Databehandleraftale

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

Shipvagoo ApS
CVR 42853097
Strandvejen 70
2900 Hellerup
Danmark

herefter ”databehandleren”

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

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

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 anvendelsen af en onlinebaseret fragtbookingplatform, hvorpå databehandleren videresælger transportydelser fra eksterne transportører til den dataansvarlige, 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 tre 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. Bestemmelserne med tilhørende bilag skal opbevares skriftligt, herunder elektronisk, af begge parter.

10. 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 EØS-medlemsstaternes 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.

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.

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 7 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 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 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.

10. 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 dataansvarlig, at oplysningerne er slettet, 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 overhol-delsen af databeskyttelsesforordningens artikel 28 og disse Bestemmelser, til rå-dighed for den dataansvarlige og

giver mulighed for og bidrager til revisioner, her-under 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 da-tabehandleren og underdatabehandlere er nærmeret angivet i Bilag C.7.

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 da-tabehandlerens fysiske faciliteter mod behørig legitimation.

12. Parternes aftale om andre forhold

1. Parterne kan aftale andre bestemmelser vedrørende tjenesten vedrørende be-handling af personoplysninger om f.eks. erstatningsansvar, så længe disse andre bestemmelser ikke direkte eller indirekte strider imod Bestemmelserne eller forrin-ger den registreredes grundlæggende rettigheder og frihedsrettigheder, som følger af databeskyttelsesforordningen.

13. Ikrafttræden og ophør

1. Bestemmelserne træder i kraft 11-07-2023 og er automatisk gældende for alle kundeforhold herefter.

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 per-sonoplysninger varer. I denne periode kan Bestemmelserne ikke opsiges, med-mindre andre bestemmelser, der regulerer levering af tjenesten vedrørende be-handling 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 overens-stemmelse med Bestemmelse 11.1 og Bilag C.4, kan Bestemmelserne opsiges med skriftlig varsel af begge parter.

Bilag A. Oplysninger om behandlingen

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

Formålet er at den dataansvarlige via databehandlerens onlineplatform kan købe og booke fragtydelser fra eksterne transportører med henblik på levering af kundebestillinger til den dataansvarliges kunder.

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

Databehandleren foretager alene behandling inden for rammerne af formålet, som er be-skrevet ovenfor.

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

Behandling omfatter almindelige og følsomme personoplysninger. Det drejer sig konkret om følgende personoplysninger:

- Navn,
- e-mailadresse,
- adresse,
- telefonnummer,
- IP-adresse,
- ordrenr., samt
- købs- og leveringshistorik på handelsplatformen.

A.4. Behandlingen omfatter følgende kategorier af registrerede

Behandlingen omhandler den dataansvarliges kunder.

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

Databehandleren behandler personoplysninger, så længe hovedaftalen mellem parterne består og i øvrigt i overensstemmelse med afsnit 11 i nærværende aftale samt gældende lovgivning.

Bilag B. Underdatabehandlere

B.1. Godkendte underdatabehandlere

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af følgende underdatabehandlere

NAVN	CVR	ADRESSE	BESKRIVELSE AF BEHANDLING
Amazon Web Services (Amazon Web Services, Dansk filial af Amazon Web Services EMEA SARL,)	CVR 39009323	One Burlington Plaza, Burlington Road, Dublin 4, Ireland (Luxembourg c/o Azets Insight A/S, Lyskær 3C, 1. tv, 2730 Herlev Denmark)	Data opbevares hos AWS i Irland/Frankrig
QuickPay	CVR 21822434	P. O. Pedersens Vej 2 8200 Aarhus N, Denmark	Betalings Gateway
Nets	CVR 27225993	Klausdalsbrovej 601, 2750 Ballerup, Danmark	Betalings indløser
Swedbank	CVR 28487150	Kalvebod Brygge 45, 1560 København V, Denmark	Betalings indløser
Relatel	CVR 40075291	Teglværksgade 18 2100 København Ø, Denmark	Telefonsystem
Google - G Suite - Ads		Google LLC Google Data Protection Office 1600 Amphitheatre Parkway Mountain View, California 94043 - USA	System til interne processer og deling af information internt samt annonceringsværktøj.
Twilio (Sendgrid)	53723673	375 Beale Street, Suite 300, San Francisco CA 94105	SMS-services
Zendesk	961919805	1019 Markets street, San Francisco, CA 94103 USA	Ticketsystem til kommunikation med kunder via mail
Hubspot		Hubspot, Inc. 25 First St., 2nd floor Cambridge, Massachusetts 02141 - USA	CRM, CMS og mailudsendelses-system.

NAVN	CVR	ADRESSE	BESKRIVELSE AF BEHANDLING
NHL Data	CVR 25575555	Gammel Køge Landevej 55 2500 Valby	Licenser
Microsoft Ireland Operations, Ltd.	DUNS989276399	One Microsoft Place South County Business Park Leopardstown Dublin 18, D18 P521, Ireland	Hosting services
Slack		Director of Legal Slack Technologies, Inc. Slack Legal Department 500 Howard Street San Francisco California 94105 - USA	Internt kommunikations-værktøj til deling af data og informationer.
Visma – E-conomics	CVR 40075291	Gærtorvet 3, 1799 København V, Denmark	Regnskab

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

Databehandleren skal ved enhver ændring – også eventuelle planlagte ændringer - vedrø-rende tilføjelse eller erstatning af andre underdatabehandlere underrette den dataansvarlige herom og derved give den dataansvarlige mulighed for at gøre indsigelse mod sådanne ændringer. En sådan underretning skal være den dataansvarlige i hænde minimum 7 dage før anvendelsen eller ændringen skal træde i kraft. Såfremt den dataansvarlige har indsigelser mod ændringerne, skal den dataansvarlige give meddelelse herom til databehandler inden 7 dage efter modtagelsen af underretningen.

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 stiller sine ydelser til rådighed for den dataansvarlige. Gennem anvendelsen af databehandlerens system, kan den dataansvarlige købe og booke fragt til den dataansvarliges kunder, hvorved databehandleren behandler oplysninger som anført i Bilag A.3 til fuldførelse og gennemførsel af den bestilte fragtydelse samt efterfølgende opfølgning på fragtydelsen.

C.2. Behandlingssikkerhed
Behandlingen omfatter almindelige personoplysninger (personoplysningerne er ej omfattet af databeskyttelsesforordningens artikel 9 om særlige kategorier af personoplysninger) på et større antal mennesker – forventeligt over 10.000 personer. Kategorien af personoplysninger kombineret med antal registrerede gør, at der skal etableres mellem sikkerhedsniveau for behandlingen af personoplysninger.

Databehandleren er herefter berettiget og forpligtet til at træffe beslutninger om, hvilke tekniske og organisatoriske sikkerhedsforanstaltninger, der skal gennemføres for at etablere det nødvendige (og aftalte) sikkerhedsniveau.

Foranstaltningerne fastlægges ud fra overvejelser om:

1. Hvad der kan lade sig gøre rent teknisk
2. Implementeringsomkostningerne
3. Den pågældende behandlings karakter, omfang, sammenhæng og formål
4. Konsekvenserne for borgerne ved et sikkerhedsbrud
5. Den risiko, der er forbundet med behandlingerne, herunder risikoen for:
    a. tilintetgørelse af oplysningerne
    b. tab af oplysningerne
    c. ændring af oplysningerne
    d. uautoriseret videregivelse af oplysningerne
    e. uautoriseret adgang til oplysningerne

Databehandleren skal dog – under alle omstændigheder og som minimum – gennemføre følgende foranstaltninger, som er aftalt med den dataansvarlige:

Generelle sikkerhedsforanstaltninger
Databehandleren skal opretholde et formelt, velimplementeret og professionelt ledelsessystem for informationssikkerhed baseret på lovgivningens krav, standarder på området og god databehandlingsskik. Formålet hermed er at sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og –tjenester, for at sikre, at personoplysninger ikke mistes eller kommer i forkerte hænder, samt for at hindre de skadevirkninger, sådanne brud måtte have for registrerede personer.

Databehandleren skal fastsætte og implementere interne politikker og bestemmelser, der er fyldestgørende og afspejler de faktiske forhold.

Derudover skal databehandleren opretholde procedurer, i henhold til gældende standarder, for regelmæssig afprøvning, vurdering og evaluering af de tekniske og organisatoriske foranstaltninger, som Databehandleren har implementeret til sikring af personoplysningerne.

Testmiljø
Såfremt der behandles personoplysninger i testmiljø, er kravene til sikkerhedsniveauet de samme som er beskrevet i denne instruks.

Instruktion af medarbejdere m.v.
Databehandleren sikrer at ansatte og eventuelle samarbejdspartnere til stadighed er bekendt med og har tilstrækkelig uddannelse og instruktion om databehandlingens formål, politikker, arbejdsgange og om deres tavshedspligt.

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

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

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

Adgangsstyring og administration af brugeradgang
Kun medarbejdere, som har et arbejdsbetinget behov for at behandle personoplysninger i forhold til hovedaftalen, må være oprettet som brugere med adgang til de personoplysninger, som behandles på vegne af den dataansvarlige. Kun de personer, der af den bemyndigede er autoriseret hertil, må have adgang til personoplysningerne. Databehandleren skal uden ugrundet ophold annullere autorisationer (og herunder adgange) for brugere, der ikke længere har et arbejdsbetinget behov for autorisation.

Der føres en liste over autoriserede medarbejdere med angivelse af, hvilken type adgang autorisationen dækker. Listen over autoriserede medarbejdere opdateres løbende iht. god databehandlingsskik. Efterspørger den dataansvarlige listen, skal listen gøres tilgængelig uden unødigt ophold.

Ved ydelsens afslutning lukkes medarbejdernes adgang.

Derudover anvender databehandleren sikre identifikations- og autorisationsteknologier, eksempelvis adgangskoder, biometri eller lignende.

Driftsafbrydelse, herunder driftsprocesser
Databehandler skal have dokumenterede beredskabsprocedurer, der sikrer genetablering af services uden ugrundet ophold i tilfælde af driftsafbrydelser i henhold til hovedaftalen.

Der skal ligeledes foreligge driftsdokumentation og driftsprocesser for alle de systemer, hvori den dataansvarliges data behandles.

Driftsdokumentationen og driftsprocesserne skal løbende ajourføres og gøres tilgængeligt for relevant personale.

Sikkerhedskopiering
Sikkerhedskopiering af data skal finde sted dagligt i et ubrudt forløb således, at relevante data kan reetableres mindst 30 dage tilbage. Sikkerhedskopierne opbevares således, at de ikke hændeligt eller ulovligt (eks. ved brand, oversvømmelse, uheld, tyveri eller lignende) tilintetgøres, fortabes, forringes, kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med de til enhver tid gældende regler og forskrifter for behandling af personoplysninger.

Ændringshåndtering
Databehandleren har formelle procedurer for ændringshåndtering med henblik på at sikre, at enhver ændring er behørigt autoriseret, testet og godkendt inden implementering. Proceduren skal understøttes af en effektiv funktionsadskillelse og/eller ledelsesopfølgning for at sikre, at ingen enkeltpersoner kan kontrollere en ændring alene.

Fysisk sikring og miljøsikring
Databehandlerenen skal opretholde fysiske sikringsforanstaltninger til sikring af lokaliteter, som anvendes til behandling af personoplysninger, herunder opbevaring af personoplysninger omfattet af Databehandleraftalen mod uvedkommendes adgang og manipulation.

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

Hjemme-/Fjernarbejdspladser
Såfremt der foretages databehandling fra ad hoc og/eller hjemmearbejdspladser, skal databehandleren sikre, at disse lever op til de sikkerhedsmæssige krav i denne Databehandleraftale med bilag, lovgivning i øvrigt samt Datatilsynets vejledninger herom.

Databehandler skal blandt andet opfylde og dokumentere følgende:

- Beskrivelse af anvendt krypteret forbindelse mellem ad hoc arbejdspladsen og databehandlerens/dataansvarliges netværk
- Databehandlerens interne instruks til egne medarbejdere vedrørende ad hoc og hjemmearbejdspladser

Derudover skal databehandleren, hvis det er teknisk muligt anvende tofaktor-autentifikation.

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:

<u>Bistand i forhold til de registreredes rettigheder, bestemmelse 9.1</u>

Databehandleren skal indrette de nødvendige tekniske og organisatoriske sikkerhedsforanstaltninger, således at databehandleren er i stand til at bistå den dataansvarlige med at sikre de registreredes rettigheder.

Databehandleren skal, på den dataansvarliges anmodning, bistå den dataansvarlige med at opfylde den dataansvarliges lovmæssige forpligtelser i forhold til den registrerede.

Såfremt databehandleren konstaterer, at en instruks fra den dataansvarlige er ulovlig skal databehandleren straks informere den dataansvarlige herom.

Bistand i forbindelse med brud på datasikkerheden, bestemmelse 9.2

I tilfælde af brud på persondatasikkerheden skal databehandleren i henhold til bestemmelse 9.2 give den dataansvarlige meddelelse herom med angivelse af:

- Fakta om det konstaterede brud (tid, sted, årsag)
- Hvornår bruddet startede, hvornår det blev opdaget og hvornår bruddet er standset
- Karakteren af bruddet på persondatasikkerheden, herunder om der er sket brud på fortrolighed, integritet og tilgængelighed
- Kategorierne og det omtrentlige antal berørte registrerede, hvis det er muligt
- Kategorierne og det omtrentlige antal berørte registreringer af personoplysninger
- Navn og kontaktoplysninger til kontaktpunkt, hvor yderligere oplysninger kan indhentes
- Beskrivelse af de sandsynlige konsekvenser af bruddet
- Beskrivelse af foranstaltninger der er truffet, eller foreslås truffet som led i håndteringen af bruddet og dets mulige skadevirkninger

Hvis det ikke er muligt at levere oplysningerne ovenfor samlet, skal de i stedet leveres trinvist.

Databehandleren er forpligtet til at bidrage aktivt til, at den dataansvarlige modtager tilstrækkelige informationer til, at den dataansvarlige kan håndtere en eventuel informationsforpligtelse til de registrerede og Datatilsynet.

Databehandleren må ikke hverken offentligt eller til tredjeparter kommunikere om brud på persondatasikkerheden, jf. pkt. 10.1 og pkt. 10.2 uden forudgående skriftlig aftale med den dataansvarlige, med mindre databehandlerenen har en retlig forpligtelse til sådan kommunikation.

C.4 Opbevaringsperiode/sletterutine
Personoplysninger opbevares mens at hovedaftalen bistår, hvorefter de slettes hos databehandleren. Ydermere kan den dataansvarlige til enhver tid selv slette de indsamlede personoplysninger hos databehandleren.

Ved ophør af tjenesten vedrørende behandling af personoplysninger, skal databehandleren enten slette eller tilbagelevere personoplysningerne i overensstemmelse med bestemmelse 11.1, medmindre den dataansvarlige – efter underskriften af disse bestemmelser – har ændret den dataansvarlige oprindelige valg. Sådanne ændringer skal være dokumenteret og opbevares skriftligt, herunder elektronisk, i tilknytning til bestemmelserne.

C.5 Lokalitet for behandling
Behandling af de af Bestemmelserne omfattede personoplysninger kan ikke uden den dataansvarliges forudgående skriftlige godkendelse ske på andre lokaliteter end følgende:

Behandlingen må alene finde sted hos Databehandleren, på de i hovedaftalen oplyse adresser, på hjemme- og fjernarbejdspladser som er omfattet og reguleret af disse Bestemmelser samt på de adresser på underdatabehandlere, som er omfattet af skemaet i bilag B.1.

C.6 Instruks vedrørende overførsel af personoplysninger til tredjelande
Databehandleren må ikke uden forudgående aftale overføre personoplysninger til tredjelande.

Derudover må overførslen udelukkende ske til sikre tredjelande, samt til underdatabehandlere, der har tilsluttet sig certificeringer om overførselsgrundlag, som er godkendt af Europa-Kommissionen.

Der overføres data til følgende tredjelande: Nej

Der overføres data til følgende underdatabehandlere: Nej

Overførselsgrundlaget er:
☐ Retligt bindende instrumenter mellem myndigheder
☐ Bindende virksomhedsregler
☐ Adfærdskodeks og certificeringsmekanismer
☐ Standardbestemmelser om databeskyttelse (SCC)
☐ Ad-hoc kontrakter

I forbindelse med overførsel af personoplysninger til lande udenfor EU/EØS, jf. afsnit 8**,** giver den Dataansvarlige hermed Databehandleren fuldmagt til at vedtage Europa-Kommissionens standardbestemmelser om databeskyttelse (SCC) med underdatabehandlere udenfor EU/EØS på den Dataansvarliges vegne og i den Dataansvarliges navn, dog forudsat at den Dataansvarlige forinden har godkendt overførslen i overensstemmelse med afsnit 7.

Hvis den dataansvarlige ikke i disse Bestemmelser eller efterfølgende giver en dokumenteret instruks vedrørende overførsel 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
Databehandleren fremsender årligt en skriftlig status, på de forhold som er omfattet af nærværende databehandleraftale og andre relevante områder, til den dataansvarlige.