netværk, storagesystem, firewall, internetforbindelse, strømforsyninger, brandslukningsudstyr og køling. Endvidere leveres backup af data.

Umbraco

NAVN	CVR	ADRESSE	BESKRIVELSE AF BEHANDLING
MCB LT		Laisvės g. 14, 89223 Mažeikiai, Lithuania	MCB LT bistår med udvikling
CloudFactory	35393692	Vestergade 4 6800 Varde	Håndterer forbindelse til MS Azure. Hosting af webløsninger

Shopify

NAVN	CVR	ADRESSE	BESKRIVELSE AF BEHANDLING
MCB Vietnam		5th floor, No. 58, Alley 221 Ton Duc Thang Str., Dong Da Hanoi, Vietnam contact@mcb.vn	MCB Vietnam bistår med udvikling jf. SCC – se pkt. C6.
Heroku		Salesforce UK Limited, Floor 26 Salesforce Tower, 110 Bishopsgate, London, EC2N 4AY, United Kingdom,	Cloud hosting af services og apps til shopify kunder.

Hubspot

NAVN	CVR	ADRESSE	BESKRIVELSE AF BEHANDLING
Heroku		Salesforce UK Limited, Floor 26 Salesforce Tower, 110 Bishopsgate, London, EC2N 4AY, United Kingdom,	Cloud hosting af services og apps til shopify kunder.

Digital Marketing

NAVN	CVR	ADRESSE	BESKRIVELSE AF BEHANDLING
ActiveCampaign		ActiveCampaign, LLC 1 North Dearborn Street 5 th Floor Chicago, IL 60602 USA	For MCB Marketings kunder, som har MCB som Service Provider. e-mail marketing tool, som benyttes til udsendelse af nyheds og reklame e-mail til kunder der har givet samtykke.

Det pålægger kundens ansvar at have databehandleraftaler med de 3´th parts produkter og services som benyttes til marketing.

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

1. Ibrugtagning af ny underdatabehandler
   MCB skal orientere de dataansvarlige ved indgåelse af aftale med ny underdatabehandler, som får adgang til databehandlernes system og data.
   Varsling foretages til den e-mail, som er registreret ved MCB´s bogholderi som fakturamodtager.

2. Ændring til databehandler:
   MCBs underdatabehandler er generelt godkendte, og ændring til underdatabehandler, som ikke direkte har påvirker kontrakter, eller de aftalte leverance områder, må foretages uden notification til dataansvarlige.

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:

Databehandler rådgiver om systemer der indeholder persondata, udveksler data mellem systemer der indeholder persondata, Opbevarer (hosting og Backup) data der indeholder persondata, udvikler systemer der indeholder persondata.

C.2. Behandlingssikkerhed

Behandlingen omfatter personfølsomme data og dermed særlige kategorier af personoplysninger, jf. Databeskyttelsesforordningens art. 9. Dette betyder at skal etableres et højt sikkerhedsniveau omkring behandlingen.

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. Fastlæggelse af sikkerhedsniveau
   Procedure for GDPR-sikkerhedshændelser: Databehandleren skal som følge af GDPR-sikkerhedshændelser eller andre identificerede forhold, der truer sikkerheden, iværksætte foranstaltninger, der nedsætter eller eliminerer konsekvenserne af de uhensigtsmæssige forhold. I øvrigt skal den dataansvarlige orienteres herom. Der skal desuden foreligge fastlagte procedurer for håndtering af GDPR-sikkerhedshændelser, som sikrer, at der hurtigt bliver grebet ind og fulgt op på disse, samt at den dataansvarlige bliver orienteret jf. databehandleraftalens punkt 9.2.

2. Processer og beredskab
   Databehandleren har processer og et beredskab, som sikrer at driften af et system genoptages i tilfælde af et nedbrud. Databehandleren skal kunne genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse. For sikring af databehandlerens evnen til at genoprette tilgængeligheden af og adgangen til data rettidigt, i tilfælde af en fysisk eller teknisk hændelse, implementerer databehandleren backups, generatorer og redundante værktøjer. Databehandleren skal ligeledes have procedurer for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed. Herunder skal databehandleren sikre, at alle systemer og enheder sikkerheds opdateres jævnligt for at lukke eventuelle sikkerhedshuller.

3. Autorisation og adgangskontrol
   Fysisk adgangskontrol til Databehandlerens lokaler.

4. Personal med adgang til personoplysninger
   Det er er kun udvalgte medarbejdere, som må have adgang til de personoplysninger, som Databehandleren behandler på vegne af den Dataansvarlige. Medarbejdere med adgang til persondata skal autoriseres via en beskrevet godkendelsesprocedure og adgang skal ske via

Active Directory. Databehandleren skal mindst én gang årligt gennemføre et årligt review, som sikrer at det fortsat kun er autoriserede personsoner hos Databehandleren, som har adgang til personoplysningerne.

5. Fortrolighed
   Medarbejdere med adgang til den Dataansvarliges personoplysninger skal have underskrevet en fortrolighedserklæring

6. Kryptering
   At Databehandlerens generelle sikkerhedssetup skal sikre en sikkerhedsmæssig forsvarlig behandling af personoplysninger både fra arbejdspladsen og fra distancen (opkobling til webkontorer fra en hvilken som helst pc med internetadgang) – herunder i form af kryptering af data. Ovenstående foregår gennem en vpn-forbindelse. Dertil skal personoplysninger under transmission krypteres på transportlageret (TLS), hvilket som minimum skal ske ved at bruge version 1.2 eller højere.

7. Firewalls og antivirus
   Databehandleren sørger for, at alle arbejdsmaskiner og servere er udstyret med antivirussoftware med henblik på at blokere vira, malware m.v. Netværket er placeret bag firewalls inkl. DNS-filter for at kunne beskytte netværket mod uautoriseret adgang. Dertil skal det sikres, at alle systemer opdateres løbende og ligeledes jævnligt scannes for eventuelle sårbarheder.

8. Fysisk sikring af lokaliteter, hvor der behandles personoplysninger
   Databehandleren skal sikre fysisk sikring af lokaliteter, hvor der behandles personoplysninger, hvorfor beskyttelsen også skal afspejle fysisk beskyttelse mod risiko for brand, storm, vandskade og andre forhold, som kan bringe personoplysningerne i fare, ødelægge data eller komme i uvedkommendes varetægt. Det skal således sikres, at når udstyr og mobile enheder ikke anvendes, skal udstyret og enhederne være låst med adgangskode og/eller være låst inde. Kontorer og bygninger skal være aflåst, når de forlades.

9. Patch Management
   Databehandleren er forpligtet til løbende og inden for rimelig tid at anvende værktøjer til sårbarhedsscanninger og derefter sikkerhedsopdatere alle enheder og systemer, hvorfra der tilgås personoplysninger.

10. Awareness træning
    Databehandleren sikrer sig, at alle ansatte er instrueret i relevante regler om navnlig informationssikkerhed og databeskyttelse. Databehandleren skal derudover sikre sig, at alle ansatte løbende modtager awareness-træning om datasikkerhed og derigennem får viden om, hvordan de generelt skal forholde sig til behandling af personoplysninger, samt de databeskyttelsesmæssige risici forbundet hermed.

11. 2-faktor godkendelse
    Databehandleren indfører 2-faktor godkendelse på alle medarbejdernes computere. Databehandleren indfører ligeledes 2-faktor godkendelse på systemet.

12. Overførsel/transmission af personoplysninger
    Transmission af personoplysninger skal ske under passende sikkerhedsforanstaltninger. Dvs. at personoplysningerne skal beskyttes under selve transmissionen. Det kunne f.eks. være i form af kryptering, opsætning af firewalls eller lignende. Krav til opbevaring af personoplysninger
    Personoplysningerne skal opbevares inden for EU og under passende sikkerhedsforanstaltninger. Passende sikkerhedsforanstaltninger kunne f.eks. være opsættelse af firewalls, kryptering eller lignende.

13. Hjemmearbejdsplads / Remote arbejde
    Hjemmearbejdspladser skal være beskyttet på tilsvarende måde som arbejdspladser i databehandlingsfaciliteterne. I tilfælde, hvor en medarbejder gør brug af hjemme-/fjernarbejdspladser, må computere og andre enheder aldrig forlades uden at være låst eller slukket. Der skal være indført 2-faktor-validering for at sikre uvedkommende ikke kan få adgang til personoplysninger. Adgang til virksomhedens netværksressourcer, herunder også adgang til systemer, skal ske via VPN.

14. Logning
    Databehandleren skal føre logning i henhold til de krav der tidligere fulgte af sikkerhedsbekendtgørelsen, dvs. logningen skal mindst indeholde oplysning om tidspunkt, bruger, typer af anvendelse og angivelse af den person de anvende oplysninger vedrørte eller det anvendte søgekriterium (Sikkerhedsbekendtgørelsens § 19, stk. 1).

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 tekniske og organisatoriske foranstaltninger i overensstemmelse med Bilag C, Afsnit C.2. ovenfor

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

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

Kunden har ret til på et hvilket som helst tidspunkt i perioden, hvor leveranceaftalen gælder at få udleveret al data, der er en del af aftalen og som tilhører den dataansvarlige. De pågældende data og informationer skal udleveres efter den dataansvarliges nærmere rimelige anvisning. Databehandleren skal sikre, at værktøjer til at foretage dataudtræk er tilgængelige, så databehandleren kan udlevere data til den dataansvarlige.

Udlevering af data skal ske direkte til den dataansvarlige eller en af den dataansvarlige udpeget tredjemand. Data bliver opbevaret i 2 x 90 dage (6 MD) som udgangspunkt, såfremt andet ikke er aftalt med den dataansvarlige, eller at den dataansvarligere har givet instruks til sletning før denne dato.

Såfremt databehandleren inden udløbet af denne periode vil slette data, skal den dataansvarlige forinden skriftligt orienteres og gives et rimeligt varsel til enten selv at få etableret en backup eller anmode om opbevaring hos databehandleren.

C.4 Opbevaringsperiode/sletterutine

Personoplysninger opbevares så længe det er nødvendigt, hvilket normalt vil perioden hvori aftalen løber med den Dataansvarlige, hvorefter personoplysningerne slettes hos Databehandleren.

Data slettes 90 dage efter ophør af samhandel, og kan findes på backup i yderligere 90 dage.

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 på MCB's adresse Læggaarvej 86, 7500 Holstebro, eller hos Bilag B1 nævnte underdatabehandlere.

C.6 Instruks vedrørende overførsel af personoplysninger til tredjelande
Den Dataansvarlige har givet generelt samtykke til, at Databehandleren og dennes underleverandører kan overføre personoplysninger til tredjelande i det omfang, Europa-Kommissionen har fastslået, at det pågældende tredjeland, område i et tredjeland, en sektor i et tredjeland eller en international organisation beliggende i et tredjeland er sikkert, og dermed har et beskyttelsesniveau, som i det væsentlige svarer til det beskyttelsesniveau, der gælder i EU. Endvidere betyder det, at den Dataansvarlige ligeledes har godkendt, at Databehandleren eller dennes underleverandører kan overføre personoplysninger til organisationer i tredjelande, som er under EU's Standard Contractual Clauses (SCC).

Ved anvendelse af Europa-Kommissionens standardbestemmelser om databeskyttelse (SCC) som grundlag for overførsel af personoplysninger udenfor EU/EØS, er databehandleren forpligtiget til at implementere og overgå til de nye standardbestemmelser pr. 27. december 2022. Databehandleren forpligter sig endvidere til at udarbejde Transfer Impact Assessment (TIA) for de overførsler af personoplysninger, som sker til usikre tredjelande med henblik på at afgøre, om behandlingen kan ske i overensstemmelse med reglerne for tredjelandsoverførsler.

Såfremt den Dataansvarlige ikke i dette afsnit eller ved en efterfølgende skriftlig meddelelse har angivet en instruks eller godkendelse vedrørende overførsel af personoplysninger til et tredjeland, må Databehandleren ikke inden for rammerne af Databehandleraftalen foretage en sådan overførsel.

Der er tekniske tiltag som forhindrer adgang til personfølsom data uden for EU.

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

Der er enighed mellem parterne om, at følgende typer af revisionserklæringer kan anvendes i overensstemmelse med en revisionserklæring:

- ISAE 3000
- ISAE 3402
- ISO 27001/2
- ISO 27701
- SOC2

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

Den dataansvarlige eller en repræsentant for den dataansvarlige kan ved henvendelse gennemføre en fysisk inspektion af lokaliteterne, hvorfra databehandleren foretager behandling af personoplysninger, herunder fysiske lokaliteter og systemer, der benyttes til eller i forbindelse med behandlingen,

med henblik på at fastslå databehandlerens overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.

Ud over det planlagte tilsyn, kan den dataansvarlige gennemføre en inspektion hos databehandleren, når den dataansvarlige finder det nødvendigt.

Den dataansvarliges eventuelle udgifter i forbindelse med en fysisk inspektion afholdes af den dataansvarlige selv på T&M basis. Databehandleren er dog forpligtet til at afsætte de ressourcer (hovedsageligt den tid), der er nødvendig(e) for, at den dataansvarlige kan gennemføre sin inspektion.

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

Databehandleren eller en repræsentant for Databehandleren kan én gang årligt foretage et fysisk tilsyn vedrørende overholdelsen af denne databehandleraftale hos underdatabehandleren.
Udover dette årlige tilsyn, kan der føres tilsyn med underdatabehandleren, når der efter Databehandlerens (eller den Dataansvarliges) rimelige vurdering opstår et behov herfor.
Dokumentation for de afholdte tilsyn sendes snarest muligt til orientering hos den Dataansvarlige.

Der er enighed mellem parterne om, at følgende typer af revisionserklæringer kan anvendes i overensstemmelse med en revisionserklæring:

- ISAE 3000
- ISAE 3402
- ISO 27001/2
- ISO 27701
- SOC2

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

Den Dataansvarlige kan – hvis det findes nødvendigt – vælge at initiere og deltage på en fysisk inspektion hos underdatabehandleren. Dette kan dog alene blive aktuelt, såfremt den Dataansvarlige dokumenterer, at Databehandlerens tilsyn med underdatabehandleren ikke har givet den Dataansvarlige tilstrækkelig sikkerhed for, at behandlingen hos underdatabehandleren sker i overensstemmelse med denne databehandleraftale.

Databehandlerens og underdatabehandleres eventuelle udgifter i forbindelse med afholdelse af et fysisk tilsyn/en inspektion hos underdatabehandleren er den Dataansvarlige uvedkommende.

Bilag D: Parternes regulering af andre forhold