

Databehandleraftale

GatewayAPI

SMS Gateway

Databehandlersaftale inkl. Standardkontraktbestemmelser

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

mellem

ONLINECITY.IO ApS
Buchwaldsgade 50
5000 Odense C
CVR nr.: 27364276

herefter "databehandleren"

og

Garuda A/S
Voldbjergvej 14, 2. sal
8240 Risskov
CVR nr.: 68755611
Att.: Søren Skou Jessen

herefter "den dataansvarlige"

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

1. Indhold	
2. Præambel	4
3. Den dataansvarliges rettigheder og forpligtelser	4
4. Databehandleren handler efter instruks	5
5. Fortrolighed	5
6. Behandlingssikkerhed	5
7. Anvendelse af underdatabehandlere	6
8. Overførsel til tredjelande eller internationale organisationer	7
9. Bistand til den dataansvarlige	8
10. Underretning om brud på persondatasikkerheden	9
11. Sletning og returnering af oplysninger	10
12. Revision, herunder inspektion	10
13. Parternes aftale om andre forhold	10
14. Ikrafttræden og ophør	10
15. Kontaktpersoner hos den dataansvarlige og databehandleren	11
Bilag A Oplysninger om behandlingen	12
Bilag B Underdatabehandlere	13
Bilag C Instruks vedrørende behandling af personoplysninger	14
Bilag D Parternes regulering af andre forhold	19

2. Præambel

1. Disse Bestemmelser fastsætter databehandlerens rettigheder og forpligtelser, når denne foretager behandling af personoplysninger på vegne af den dataansvarlige.
2. Disse bestemmelser er udformet med henblik på parternes efterlevelse af 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 SMS Gateway (herefter "GatewayAPI") 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 medlemsstaternes¹ nationale ret og disse Bestemmelser.
2. Den dataansvarlige har ret og pligt til at træffe beslutninger om, til hvilke(t) formål og med hvilke hjælpemidler, der må ske behandling af personoplysninger.
3. Den dataansvarlige er ansvarlig for, blandt andet, at sikre, at der er et behandlingsgrundlag for behandlingen af personoplysninger, som databehandleren instrueres i at foretage.

4. Databehandleren handler efter instruks

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

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

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. 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 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 dataansvarlig, at oplysningerne er slettet, medmindre EU-retten eller medlemsstaternes nationale ret foreskriver opbevaring af personoplysningerne.
2. Følgende regler i EU-retten eller medlemsstaternes nationale ret foreskriver opbevaring af personoplysningerne efter ophør af tjenesterne vedrørende behandling af personoplysninger:
 - a. Bogføringslov, jf. lov nr. 1006 af 23. december 1998, med de ændringer, der følger af § 122 i lov nr. 428 af 6. juni 2005, § 2 i lov nr. 245 af 27. marts 2006 og § 1 i lov nr. 509 af 7. juni 2006.

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

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 lovgivningen har adgang til den dataansvarliges eller databehandlerens faciliteter, eller repræsentanter, der optræder på tilsynsmyndighedens vegne, adgang til databehandlerens fysiske faciliteter mod behørig legitimation.

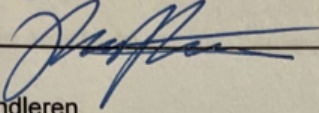
13. Parternes aftale om andre forhold

1. Parterne kan aftale andre bestemmelser vedrørende tjenesten 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 u hensigtsmæssigheder 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

Navn Rasmus Hall Mortensen
Stilling Adm. direktør
Telefonnummer 45 22630389
E-mail RAM@GARUDA.DK
Underskrift 

På vegne af databehandleren

Navn Dennis Benneballe Grade
Stilling Compliance-Specialist
Telefonnummer +45 66 11 83 11
E-mail gdpr@gatewayapi.com
Underskrift 

15. Kontaktpersoner hos den dataansvarlige og databehandleren

1. Parterne kan kontakte hinanden via nedenstående kontaktpersoner.

På vegne af dataansvarlig:

Navn Søren Skou Jessen
Stilling GDPR Compliance konsulent
Telefonnummer +45 87 46 86 00
E-mail ssj@garuda.dk

På vegne af databehandleren:

Navn Dennis Benneballe Grade
Stilling Compliance-Specialist
Telefonnummer +45 66 11 83 11
E-mail gdpr@gatewayapi.com

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

Bilag A Oplysninger om behandlingen

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

Til visning af beskedlog af både sendte og evt. modtagne beskeder og leveringsbesked ved sendte beskeder

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

Opbevaring i 30 dage

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

Telefonnummer, beskedindhold (og afhængigt herfra mulige oplysninger som medlemsnumre, abonnementsnumre, abonnements typer, aftaletidspunkter, m.fl.) afsendernavn/-nummer

A.4. Behandlingen omfatter følgende kategorier af registrerede

Kunder, samarbejdspartnere, medarbejdere

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

Indtil ophør af samarbejdet ved opsigelse af nærværende aftale eller brugerkonto, ved overtrædelse af alm. brugsbetingelser eller ved længerevarende inaktivitet på brugerkontoen (se "Vilkår & Betingelser" for nærmere oplysninger).

Bilag B Underdatabehandlere

B.1. Godkendte underdatabehandlere

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af følgende underdatabehandlere

NAVN	CVR	ADRESSE	BESKRIVELSE AF BEHANDLING
Google LLC	BE 0876065378 IE 6388047V DK 28866984 NL 812788515B01 FI 09073468	Belgien: 7331 Mons Saint-Ghislain, Hainaut Irland: Gordon House 4 Barrow St, Dublin Danmark: Tuevej / Kongstedvej 7000 Fredericia Nederlandene: Oostpolder 4, 9979 XT Eemshaven Finland: Ensontie 1, 49420 Hamina	Hosting af SMS-database (opbevaring) --- Belgien som hoved-datacenter, redundans i resterende EU-datacentre

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

OnlineCity sender en varseling ved ændring af underdatabehandlere ud til den dataansvarlige 30 dage inden skiftet, og anser mangel på tilbagemeldelse af varselingen som godkendelse af underdatabehandleren.

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:

Forsendelse og modtagelse af SMS via SMS-API-gateway samt samarbejdspartners SMS-API-gateways.

C.2. Behandlingssikkerhed

Behandlingen omfatter ingen personoplysninger omfattet af Databeskyttelsesforordningen Artikel 9 om "særlige kategorier af personoplysninger", hvorfor der skal etableres "lille sikkerhedsniveau".

Sikkerhedsniveauet skal afspejle:

- At sikre, at login- og adgangskodeprocedurer, firewall og antivirus-software samt underlægning af stærk kryptering på transmission af personoplysninger er vedligeholdt
- At sikre, at alene medarbejdere med arbejdsrelaterede formål hertil adgang til personoplysninger
- At opbevare datalagermedier på forsvarlig vis, således at disse ikke er tilgængelig for tredjemand
- At sikre, at bygninger og systemer, der anvendes i forbindelse med databehandlingen er sikre, samt at der alene anvendes hardware og software af høj kvalitet, som opdateres løbende
- At sikre, at medarbejdere modtager fyldestgørende instruktioner i og retningslinjer for behandlingen af personoplysninger. Databehandleren er forpligtet til at sikre, at de medarbejdere, som er involveret i behandlingen af personoplysninger, er bekendte med sikkerhedskravene
- At sikre, at de medarbejdere, der er autoriserede til at behandle personoplysninger, har indgået fortrolighedsaftaler eller er underlagt fornøden lovreguleret fortrolighedsforpligtelse
- At sikre, at data alene benyttes på vegne af Dataansvarlig, og at Databehandleren ikke selv kan disponere over oplysningerne til egne formål, herunder kommercielt brug

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:

Databehandleren anonymiserer modtagenummeret (sidste 4 cifre), beskedindholdet og afsender-ID af SMS'er 30 dage efter, at meddelelsen er sendt. For overtaksede SMS'er lagres dataene i 6 måneder, så vi kan behandle refusionsanmodninger rettidigt. Herefter anonymiseres disse persondata helt.

Etablering, vedligeholdelse og årlig test af beredskabsplan samt regelmæssig backup af personoplysninger, samt 24/7 monitorering af driftssystemerne.

Årlig gennemgang af procedurerne indeholdt i procedurerne som indgår som kontrolområde i ISAE 3000 virksomhedsrevision, som årligt gennemføres.

Adgang til personoplysninger via internettet udelukkende via autoriserede brugere og igennem krypterede og/eller sikre forbindelse, dvs. HTTPS, TLS 1.2, m.fl, samt logisk adgangskontrol samt autorisations- og rettighedsstyring.

Fortrolighedserklæringer med medarbejdere og samarbejdspartnere.

Træning af og bevidstliggørelse om sikkerhed hos medarbejdere samt deling af retningslinjer, procedurebeskrivelser og politikker.

Beskyttelse af personoplysninger under transmission vha. stærk krypterede internetforbindelser og e-mails.

Firewall og antivirus-software til sikring mod uautoriseret adgang til personoplysninger.

Kryptering af personoplysninger under opbevaring samt sikker opbevaring af evt. datalagermedier.

Alarmeredskab, alarmsikring på dør, vinduer og indgange, og låsning af printede personoplysninger i pengeskab, overvågning af fællesarealer.

Adgang til arbejdsrelaterede systemer til medarbejdere på eksterne kommunikationsforbindelser, eks. i hjemmet eller offentlige steder, kun via krypterede og sikre internetforbindelser, TLS 2.1 som minimum.

Logning af systemer, databaser og netværk, dvs. af logins og transmissioner via API samt adgang til database med personoplysninger.

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:

Databehandler har indført politikker og procedurer, der sikrer, at OnlineCity kan bistå den dataansvarlige med at opfylde dennes forpligtelse til at besvare anmodninger om udøvelse af de registreredes rettigheder.

Databehandler har indført politikker og procedurer, der sikrer, at OnlineCity kan bistå den dataansvarlige med at sikre overholdelse af forpligtelserne i artikel 32 om behandlingssikkerhed, artikel 33 om anmeldelse og underretning af brud på persondatasikkerheden samt artikel 34 – 36 om konsekvensanalyser.

Databehandler indført politikker og procedurer, der sikrer, at OnlineCity kan stille alle oplysninger, der er nødvendige for at påvise overholdelse af kravene til databehandlere, til rådighed for den dataansvarlige.

Databehandler giver desuden mulighed for og bidrager til revisioner, herunder inspektioner, der foretages af den dataansvarlige eller andre, som er bemyndiget hertil af den dataansvarlige.

C.4 Opbevaringsperiode/sletterutine

Personoplysninger opbevares i maks. 30 dage efter forsendelse hhv. modtagelse af SMS, hvorefter de slettes 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 Lokaltet for behandling

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

I Databehandlerens lokaler eller hos databehandlerens underdatabehandlere. Hovedkontor for databehandleren, OnlineCity.IO ApS, er Buchwaldsgade 50, 5000 Odense C, med øvrige kontorer i København og Danneskiold-Samsøe-Allé 41, 1434 København K og C. A. Olesens Gade 4, 9000 Aalborg. Underdatabehandlere har adresse jf. Bilag B, afsnit 1.

C.6 Instruks vedrørende overførsel af personoplysninger til tredjelande

Personoplysninger må kun overføres til sikre tredjelande hhv. internationale organisationer eller tredjelande hhv. internationale organisationer med gyldigt hjemmel og kun med nødvendig formål. Dog skal personoplysninger under alle omstændigheder forsøges at forblive inden for EU.

Grundlaget for overførslen som omhandlet i Databeskyttelsesforordningens artikel 5 er EUs standardkontraktbestemmelser samt de krav omtalt i Schrems-II-dommen.

Derudover vil databehandleren sikre, at evt. overførsler til usikre tredjelande er sikret vha. indgåelse af EUs standardkontraktbestemmelser, samt understøttes af supplerende tekniske og organisatoriske foranstaltninger som nævnt i EU Domstolens dom i Schrems-II-sagen. Disse skal understøtte at give de registrerede samme tilsvarende beskyttelsesniveau som i EU under GDPR, samt mulighed for håndhævelse af deres rettigheder under GDPR.

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

Databehandleren skal årligt for egen regning indhente en revisionserklæring fra en uafhængig tredjepart vedrørende databehandlerens overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.

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

- ISAE 3000

Revisionserklæringer fremsendes uden unødigt forsinkelse til den dataansvarlige til orientering. Den dataansvarlige kan anfægte rammerne for og/eller metoden i revisionserklæringen og kan i sådanne tilfælde anmode om en ny revisionserklæring under andre rammer og/eller under anvendelse af anden metode.

Baseret på resultaterne af revisionserklæringen, 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 har herudover adgang til at foretage inspektioner, herunder fysiske inspektioner, med lokaliteterne hvorfra databehandleren foretager behandling af personoplysninger, herunder fysiske lokaliteter og systemer, der benyttes til eller i forbindelse med behandlingen. Sådanne inspektioner kan gennemføres, når den dataansvarlige finder det nødvendigt.

Den dataansvarliges eventuelle udgifter i forbindelse med en fysisk inspektion afholdes af den dataansvarlige selv. 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 skal årligt for egen regning indhente en revisionserklæring fra en uafhængig tredjepart vedrørende underdatabehandlerens overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.

Der er enighed mellem parterne om, at følgende typer af revisionserklæring samt certifikater kan anvendes i overensstemmelse med disse bestemmelser:

SSAE18 SOC 2 rapport
SSAE18 SOC 3 rapport
ISO 27701

Revisorerklæringer og certifikater fremsendes uden unødigt forsinkelse til den dataansvarlige til orientering. Den dataansvarlige kan anfægte rammerne for og/eller metoden i erklæringen og kan i sådanne tilfælde anmode om en ny revisorerklæring under andre rammer og/eller under anvendelse af anden metode.

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.

Databehandleren eller en repræsentant for databehandleren har ikke adgang til at foretage inspektioner selv, herunder fysiske inspektioner, med lokaliteterne hvorfra underdatabehandleren foretager behandling af personoplysninger, herunder fysiske lokaliteter og systemer, der benyttes til eller i forbindelse med behandlingen. Sådanne inspektioner gennemføres i en virksomhedsrevision og resultaterne heraf er fastholdt i de ovennævnte revisorerklæringer og certifikater.

Dokumentation for sådanne inspektioner, dvs. ovennævnte revisorerklæringer og certifikater, fremsendes uden unødigt forsinkelse til den dataansvarlige til orientering, hvis denne anmoder om indsigt i disse. Den dataansvarlige kan anfægte rammerne for og/eller metoden af inspektionen og kan i sådanne tilfælde anmode om afbrydelse af databehandlingen indtil rammerne enten er tilfredsstillende for den dataansvarlige, eller den dataansvarlige vælger at stoppe samarbejdet, med videre.

Bilag D Parternes regulering af andre forhold