

## Standardkontraktbestemmelser

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

mellem

KUNDEN

herefter "den dataansvarlige"

og

**Heyloyalty**

CVR 29394458

Jens Baggesens Vej 47 8200 Aarhus N

Danmark

herefter "databehandleren"

der hver især er en "part" og sammen udgør "parterne"

HAR AFTALT følgende standardkontraktbestemmelser (Bestemmelserne) med henblik på at overholde databeskyttelsesforordningen og sikre beskyttelse af privatlivets fred og fysiske personers grundlæggende rettigheder og frihedsrettigheder

<b>1. Indhold</b>	
2. Præambel .....	3
3. Den dataansvarliges rettigheder og forpligtelser .....	3
4. Databehandleren handler efter instruks .....	3
5. Fortrolighed .....	4
6. Behandlingssikkerhed .....	4
7. Anvendelse af underdatabehandlere.....	5
8. Overførsel til tredjelande eller internationale organisationer .....	5
9. Bistand til den dataansvarlige.....	6
10. Underretning om brud på persondatasikkerheden .....	7
11. Sletning og returnering af oplysninger.....	7
12. Parternes aftale om andre forhold .....	8
13. Ikrafttræden og ophør.....	8
14. Kontaktpersoner hos den dataansvarlige og databehandleren .....	8
Bilag A Oplysninger om behandlingen.....	9
Bilag B Underdatabehandlere.....	10
Bilag C Instruks vedrørende behandling af personoplysninger.....	11
Bilag D Parternes regulering af andre forhold .....	14

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 Marketing automation 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 er 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 personoplysninger sker i overensstemmelse med databeskyttelsesforordningen (se forordningens artikel 24), databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes<sup>1</sup> 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

---

<sup>1</sup> Henvvisninger til "medlemsstat" i disse bestemmelser skal forstås som en henvielse til "EØS medlemsstater".

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.

## 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 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.

## 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. 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.

## 7. 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 30 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. Databehandleren skal i sin aftale med underdatabehandleren indføre 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.

## 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 standardkontraktbestemmelser 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 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. indsigtretten
  - 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 unødigt 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 unødigt 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 unødigt 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. 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 slette alle personoplysninger, der er blevet behandlet på vegne af den dataansvarlige og bekræfte over for den dataansvarlige, at oplysningerne er slettet, 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. Procedurene 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 lovgivning 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

Side 8 af 14

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 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

Navn  
Telefonnummer  
E-mail  
Underskrift

På vegne af databehandleren

Navn	Nicolaj Balle Ladiges
Stilling	Adm. direktør
Telefonnummer	26 85 34 14
E-mail	nl@heyloyalty.com
Underskrift	

### 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.

Navn  
Telefonnummer  
E-mail

Navn	Niels Mørk
Telefonnummer	42 54 56 57
E-mail	gdpa@arnsbogroup.com



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

Indsamling og opbevaring af datasubjektets (herefter kontakten) data og dennes interesser, for herigennem at personliggøre og udsende nyhedsbreve via SMS, mails eller andre elektroniske kanaler, indeholdende kontakten data og målrettet dennes interesser.

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

- Udvikling og support af Heyloyalty systemet, som er et kampagne- og automation-værktøj til e-commerce.
- Databehandleren stiller Heyloyalty systemet til rådighed for den dataansvarlige. Heri opbevares den dataansvarliges kontaktlister.
- Heyloyalty systemet afsender på vegne af den dataansvarlige nyhedsbreve/emails til den dataansvarliges registrerede modtagere – samt yder support herpå.
- Levering af support og konsulenttydelser.
- Ved tilkøb af Heycommerce licens, indsamles der adfærdsbaseret informationer om kontakten på kundens hjemmeside/webshop med henblik på i højere grad at skræddersy nyhedsbreve og lave individuelt tilpassede kampagner. Adfærden indbefatter desuden "tabt kurv", dvs. når kundens kontakt lægger ting i kurven med henblik på at købe, men ikke gennemfører købet, samt hvilke produkter og produktkategorier kundens kontakt søger og/eller klikker på.
- Ved tilkøb af Heypush modulet, indsamles der informationer om kontakten adfærd på kundens hjemmeside med henblik på afsendelse af webpush beskeder (denne service benytter Webpush)
- Ved tilkøb af Heypush modulet, er der mulighed for at parre eventuelt per mission til webpush, med den eksisterende kontakt på listen via Heyloyalty Heycommerce tracking Script.

Sammensætningen af kundens valg af Heyloyalty ydelser og dermed karakteren af behandlingen, fremgår altid på kundens Heyloyalty konto under "Integration" og "Listeintegrationer".

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

Typen af data der behandles, vil være af betegnelsen "almindelige artikel 6 oplysninger", som modtageren afgiver ved tilmelding til nyhedsbrevs-, eller ved senere opdatering af egne data. Eksempelvis

- Kontakten for- og efternavn
- Kontakten e-mailadresse og mobilnummer
- Kontakten interesser og præferencer
- Køn
- Fødselsdato
- Adresse
- Postnummer, by og land
- Reference (tilmeldingsoprindelse)

Den indsamlede data vil fremgå af den dataansvarliges Heyloyalty konto, på kontaktlisterne og den dataansvarliges Heycommerce database (hvis tilkøbt).

Den dataansvarlige har mulighed for at anmode kontakten om yderligere oplysninger (via den dataansvarliges egne definerede felter), herunder evt. følsomme personoplysninger ved tilmelding eller senere opdatering. Databehandleren skal informeres og forberedes af den dataansvarlige med et passende varsel, hvis den dataansvarlige ønsker at Heyloyalty behandler følsomme personoplysninger.

**A.4. Behandlingen omfatter følgende kategorier af registrerede**

Kontakter som har eller har haft tilmeldt sig en kontakliste hos den dataansvarlige og dermed har afgivet samtykke til modtagelse af direkte markedsføring.

**A.5. Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige kan påbegyndes efter disse Bestemmelser i krafttræden. Behandlingen har følgende varighed**

Behandlingen af personoplysninger er ikke tidsbegrænset og varer indtil samarbejdsaftalen ophører.

## Bilag B Underdatabehandlere

### B.1. Godkendte underdatabehandlere

Ved Bestemmelsernes i krafttræden har den dataansvarlige godkendt brugen af følgende underdatabehandlere

NAVN	CVR	ADRESSE	BESKRIVELSE AF BEHANDLING
Team.Blue Denmark A/S	29412006	Højvangen 4, 8660 Skanderborg	Hosting af data
Ubivox Technologies ApS	27379494	Østre Stationsvej 43, 3., 5000 Odense C	E-mail tjenester
InMobile	31426472	Axel Kiers Vej 18L, 8270 Højbjerg Danmark	SMS tjenester
Analysér Software A/S	32443591	Refshalevej 147 1432 København K	Survey værktøj
Gateway API	27364276	Onlinicity.IO.ApS Buchwaldsgade 50 5000 Odense C	SMS tjenester

Ved Bestemmelsernes i krafttræden 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

Intet yderligere

**C.1. Behandlingens genstand/instruks**

Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige sker ved, at databehandleren udfører følgende:

Databehandling sker til opfyldelse af samarbejdsaftalen mellem parterne, samt levering af de ydelser som den dataansvarlige har tilkøbt fra Heyloyalty og som fremgår af den dataansvarliges Heyloyalty konto, jf. nærmere herom i afsnit A2: karakteren af behandlingen.

**C.2. Behandlingssikkerhed**

Sikkerhedsniveauet skal afspejle:

- Databehandleren gennemfører de nødvendige tekniske og organisatoriske foranstaltninger for at sikre databeskyttelse i overensstemmelse med Databeskyttelseslovgivningen og i overensstemmelse med GDPR artikel 32 samt artikel 25 om privacy by design og default.
- Databehandleren har gennemført en kortlægning af sin behandling af personoplysninger, herunder en vurdering af følsomheden. Derudover har databehandleren lavet en sikkerhedsvurdering af alle datalokationer, herunder alle data-overførselssteder og implementeret sikkerhedsforanstaltninger relevante i forhold til risikovurdering for de klassificerede personoplysninger.
- Databehandlerens tekniske og organisatoriske sikkerhedsforanstaltning sikrer derved mod, at personoplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes, samt mod at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med lovgivningen.

**Generelle sikkerhedsforanstaltninger**

- Databehandleren skal implementere kryptering og pseudonymisering af personoplysninger som risikoreducerende faktorer, hvor databehandleren vurderer, at det er relevant.
- Databehandleren skal begrænse adgangen til personoplysninger til de relevante personer for at overholde krav og forpligtelser i samarbejdsaftalen.
- Databehandleren skal implementere systemer, der kan opdage, genoprette, imødegå og rapportere hændelser i forhold til personoplysninger.
- Databehandleren skal sikre at overførsel af personoplysninger til underdatabehandlere sker på forsvarlig vis.
- Databehandleren har sikret, at al tilgang til personoplysninger fra den dataansvarlige eller dennes repræsentanter sker via SSL-kryptering.
- Den i samarbejdsaftalen leverede software indeholder et rollestyringssystem, der gør det muligt for den dataansvarlige at styre den dataansvarliges repræsentanters adgang til personoplysninger.
- Databehandler har etableret en hosting platform, der sikrer, at alle personoplysninger er forsvarligt gemt, at data ikke tilgås utilsigtet samt tilhørende backupsystemer, som sikrer at alle oplysninger kan genskabes ved hændelser på hosting platformen.
- Databehandleren har implementeret software og procedurer til løbende at sikre, at den interne IT-sikkerhed er på et højt niveau.

Yderligere information om sikkerhed kan findes på Heyloyaltys hjemmeside (Privacy Policy)

### **Autorisation og adgangskontrol**

Enhver tilgang til personoplysninger sker via autorisation med personligt brugernavn og password i de interne systemer, som databehandleren har etableret til at opfylde sine forpligtelser i henhold til samarbejdsaftalen og databehandleraftalen. Databehandler har sikret sig, at underdatabehandlere benytter personlig autorisation og adgangskontrol til Heyloyalty systemet, i forbindelse med deres ydelser (hvis der er formål med adgang for underdatabehandlere).

### **Eksterne kommunikationsforbindelser**

Enhver adgang til Heyloyalty systemet sker via SSL-kryptering. Ved udsendelser TLS-krypteres mailen, hvis kontakten's mailklient accepterer dette.

### **Kontrol med afviste adgangsforsøg**

Utilsigtet adgang, forhindres af firewalls så gentagende forsøg på adgang til servere bliver blokeret.

### **Logning**

- Der føres log over dato og hvilken repræsentant fra databehandler, når personoplysninger tilgås som led i opfyldelsen af samarbejdsaftalen.
- Der udtages løbende stikprøvekontroller af overstående log for at sikre at tilgang til personoplysninger kun sker i overensstemmelse med de instrukser, som Heyloyaltys medarbejdere arbejder under.
- Der føres løbende stikprøvekontroller med at underdatabehandlere og deres repræsentanters tilgang til personoplysninger kun sker, når det er relevant i henhold til den ydelse de leverer eller under direkte instruks fra databehandleren.

### **Hjemme- og/eller fjernarbejdspladser**

- Databehandlerens behandling af personoplysninger kan ske anvendelse af hjemme- og/eller fjernarbejdspladser.
- Tilgang til personoplysninger sker via krypteret trafik (HTTPS) til og fra Heyloyalty, vha. industristandard SSL-certifikater.
- Alle medarbejdere hos databehandleren, der er autoriseret til at behandle oplysningerne, er underlagt en fortrolighedsforpligtelse og har modtaget relevant uddannelse i persondatasikkerhed og er alene berettiget til at anvende personoplysningerne som led i opfyldelse af databehandlerens forpligtelser og rettigheder i henhold til samarbejdsaftalen med den dataansvarlige.

### **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:

Databehandleren bistår den dataansvarlige med at sikre dennes overholdelse af forpligtelserne i forordningens artikel 32-36 om blandt andet sikkerhedsforanstaltninger, anmeldelse ved sikkerhedsbrud og eventuel konsultation med tilsynsmyndighederne.

Databehandleren udleverer alle nødvendige informationer med henblik på, at den dataansvarlige kan dokumentere, at behandlingen hos databehandleren lever op til forpligtelserne, samt tillader og medvirker til kontrol og audits heraf. Herunder er databehandleren forpligtet til at informere den dataansvarlige, såfremt det er databehandlerens opfattelse, at en instruks er ulovlig.

Databehandleren informerer hermed den dataansvarlige om, at indsamling af personoplysninger skal ske efter gældende lovgivning, specifikt orienteres den dataansvarlige om, at kontakter skal give informeret, specifikt samtykke til den intendede databrug, såfremt samtykke er nødvendigt efter gældende lovgivning. Databehandleren informerer også den dataansvarlige om, at udsendelse af e-mails og sms'er via Heyloyalty sker i klartekst, dvs. et medium, der ikke er adækvat til at indeholde følsomme personoplysninger, og at modtagerens adgang til

egne personoplysninger bør være password-beskyttet. U krypterede e-mails og sms'er må betragtes som et adækvat medium til almindelige personoplysninger, så som navn og adresse.

#### **C.4 Opbevaringsperiode/sletterutine**

Personoplysningerne opbevares hos databehandleren, så længe samarbejdet varer eller indtil den dataansvarlige anmoder om at få oplysningerne slettet eller tilbageleveret.

Databehandleren skal, efter den dataansvarliges valg, slette eller tilbagelevere alle personoplysninger til den dataansvarlige eller en af den dataansvarlige udpeget tredjemand, samt slette alle kopier, medmindre lovgivningen stiller krav om opbevaring af en kopi af personoplysningerne. Gives der ikke anden instruks til databehandleren fra den dataansvarlige eller den udpegede tredjemand, slettes personoplysningerne efter 120 dage fra samarbejdets ophør. Såfremt den dataansvarlige instruerer i tilbage- eller overlevering af personoplysningerne, fastsætter den dataansvarlige på tilbageleveringstidspunktet, hvordan og på hvilket lagringsmedium, personoplysningerne skal tilbageleveres. Ethvert valgt medium skal være sædvanligt for sådanne dataoverførsler.

#### **C.5 Lokaltet for behandling**

Behandling af de af Bestemmelserne omfattede personoplysninger kan ikke uden den dataansvarliges forudgående skriftlige godkendelse ske på andre lokaliteter end følgende:

- Heyloyalty's kontor i Aarhus eller en af de ansattes adresser som følge af hjemmearbejde.
- De godkendte underdatabehandlers adresse (oplyst i Bilag B.1.)
- De personoplysninger databehandleren modtager fra kundens kontakter opbevares hos 3.-part. Data lagres på servere i Danmark, der ejes af firmaet Team.Blue Denmark A/S, med hvem der er indgået databehandleraftale, således datasikkerheden er garanteret.
- Ønsker kunden at benytte 3. part, som ikke er integreret direkte med Heyloyalty, vil dette ansvar pålægge kunden.

#### **C.6 Instruks vedrørende overførsel af personoplysninger til tredjelande**

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

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

Den dataansvarlige kan føre tilsyn med databehandleren, når der efter den dataansvarliges vurdering opstår et behov herfor.

Den dataansvarlige eller en repræsentant for den dataansvarlige har ret til med et passende mellemrum og mod forudgående varsel at foretage et fysisk tilsyn vedrørende overholdelsen af denne databehandleraftale hos databehandleren. Den dataansvarliges tilsyn kan endvidere foretages ved spørgeskemaer, anmodning om udlevering af dokumentationsmateriale eller redegørelser mv.

Den dataansvarliges eventuelle udgifter i forbindelse med tilsyn afholdes af den dataansvarlige selv. Databehandleren er dog forpligtet til at afsætte de ressourcer (hovedsageligt den tid), der er nødvendig for, at den dataansvarlige kan gennemføre sit tilsyn.

Databehandlerens tidsforbrug ud over de første 4 timer kan afregnes efter databehandlerens almindelige timesatser og efter forbrugt tid. Dette skal i så fald aftales forud for det enkelte tilsyn.

Ønsker databehandleren en anden form for tilsyn, eksempelvis en ISAE 3000 revisorerklæring fra en uafhængig tredjepart vedrørende databehandlerens overholdelse af databeskyttelsesforordningen, tilbyder databehandleren udarbejdelse af en sådan, for den dataansvarliges egen regning.

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

Side 14 af 14

Det påhviler databehandleren at føre tilsyn på passende vis med eventuelle underdatabehandlere vedrørende underdatabehandlerens overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser. Databehandler er berettiget til selv at vurdere, hvad der udgør et passende tilsyn under hensyntagen til den konkrete risiko, som behandlingen hos underdatabehandleren er forbundet med.

Udover det planlagte tilsyn, kan der føres tilsyn med underdatabehandleren, når der efter databehandlerens (eller den dataansvarliges) vurdering opstår et behov herfor.

Dokumentation for databehandlerens tilsyn med underdatabehandler fremsendes til den dataansvarlige uden unødigt forsinkelse. Den dataansvarlige kan anfægte rammerne for og/eller metoden af tilsynet og kan i sådanne tilfælde anmode om gennemførelsen af et nyt tilsyn under andre rammer og/eller under anvendelse af anden metode.

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

## **Bilag D Parternes regulering af andre forhold**

Ingen særlige forhold er pt. noteret