Effecttracker.com databehandleraftale

Denne databehandleraftale er en del af licensaftalen eller anden skriftlig eller elektronisk aftale mellem Kenneth Christiansen Holding ApS og licenstager om køb af adgang til Effecttracker.com tjenesten og afspejler parternes aftale om behandling af persondata.

Ved tiltrædelse af licensaftalen tiltræder licenstager ligeledes denne databehandleraftale mellem:

Dataansvarlig
Virksomhed
Kontaktperson:
Adresse
Postnummer By
Telefon:
Mail:
CVR-nr.:

Underskrift:

Dato: / - 2021

og

Databehandler
Effecttracker.com / Kenneth Christiansen Holding ApS
Sønderdalen 26
2870 Dyssegård
Danmark
CVR-nr.: 29394059
Telefon: +45 21656973
Mail: kenneth@Effecttracker.com
Kontaktperson: Kenneth Christiansen
Telefon: +45 21 64 69 73
Mail: info@effecttracker.com

Underskrift:

Dato: 26/07 - 2021

Parterne kaldes i det følgende henholdsvis den "dataansvarlige" og "databehandleren", og "part" eller tilsammen "parterne".

1. Introduktion

Ved brug af Effecttracker.com tjenesten og ethvert website eller applikation i tilknytning til Effecttracker.com tjenesten (samlet benævnt “Effecttracker.com tjenesten”), vil den dataansvarlige være ansvarlig for sin behandling af personoplysninger i Effecttracker.com tjenesten. Databehandleren vil behandle personoplysninger på vegne af den dataansvarlige. For at sikre, at parterne lever op til sine forpligtelser under nationale databeskyttelsesregler samt Europa-Parlamentet og Rådets forordning (EU) 2016/279 ("GDPR"), har parterne indgået denne

databehandleraftale, som udgør instruksen fra den dataansvarlige til databehandleren og dermed regulerer databehandlerens behandling af personoplysninger på vegne af den dataansvarlige.

Begge parter bekræfter, at de har fuldmagt til at tiltræde og underskrive databehandleraftalen.

Det gælder for hele databehandleraftalen og i forholdet mellem den dataansvarlige og databehandleren, at krav, der følger af GDPR, som er beskrevet i denne aftale og som ikke følger af nuværende lovgivning, først er gældende fra 25. maj 2018, hvor GDPR træder i kraft.

2. Definitioner

Definitionen af personoplysninger, særlige kategorier af data (ufølsomme oplysninger), behandling, den registrerede, dataansvarlig og databehandler er den samme som den relevante persondatalovgivning, herunder GDPR.

Aftalen regulerer databehandlerens behandling af personoplysninger på vegne af den dataansvarlige, og beskriver, hvordan databehandleren skal medvirke til at beskytte privatliv på vegne af den dataansvarlige og dennes registrerede gennem tekniske og organisatoriske foranstaltninger, som er krævet under den gældende databeskyttelseslovgivning, herunder GDPR fra den 25. maj 2018.

Formålet med databehandlerens behandling af personoplysninger på vegne af den dataansvarlige er at kunne opfylde aftalen om levering af Effecttracker.com tjenesten til den dataansvarlige.

Databehandleraftalen har forrang for andre modstridende bestemmelser vedrørende behandling af personoplysninger for så vidt angår vilkår for brugen af Effecttracker.com tjenesten

eller i

andre aftaler gældende parterne imellem. Databehandleraftalen er gyldig, så længe den dataansvarlige abonnerer på Effecttracker.com tjenesten jf. bestemmelserne i licensaftalen, og databehandleren derfor skal behandle personoplysninger på vegne af den dataansvarlige.

3. Databehandlerens forpligtelser

Databehandleren skal udelukkende behandle personoplysninger på vegne af og som følge af den dataansvarliges instruktioner. Ved at indgå denne databehandleraftale, instruerer den dataansvarlige databehandleren i at behandle personoplysninger på følgende måder:

- i overensstemmelse med gældende lovgivning i Danmark.
- for at opfylde sine forpligtelser i henhold til licensaftalen for Effecttracker.com tjenesten
- som yderligere specificeret ved den dataansvarliges normale brug af Effecttracker.com tjenesten
- som beskrevet i denne databehandleraftale

Databehandleren har ikke nogen grund til at tro, at gældende lovgivning forhindrer databehandleren i at efterleve instruktionerne gengivet ovenfor. Databehandleren skal, hvis denne bliver opmærksom på det, give den dataansvarlige besked om instruktioner eller andre behandlingsaktiviteter udført af den dataansvarlige, som efter databehandlerens opfattelse strider imod den gældende databeskyttelseslovgivning. Kategorierne af registrerede og personoplysninger, som behandles i henhold til denne databehandleraftale er som følger:

- **Kategorier af registrerede**

- den dataansvarliges kunder
- den dataansvarliges medarbejdere
- den dataansvarliges kontaktpersoner
- den dataansvarliges samarbejdspartnere
- den dataansvarliges samarbejdspartneres medarbejdere
- eventuelle andre

- **Kategorier af personoplysninger**

- Fulde navn
- Titel
- E-mail adresse
- Telefonnummer
- Adresse

Under hensyntagen til den teknologi, der er tilgængelig, og omkostningerne ved implementeringen, samt omfanget, konteksten og formålet med behandlingen, er databehandleren forpligtet til at foretage alle rimelige foranstaltninger, herunder tekniske og organisatoriske, for at sikre et tilstrækkeligt sikkerhedsniveau i forhold til den risiko og kategorien af personoplysninger, der skal beskyttes.

Databehandleren skal bistå den dataansvarlige med passende tekniske og organisatoriske foranstaltninger, så vidt som dette er muligt og under hensyntagen til behandlingens art og kategorien af oplysninger, der er tilgængelige for databehandleren, for at sikre overholdelse af den dataansvarliges forpligtelser i henhold til gældende databeskyttelseslovgivning, herunder for så vidt angår bistand i forhold til opfyldelse af anmodninger fra registrerede samt generel overholdelse af bestemmelserne under GDPR artikel 32-36.

Databehandleren skal underrette den dataansvarlige uden unødig forsinkelse via kontaktperson oplyst i databehandleraftalen, hvis databehandleren bliver bekendt med sikkerhedsbrist. Endvidere skal databehandleren så vidt muligt og lovligt underrette den dataansvarlige, hvis;

- en anmodning om indsigt i personoplysninger modtages direkte fra den registrerede
- en anmodning om indsigt i personoplysninger modtages direkte fra statslige myndigheder, herunder politiet.

Databehandleren må ikke besvare sådanne anmodninger fra registrerede, medmindre denne er autoriseret af den dataansvarlige til at gøre det. Databehandleren vil endvidere ikke videregive information om denne databehandleraftale til statslige myndigheder såsom politiet, herunder personoplysninger, medmindre databehandleren er forpligtet til det i medfør af lovgivningen, såsom ved en retskendelse eller lignende.

Hvis den dataansvarlige kræver information eller assistance omkring sikkerhedsforanstaltninger, dokumentation eller information om, hvordan databehandleren behandler personoplysninger generelt, og en sådan anmodning indeholder information, som går ud over, hvad der er nødvendigt ifølge gældende databeskyttelseslovgivning, må databehandleren kræve betaling for sådanne yderligere services. Databehandleren og dennes ansatte skal sikre fortrolighed i forhold til personoplysninger, som behandles i henhold til databehandleraftalen. Denne bestemmelse skal ligeledes gælde efter ophør af databehandleraftalen.

4. Den dataansvarliges forpligtelser

Den dataansvarlige bekræfter ved indgåelse af denne aftale, at:

- Den dataansvarlige skal ved brug af Effecttracker.com tjenesten stillet til rådighed af databehandleren, udelukkende behandler personoplysninger i overensstemmelse med kravene i den til enhver tid gældende databeskyttelseslovgivning.
- Den dataansvarlige har et lovligt grundlag for at behandle og videregive personoplysninger til databehandleren (herunder til underdatabehandlere som databehandleren anvender).
- Den dataansvarlige har ansvaret for nøjagtigheden, integriteten, pålideligheden og lovligheden af de personoplysninger som skal behandles af databehandleren.
- Hvis det er nødvendigt for at kunne anvende Effecttracker.com tjenesten, at den dataansvarlige har opfyldt alle obligatoriske krav og pligter i forhold til anmeldelse hos eller opnåelse af tilladelse fra de relevante offentlige myndigheder for så vidt angår behandlingen af personoplysninger.
- Den dataansvarlige har opfyldt sin oplysningsforpligtelser over for de registrerede vedrørende behandlingen af personoplysninger i henhold til gældende databeskyttelseslovgivning.
- Den dataansvarlige er enig i, at databehandleren har givet de relevante garantier for så vidt angår implementeringen af tekniske og organisatoriske sikkerhedsforanstaltninger for at sikre de registreredes rettigheder og deres personoplysninger.
- Den dataansvarlige skal ved brug af Effecttracker.com tjenesten ikke behandle følsomme persondata.
- Den dataansvarlige skal have en opdateret liste over de kategorier af personoplysninger, som databehandleren behandler. Dette gælder særligt i det omfang sådan behandling afviger fra de kategorier af oplysninger, som fremgår af nærværende databehandleraftale.

5. Underdatabehandlere og videregivelse af data

Som en del af driften af Effecttracker.com tjenesten anvender databehandleren underleverandører (“underdatabehandlere").

Databehandlerens underleverandører er oplistet i den til enhver tid opdaterede liste over underdatabehandlere. Databehandleren skal sikre sig, at dennes underdatabehandlere skal overholde tilsvarende forpligtelser og krav, som er beskrevet i denne databehandleraftale.

Denne databehandleraftale udgør den dataansvarliges forudgående generelle og specifikke skriftlige godkendelse af databehandlerens brug af underdatabehandlere.

Den dataansvarlige skal orienteres, inden databehandleren udskifter sine underdatabehandlere. Den dataansvarlige har dog kun ret til at protestere imod en ny underdatabehandler, som behandler personoplysninger på vegne af den dataansvarlige, hvis denne ikke behandler data i overensstemmelse med gældende databeskyttelseslovgivning. I en sådan situation skal databehandleren demonstrere overensstemmelse ved at give den dataansvarlige adgang til databehandlerens databeskyttelsesvurdering af underdatabehandleren. Hvis der stadig er uenighed om anvendelsen af underdatabehandleren kan den dataansvarlige opsige sit abonnement på Effecttracker.com tjenesten, herunder med et kortere varsel end normalt for at sikre, at den dataansvarliges personoplysninger ikke behandles af den pågældende underdatabehandler.

6. Sikkerhed

Databehandleren er forpligtet til at sikre et højt sikkerhedsniveau på Effecttracker.com tjenesten og tilhørende services og applikationer, hvilket sikres ved relevante organisatoriske, tekniske og fysiske sikkerhedsforanstaltninger, som er påkrævede i henhold til information om sikkerhedsforanstaltninger som beskrevet i GDPR artikel 32.

De følgende foranstaltninger er særligt væsentlige:

- Klassificering af personoplysninger for at sikre implementering af sikkerhedsforanstaltninger, der er relevante i forhold til risikovurderinger.
- Vurdering af kryptering og pseudonymisering som risikoreducerende faktorer.
- Begrænse adgangen til personoplysninger til de relevante personer, der skal til for at overholde krav og forpligtelser i databehandleraftalen eller i henhold til parternes aftale om anvendelse af Effecttracker.com tjenesten jf. licensaftalen.
- Drift og implementering af systemer, der kan opdage, genoprette, imødegå og rapportere hændelser i forhold til personoplysninger.
- Kortlægge sikkerhedsstrukturen samt hvordan personoplysninger overføres imellem parterne.
- Foretage vurdering af eget sikkerhedsniveau for at sikre, at nuværende tekniske og organisatoriske foranstaltninger er tilstrækkelige til beskyttelse af personoplysninger, herunder i henhold til GDPR artikel 32 om behandlingssikkerhed samt artikel 25 om privacy by design og default.

7. Adgang til revision

Den dataansvarlige er berettiget til at igangsætte en revision af databehandlerens forpligtelser i henhold til denne databehandleraftale én gang årligt. Hvis den dataansvarlige er forpligtet hertil

efter gældende lovgivning, kan der foretages revision oftere en én gang årligt. Den dataansvarlige skal i forbindelse med anmodning om en revision medsende en detaljeret revisionsplan med en beskrivelse af omfang, varighed og startdato minimum fire uger forud for den foreslåede startdato. Det skal besluttes i fællesskab mellem parterne, hvis en tredjepart skal foretage revisionen. Imidlertid kan den dataansvarlige lade databehandleren bestemme, at revisionen af sikkerhedsårsager skal foretages af en neutral tredjepart efter databehandlerens valg, såfremt der er tale om et behandlingsmiljø, hvor flere dataansvarliges data er anvendt.

Hvis det foreslåede omfang for revisionen følger en ISAE, ISO eller lignende certificeringsrapport udført af en kvalificeret tredjepartsrevisor inden for de forudgående tolv måneder, og databehandleren bekræfter, at der ikke har været nogen materielle ændringer i de foranstaltninger, som har været under revision, skal den dataansvarlige acceptere denne revision i stedet for at anmode om en ny revision af de foranstaltninger, som allerede er dækket.

Under alle omstændigheder skal revision finde sted i normal kontortid på den relevante facilitet i overensstemmelse med databehandlerens politikker og må ikke på urimelig vis forstyrre databehandlerens sædvanlige kommercielle aktiviteter

Den dataansvarlige er ansvarlig for alle omkostninger i forbindelse med anmodningen om revision. Databehandlerens assistance i forbindelse hermed, som overskrider den almindelige service som databehandleren skal stille til rådighed som følge af gældende databeskyttelseslovgivning, afregnes særskilt.

8. Varighed og ophør

Nærværende databehandleraftale er gældende, så længe databehandleren behandler personoplysninger på vegne af den dataansvarlige i forbindelse med den dataansvarliges brug af Effecttracker.com tjenesten. Denne databehandleraftale vil automatisk ophøre ved udgangen af den dataansvarliges opsigelsesperiode i forhold til abonnement på Effecttracker.com tjenesten. Ved ophør af abonnementet skal den dataansvarlige selv slette alle persondata, som databehandleren har behandlet på vegne af den dataansvarlige under databehandleraftalen før lukning af kontoen.

Såfremt den dataansvarlige ønsker bistand til returnering af data, fastsættes omkostninger forbundet hermed i fællesskab af parterne og skal baseres på:

- Timetakster for databehandlerens anvendte tid
- Kompleksiteten af den anmodede proces og
- Det valgte format.

Når data slettes af den dataansvarlige, slettes de samtidig permanent, og kan ikke genskabes. Databehandleren kan under særlige forhold være er berettiget til at beholde personoplysninger efter ophør af databehandleraftalen i det omfang, det er nødvendigt i henhold til gældende lov, hvilket i så fald vil ske i overensstemmelse med de tekniske og organisatoriske sikkerhedsforanstaltninger, som er beskrevet i databehandleraftalen, og det vil fremgå af en tillægsaftale til databehandleraftalen.

Ændringer

Ændringer til databehandleraftalen skal vedlægges i et særskilt bilag til databehandleraftalen. Hvis nogen af bestemmelserne i databehandleraftalen er ugyldige, får dette ikke indvirkning på de resterende bestemmelser. Parterne skal erstatte ugyldige bestemmelser med en lovlig bestemmelse, som afspejler formålet med den ugyldige bestemmelse.

Ansvar

Ansvar for handlinger i strid med bestemmelserne i denne databehandleraftale reguleres af ansvars- og erstatningsbestemmelser i licensaftalen for Effecttracker.com tjenesten. Dette gælder ligeledes for enhver overtrædelse, som foretages af databehandlerens underdatabehandlere. Lovvalg og værneting Aftalen er underlagt dansk ret og enhver tvist skal forelægges en dansk domstol.

9. Version

Denne udgave af databehandleraftalen er version 8, og erstatter tidligere gældende databehandleraftaler.

Senest opdateret den 25. Juli 2021.

Opdateringen vedrører

1. Ekstra IT udvikler fra DOTBUCH, således at der er 2 udviklere tilknyttet Effecttracker
2. Flytning af Effecttracker hosting fra Amazon til Hosteurope
   (Hosteuropes databehandleraftale er indsat som bilag C)

Bilag A: Underdatabehandlere

Følgende underdatabehandlere er godkendt på tidspunktet for indgåelse af denne licensaftale på de betingelser, der følger af databehandleraftalen og databeskyttelseslovgivningen:

Hostingleverandør og C1 CMS udbyder – (Aftalen er indsat som bilag til licensaftalen)
Host Europe GmbH
Hansestr. 111
51149 Cologne
Kundeaftalen med Hosteurope er indsat nederst i dette dokument som Bilag C

GDPR compliant underdatabehandlere, hvor databehandling kan ske uden for EU, som er har leveret aftaler indeholdende Standard Contractual Clauses:

Email validering – (Sikrer at sendte emails ikke kategoriseres som spam og dokumenterer at mailen er leveret.)

Sendgrid.com Denver, CO 1801 California Street Suite 500 Denver, CO 80202	Twilio.com 7 Soho Square, Fifth Floor W1D 3QB, London, United Kingdom

Standard Contractual Clauses Addendum – tilføjelse til aftale findes som Bilag D i denne aftale eller link her:
https://www.twilio.com/legal/data-protection-addendum

Afstandsmåling via Google Maps – (Bruges af nogle licensbrugere til at udregne kørselstid mellem to adresser)
Google Ireland Limited
Gordon House
Barrow Street
Dublin 4
Ireland
VAT number: IE 6388047VAddendum – tilføjelse til aftale findes som Bilag E i denne aftale:

EFFECTTRACKER

Bilag B – Leverandør af IT udvikling

Ny Ekstern IT afdeling, ansvarlig for sikkerhed og programmering
(Er underlagt samme fortrolighed vedr. persondata som medarbejdere på Effecttracker.com)
Der er tegnet 2 kontrakter med udviklere. En NDA og en udvikleraftale.

Fra marts 2021:

Company	InTouch Soft SRL
Name	Adrian Cojocariu
Address	11th Papadiei Street, 707410 – Valea Lupului, Iasi (Romania)
Phone:	(+40) 762.664.128
Email	adi.cojocariu@gmail.com
Code	RO42179905
EUID	ROONRC.J22 / 2935/2019

Fra juli 2021:

Company:	DOTBUCH
Name:	Jesper Buch
Address:	Nørrebrogade 55 a 2
Phone:	30 64 11 83
Email	info@dotbuch.dk
CVR	33 55 94 37

Bilag C – HOSTEUROPE

CO2-
neutrales
Hosting
Host Europe GmbH
Hansestr. 111 · 51149 Köln
www.hosteurope.de · info@hosteurope.de
Bankverbindungen
DE: Commerzbank Köln
BIC: COBADEFF370 · IBAN: DE35 3704 0044 0502 1985 00
CH: PostFinance Basel/Bern · Kto.-Nr. 91-181312-4 (EUR)
IBAN: CH55 0900 0000 9118 1312 4
Geschäftsführer:
Dr. Christian Koch
Jonathan Wong
Tim Montag
Amtsgericht Köln:
HRB 28495
USt-IdNr.:
DE187370678

Order Processing in accordance with Article 28 General Data Protection Regulation (GDPR) Agreement

1. Subject matter (Art. 28 (1) GDPR)

1.1 The subject matter of the contract is the provision of web hosting services or one (or more) dedicated web server(s) as well as the associated services such as e-mail, domain registration, etc. Within the scope of this contract, the client has – depending on the agreed scope of services – the possibility of processing (storing, modifying, transmitting and deleting data) using e.g. a web server, FTP server or SSH access.

1.2 The subject matter of the contract is **not** the original use or processing of personal data by the supplier. However, access to personal data cannot be ruled out in the course of the clients' performance as a central IT service provider in the area of hosting, support or administration of the client

1.3 Details can be found in the main contract(s) summarized under the named customer number. The agreement applies to the entire service relationship, insofar as the services described in section 1.1 are concerned.

1.4 Insofar as data is mentioned below, personal data in the scope of GDPR is meant. The following data protection and data security regulations apply to all services of the commissioned data processing in accordance with Art. 28

1.5 **In addition** to the contract(s) concluded between the parties, the contracting parties specify the general obligations how the personal data of the client should be processed.

2. Duration, Completion, Erasure of data (Art. 28 (1) GDPR)

2.1 The duration of the contract depends on the duration of the hosting services provided by the supplier to the client. The order ends if the client does not use any hosting services of the supplier according to the specific service agreements/offers.

2.2 The rights of data subjects, especially with regard to rectification, deletion and blocking, shall be asserted against the client. The client is solely responsible for the protection of these rights.

2.3 After conclusion of the contracted work, or earlier upon request by the client, at the latest upon termination of the Service Agreement, the supplier shall hand over to the client or – subject to prior consent – destroy all documents, processing and utilization results, and data sets related to the contract that have come into its possession in a data protection compliant manner. The same applies to any and

all connected test, waste, redundant and discarded material. The log of the destruction or deletion shall

be provided on request. If additional costs are incurred due to deletion prior to termination of the contract, these shall be borne by the client.
2.4 The supplier shall be obliged to forward any requests by data subjects concerning the processing of personal data to the client without any delay. The supplier is not entitled to handle those requests on its own initiative without consultation with the client.
2.5 The supplier shall assist the client in the implementation of the data subjects rights under the scope of chapter III of GDPR, in particular with regard to rectification, blocking and deletion, notification and provision of information, within the limits of technical possibilities, especially with regard to the nature of the provided service.
2.6 Because there is no exchange of medium in accordance with Art. 28 (3) lit. g GDPR between the parties, there is no need to regulate a return.

3. Scope, nature and purpose of the intended collection, processing and/or use of data

3.1 The scope, type and purpose of the intended collection, processing and/or use of the data result from the service agreement between the parties.
The supplier is obliged to use the personal data exclusively for the contractually agreed services. The supplier is permitted to create intermediate, temporary or duplicate files necessary for procedural and safety reasons (including backups) for the collection, processing and / or use of the personal data, as far as this does not lead to a redesign of the content. The supplier is not permitted to make unauthorized copies of personal data.
The client shall inform the supplier without delay if it finds errors or irregularities in the examination of the contractual results.
Data from address books and directories may only be used to communicate with the client within the framework of fulfilling the order. Any other use and transmission of the processed data for own or third party purposes, including marketing purposes, is not permitted.
3.2 The undertaking of the contractually agreed Processing of Data shall be carried out within the Federal Republic of Germany, in a Member State of the European Union (EU), in a Member State of the

European Economic Area (EEA), or in non-member states under the condition that the specific requirements of the GDPR have been fulfilled.

4. Type of data and group of data subjects (Art. 28 (3) 1 GDPR)

4.1 Type of data

The following data types are the subject matter of the collection, processing and/or use of the client's data in accordance with section 1.2. sentence 2:
(to be filled out completely and correctly by the client!)
□-Person master data
□-Communications data (e.g. telephone, e-mail)
□-Contract master data (contractual relation, interest in products/contracts)
□-Customer history
□-Contract billing data
□-Disclosure data (from third parties, e.g. credit agencies, from public directories)
□-Other data: _____

4.2 Group of data subject

The group of data subject according to section 1.2 sentence 2 includes:
(to be filled out completely and correctly by the client!)
□-Customers
□-Interested people
□-Subscribers
□-Employees
□-Suppliers
□-Sales agents
□-Contact persons
□-Other data subjects: _____

5. Obligations of the suppliers

5.1 General obligations Art. 28-33 GDPR

5.1.1 The supplier (Host Europe GmbH) undertakes to place a written order with a data protection officer, who can carry out his work in accordance with Art. 37, 38 GDPR. The contact details will be communicated to the client on request for the purpose of direct contact.

5.1.2 Insofar as collection, processing and / or use of the data is carried out by the supplier, this is only permissible within the framework of the contractual agreements between the client and the supplier. Insofar as the supplier has access to data of the client, he shall not use such data for purposes other than those stipulated in the contract, in particular he shall only pass them on to third parties insofar as there is a legal or contractual obligation to do so. Copies of data may only be made with the consent of the client. This does not apply to backup copies, insofar as they are necessary to guarantee proper data processing or fulfilment of contractual or legal obligations.

5.1.3 The contractor shall ensure that confidentiality is maintained in accordance with Art. 28 (3) S. 2 lit. b, 29, 32 (4) GDPR. All persons who could access the client's data listed in point 4.1 in accordance with the order must be obliged to maintain confidentiality and must be informed of the special data protection obligations resulting from this order as well as the existing instruction or earmarking of purpose.

5.1.4 The supplier shall ensure the implementation and adherence to all technical and organisational measures necessary for this order in accordance with Art. 32 GDPR.

5.1.5 The supplier shall inform the client without delay in the event of breaches of data protection regulations committed by the supplier or persons employed by him. The same shall apply in the event of serious disruptions to the course of business or other irregularities in the handling of the client's data. To the extent that the client is subject to obligations pursuant to Art. 32 and 33 GDPR, the supplier shall assist him in this respect. Insofar as the client fulfils obligations pursuant to Art. 32-36 GDPR, e.g. in the event of loss or unlawful transmission or knowledge of personal data by third parties, the supplier shall support the client within the scope of the character of the service provided by the supplier.

5.2 Technical and organisational measures (Art. 32 GDPR)

5.2.1 Before the commencement of processing, the supplier shall document the execution of the necessary technical and organisational measures, set out in advance of the awarding of the order or

contract, specifically with regard to the client for inspection. Upon acceptance by the client, the documented measures become the foundation of the contract. Insofar as the inspection/audit by the client shows the need for amendments, such amendments shall be implemented by mutual agreement.

5.2.2 The Technical and Organisational Measures are subject to technical progress and further development. In this respect, it is permissible for the Supplier to implement alternative adequate measures. In so doing, the security level of the defined measures must not be reduced. The supplier shall establish the security in accordance with Article 28 (3) lit. c and Article 32 GDPR in particular in conjunction with Article 5 (1), and (2) GDPR. The measures to be taken are measures of data security and measures that guarantee a protection level appropriate to the risk concerning confidentially, integrity, availability and resilience of the systems. Substantial changes must be documented.

6. Subcontracting (Art. 28 (2), (4) GDPR)

6.1 The Client agrees to the supplier's commissioning of its affiliated companies or of subcontractor companies for the purpose of fulfilling its contractually agreed services. Subcontracting for the purpose of this Agreement is to be understood as services which relate directly to the provision of the principal service. This does not include ancillary services, such as telecommunication services, postal / transport services, maintenance and user support services or the disposal of data carriers, as well as other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing equipment. The supplier reserves the right to commission subcontractors in the regions according to section 3.2 of this Agreement.

6.2 The supplier shall ensure that a list of the subcontractors it deploys is made available to client for retrieval and review, whether it be in the customer portal, as part of this contractual agreement, or in some other manner that is communicated to the client. The Client acknowledges the commission of the mentioned subcontractors. The Client will be informed about changes, additions or removals to the list. These changes shall be considered accepted, should the Client not dissent within 4 weeks after publishing.

6.3 If the supplier issues orders to subcontractors, it is incumbent upon the supplier to transfer its obligations under this contract to the subcontractor.

7. Obligations of the client (Art. 24, 13, 14 GDPR)

7.1 The client is responsible for compliance with the relevant data protection regulations.

7.2 The client shall inform the supplier immediately of any breaches of the supplier's data protection regulations.

7.3 The client shall be subject to the information obligations resulting from Art. 24 GDPR and Art. 13, 14 GDPR.

8. Authority of the client to issue instructions, rectification, restriction and erasure of data, rights of data subject (Art. 29, 28 GDPR as well as chapter III of GDPR)

8.1 The client has comprehensive access to the data at any time, so that it is not necessary for the supplier to cooperate with the client, in particular with regard to correction, blocking, deletion, etc. Insofar as it is necessary for the supplier to cooperate, the client shall be obliged to do so against reimbursement of the costs incurred. In this case, the client shall have a comprehensive right to issue instructions on the type, scope and procedures of data processing pursuant to Art. 29 in conjunction with Art. 28 GDPR. The supplier shall inform the client immediately if she is of the opinion that an instruction violates data protection regulations. The supplier is entitled to suspend the execution of the corresponding instruction until it has been confirmed or changed by the person responsible at the client.

8.2 Insofar as a data subject contacts the supplier directly concerning a rectification, erasure, or restriction of processing, the supplier will immediately forward the data subject's request to the client. If the client is obliged by applicable data protection laws to provide information on the collection, processing and/or use of data, the client shall assist the client in providing such information to the necessary extent. The client must send a request to the supplier in writing and reimburse him for the costs incurred in this connection.

9. Supervisory powers of the clients

9.1 The client has the right to convince himself of the compliance with the technical and organisational measures taken by the contractor before the beginning of the data processing and then regularly.

9.2 For this purpose, the client shall be provided with the documentation on the existing technical and organisational measures prepared by the contractor's data protection officer, which is regularly revised and according to the legal requirements.

Attachment:
Technical and organisational measures
List of subcontractors

Bilag D – Sendgrid/Twilio tillægsaftale

DATA PROTECTION ADDENDUM

Effective: July 16, 2020

This Data Protection Addendum ("***Addendum***") supplements the agreement between Customer and Twilio into which it is incorporated by reference ("***Agreement***").

I. Introduction

1. **Definitions.**

. ***"Applicable Data Protection Law***" refers to all laws and regulations applicable to Twilio's processing of personal data under the Agreement including, without limitation, the General Data Protection Regulation (EU 2016/679) ("***GDPR***").
. ***"controller"***, "***processor***", "***data subject***", "***personal data,***" and "***processing***" (and "***process***") have the meanings given in accordance with Applicable Data Protection Law.
. ***"Customer Account Data"*** means personal data that relates to Customer's relationship with Twilio, including the names and/or contact information of individuals authorized by Customer to access Customer's account and billing information of individuals that Customer has associated with its account. Customer Account Data also includes any data Twilio may need to collect for the purpose of identity verification, or as part of its legal obligation to retain subscriber records.
. ***"Customer Content"*** means (a) personal data exchanged by means of use of the Services, such as text, message bodies, voice and video media, images, email bodies, email recipients, and sound, and (b) data stored on Customer's behalf such as communication logs within the Services or marketing campaign data Customer has uploaded to the SendGrid Services.
. ***"Customer Data"*** has the meaning given in the Agreement. Customer Data includes Customer Account Data, Customer Usage Data, Customer Content and Sensitive Data, as defined in this Agreement.
. ***"Customer Usage Data"*** means data processed by Twilio for the purposes of transmitting or exchanging Customer Content; including data used to identify the source and destination of a communication, such as (a) individual data subjects' telephone numbers, data on the location of the device generated in the context of providing the Services, and the date, time, duration and the type of communication; and (b) activity logs used to identify the source of Service requests, optimize and maintain performance of the Services, and investigate and prevent system abuse.
. ***"Swiss-US Privacy Shield Framework"*** means the Swiss-US Privacy Shield self-certification program operated by the US Department of Commerce.
. ***"Privacy Shield Principles"*** means the Privacy Shield Framework Principles (as supplemented by the Supplemental Principles).
. ***"Security Incident"*** means a confirmed or reasonably suspected accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data.
. ***"SendGrid Services"*** means the services enabling companies to develop, transmit, analyze, and manage email communications and other related digital communications and tools through the

website at http://www.sendgrid.com, including all programs, features, functions and report formats, and subsequent updates or upgrades of any of the foregoing made generally available by Twilio, and excluding any Twilio Services.
. ***"Sensitive Data"*** has the meaning given in the Twilio Acceptable Use Policy available at https://www.twilio.com/legal/aup, which may be updated from time to time as stated in the AUP.
. ***"Twilio Services"*** means the products and services that are ordered by Customer under an Order Form or by using the Twilio account, or provided by Twilio to Customer on a trial basis or otherwise free of charge. As of the Effective Date, Twilio Services generally consist of: (a) platform services, namely access to the Twilio application programming interface (referred to herein as Twilio APIs) and, where applicable, (b) connectivity services, that link the Twilio Services to the telecommunication providers' networks via the Internet. The Twilio Services excludes any SendGrid Services.
Any capitalized term used but not defined in this Addendum has the meaning provided to it in the Agreement.

II. Controller and Processor

2. Relationship of the Parties.

2.1 Twilio as a Processor: The parties acknowledge and agree that with regard to the processing of Customer Content, Customer may act either as a controller or processor and Twilio is a processor.

2.2 Twilio as a Controller of Customer Account Data: The parties acknowledge that, with regard to the processing of Customer Account Data, Customer is a controller and Twilio is an independent controller, not a joint controller with Customer.

2.3 Twilio as a Controller of Customer Usage Data: The parties acknowledge that, with regard to the processing of Customer Usage Data, Customer may act either as a controller or processor and Twilio is an independent controller, not a joint controller with Customer.

3. Purpose Limitation. Twilio will process personal data in order to provide the Services in accordance with the Agreement. Section 2.1 of Schedule 1 further specifies the duration of the processing, the nature and purpose of the processing, and the types of personal data and categories of data subjects. Twilio will process Customer Content in accordance with Customer's instructions as outlined in Section 5. Twilio will process Customer Account Data and Customer Usage Data in accordance with Applicable Data Protection Law and consistent with the Privacy Policy, the Agreement, and this Addendum.

4. Compliance. Customer is responsible for ensuring that (a) it has complied, and will continue to comply, with Applicable Data Protection Law in its use of the Services and its own processing of personal data; and (b) it has, and will continue to have, the right to transfer, or provide access to, the personal data to Twilio for processing in accordance with the terms of the Agreement and this Addendum.

III. Twilio as a Processor - Processing Customer Content

5. Customer Instructions. Customer appoints Twilio as a processor to process Customer Content on behalf of, and in accordance with, Customer's instructions (a) as set forth in the Agreement, this Addendum, and as otherwise necessary to provide the Services to Customer (which may include investigating security incidents and preventing spam or fraudulent activity, and detecting and preventing network exploits and abuse); (b) as necessary to comply with applicable law; and (c) as otherwise agreed in writing by the parties ("***Permitted Purposes***").

5.1 Lawfulness of Instructions.Customer will ensure that its instructions comply with Applicable Data Protection Law. Customer will ensure that its instructions relating to Twilio's processing of the Customer Content will not cause Twilio to violate any applicable law, regulation, or rule, including Applicable Data Protection Law. Twilio will inform Customer if it becomes aware or reasonably believes that Customer's data processing instructions violate any applicable law, regulation, or rule, including Applicable Data Protection Law.

5.2 Additional Instructions. Additional instructions outside the scope of the Agreement, an Order Form, or this Addendum will be agreed to between the parties in writing, including any additional fees that may be payable by Customer to Twilio for carrying out those instructions.

6. Confidentiality.

6.1 Responding to Third Party Requests. In the event that any request, correspondence, enquiry or complaint from a data subject, regulatory authority, or third party is made directly to Twilio in connection with Twilio's processing of Customer Content, Twilio will promptly inform Customer and provide details of the same, to the extent legally permitted. Unless legally obligated to do so, Twilio will not respond to any such request, inquiry, or complaint without Customer's prior consent except to confirm that the request relates to Customer.

6.2 Confidentiality Obligations of Twilio Personnel.Twilio will ensure that any person it authorizes to process the Customer Content has agreed to protect personal data in accordance with Twilio's confidentiality obligations under the Agreement.

7. Sub-processing.

7.1 Sub-processors. Customer agrees that Twilio may use sub-processors to fulfill its contractual obligations under the Agreement. Where Twilio authorizes any sub-processor as described in this Section 7, Twilio agrees to impose data protection terms on any sub-processor it appoints that require it to protect the Customer Content to the standard required by Applicable Data Protection Law, such as including the same data protection obligations referred to in Article 28(3) of the GDPR, in particular providing sufficient

guarantees to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of the GDPR.

7.2 General Consent for Onward Sub-processing. Customer provides a general consent for Twilio to engage onward sub-processors, conditional on the following requirements:

(a) Any onward sub-processor must agree in writing to only process data in a country that the European Commission has declared to have an "adequate" level of protection; or to only process data on terms equivalent to the Standard Contractual Clauses, or pursuant to a Binding Corporate Rules approval granted by competent European data protection authorities; and
(b) Twilio will restrict the onward sub-processor's access to personal data only to what is strictly necessary to provide the Services, and Twilio will prohibit the sub-processor from processing the personal data for any other purpose.

7.3 Current Sub-processors and Notification of New Sub-processors. If Twilio Ireland Limited or Twilio Japan G.K. is the Twilio party to the Agreement, then Customer consents to Twilio engaging Twilio Inc. as a sub-processor, which has its primary processing facilities in the United States of America. Customer consents to Twilio engaging additional third party sub-processors to process Customer Content within the Services for the Permitted Purposes provided that Twilio maintains an up-to-date list of its sub-processors for the Twilio Services at https://www.twilio.com/legal/sub-processors and for the SendGrid Services at https://sendgrid.com/policies/privacy/sub-processors, which each contain a mechanism for Customer to subscribe to notifications of new sub-processors. If Customer subscribes to such notifications, Twilio will provide details of any change in sub-processors as soon as reasonably practicable. With respect to changes in infrastructure providers, Twilio will endeavor to give notice sixty (60) days prior to any change, but in any event will give notice no less than thirty (30) days prior to any such change. With respect to Twilio's other sub-processors, Twilio will endeavor to give notice thirty (30) days prior to any change, but will give notice no less than ten (10) days prior to any such change.

7.4 Objection Right for new Sub-processors. Customer may object to Twilio's appointment or replacement of a sub-processor prior to its appointment or replacement, provided such objection is in writing and based on reasonable grounds relating to data protection. In such event, the parties agree to discuss commercial reasonable alternative solutions in good faith. If the parties cannot reach a resolution within ninety (90) days, Customer may suspend or terminate the affected service in accordance with the termination provisions of the Agreement. Such termination will be without prejudice to any fees incurred by Customer prior to suspension or termination. If no objection has been raised prior to Twilio replacing or appointing a new a sub-processor, Twilio will deem Customer to have authorized the new sub-processor.

7.5 Sub-processor Liability. Twilio will remain liable for any breach of this Addendum that is caused by an act, error or omission of its sub-processors.

8. Data Subject Rights.

8.1 Twilio Services. As part of the Twilio Services, Twilio provides Customer with a number of self-service features, including the ability to delete, obtain a copy of, or restrict use of Customer Content, which may be used by Customer to assist in complying with its obligations under Applicable Data Protection Law with respect to responding to requests from data subjects via the Twilio Services at no additional cost. In addition, upon Customer's request, Twilio will provide reasonable additional and timely assistance (at Customer's expense only if complying with the Customer's request will require Twilio to assign significant resources to that effort) to assist Customer in complying with its data protection obligations with respect to data subject rights under Applicable Data Protection Law.

8.2 SendGrid Services. Twilio will, taking into account the nature of the processing, provide reasonable assistance to Customer to the extent possible to enable Customer to respond to requests from a data subject seeking to exercise its rights under Applicable Data Protection Law with respect to Customer Content being processed via the SendGrid Services.

9. Impact Assessments and Consultations. Twilio will provide reasonable cooperation to Customer in connection with any data protection impact assessment (at Customer's expense only if such reasonable cooperation will require Twilio to assign significant resources to that effort) or consultations with regulatory authorities that may be required in accordance with Applicable Data Protection Law.

10. Return or Deletion of Customer Content. Twilio will, in accordance with Section 2 of Schedule 1, delete or return to Customer any Customer Content stored in the Services.

10.1 Extension of Addendum. Upon termination of the Agreement, Twilio may retain Customer Content in storage for the time periods set forth in Schedule 1, provided that Twilio will ensure that Customer Content is processed only as necessary for the Permitted Purposes, and Customer Content remains protected in accordance with the terms of the Agreement, this Addendum, and Applicable Data Protection Law.

10.2 Retention Required by Law. Notwithstanding anything to the contrary in this Section 10, Twilio may retain Customer Content or any portion of it if required by applicable law, provided that it remains protected in accordance with the terms of the Agreement, this Addendum, and Applicable Data Protection Law.

IV. Security and Audits

11. Security Measures. Twilio has implemented and will maintain appropriate technical and organizational measures to protect personal data from a Security Incident. Measures to protect Customer Content from a Security Incident are provided in the Security Overview referenced in Appendix 2. Additional information about the technical and organizational security measures involving (a) the Twilio Services are described at https://www.twilio.com/security and (b) the SendGrid Services are described at https://sendgrid.com/policies/security.

11.1 Determination of Security Requirements: Customer acknowledges that the Services include certain features and functionalities that Customer may elect to use that impact the security of the data processed by Customer's use of the Services, such as, but not limited to, encryption of voice recordings and availability of multi-factor authentication on Customer's Services account or optional TLS encryption within the SendGrid Services. Customer is responsible for reviewing the information Twilio makes available regarding its data security, including its audit reports, and making an independent determination as to whether the Services meet the Customer's requirements and legal obligations, including its obligations under Applicable Data Protection Law. Customer is further responsible for properly configuring the Services and using features and functionalities made available by Twilio to maintain appropriate security in light of the nature of the data processed by Customer's use of the Services.

11.2 Security Incident Notification: Twilio will provide notification of a Security Incident in the following manner:

a. Twilio will, to the extent permitted by applicable law, notify Customer without undue delay, but in no event later than seventy-two (72) hours after, Twilio's confirmation or reasonable suspicion of a Security Incident impacting Customer Data of which Twilio is a processor;
b. Twilio will, to the extent permitted and required by applicable law, notify Customer without undue delay of any Security Incident involving Customer Data of which Twilio is a controller; and
c. Twilio will notify the email address of Customer's account owner.

Twilio will make reasonable efforts to identify and, to the extent such Security Incident is caused by a violation of the requirements of this Addendum by Twilio, remediate the cause of such Security Incident. Twilio will provide reasonable assistance to Customer in the event that Customer is required under Applicable Data Protection Law to notify a regulatory authority or any data subjects of a Security Incident.

12. Audits. The parties acknowledge that Customer must be able to assess Twilio's compliance with its obligations under Applicable Data Protection Law and this Addendum, insofar as Twilio is acting as a processor on behalf of Customer.

12.1 Twilio's Audit Program: Twilio uses external auditors to verify the adequacy of its security measures with respect to its processing of Customer Content. Such audits are performed at least once annually at Twilio's expense by independent third party security professionals at Twilio's selection and result in the generation of a confidential audit report ("***Audit Report***"). A description of Twilio's certifications and/or standards for audit of the (a) Twilio Services can be found at https://www.twilio.com/security; and (b) SendGrid Services can be found at https://sendgrid.com/policies/security.

12.2 Customer Audit: Upon Customer's written request at reasonable intervals, and subject to reasonable confidentiality controls, Twilio will make available to Customer a copy of Twilio's most recent Audit Report. Customer agrees that any audit rights granted by Applicable Data Protection Law (including, where applicable, Article 28(3) of the GDPR or Clauses 5(f) and 12(2) of the Standard Contractual Clauses) will be satisfied by these

Audit Reports. To the extent that Twilio's provision of an Audit Report does not provide sufficient information or to the extent that Customer must respond to a regulatory authority audit, Customer agrees to a mutually agreed-upon audit plan with Twilio that: (a) ensures the use of an independent third party; (b) provides notice to Twilio in a timely fashion; (c) requests access only during business hours; (d) accepts billing to Customer at Twilio's then-current rates unless Customer is on Twilio's Enterprise Edition; (e) occurs no more than once annually; (f) restricts its findings to only data relevant to Customer; and (g) obligates Customer, to the extent permitted by law, to keep confidential any information gathered that, by its nature, should be confidential.

V. International Provisions

13. Processing in the United States. Customer acknowledges that, as of the Effective Date of this Addendum, Twilio's primary processing facilities are in the United States of America.

14. Cross Border Data Transfer Mechanisms for Data Transfers. To the extent that Customer's use of the Twilio Services requires transfer of personal data out of the European Economic Area ("***EEA***"), Switzerland, or a jurisdiction set forth in Schedule 4, then Twilio will take such measures as are necessary to ensure the transfer is in compliance with Applicable Data Protection Law.

14.1 Order of Precedence. In the event that the Services are covered by more than one transfer mechanism, the transfer of personal data will be subject to a single transfer mechanism in accordance with the following order of precedence: (a) Twilio's binding corporate rules as set forth in Section 14.2; (b) Swiss–US Privacy Shield Framework self-certifications as set forth in Section 14.3; and (c) the Standard Contractual Clauses as set forth in Section 14.4.

14.2 Twilio BCRs - Twilio Services. The parties agree that Twilio will process personal data in the Twilio Services in accordance with Twilio's Binding Corporate Rules as set forth at https://www.twilio.com/legal/binding-corporate-rules ("***Twilio BCRs***"). The parties further agree that, with respect to the Twilio Services, the Twilio BCRs will be the lawful transfer mechanism of Customer Account Data, Customer Content and Customer Usage Data from the EEA, Switzerland, or the United Kingdom to Twilio in the United States, or any other non-EEA Twilio entity subject to the binding corporate rules. For avoidance of doubt, the Twilio BCRs do not apply to SendGrid Services.

14.3 Swiss-US Privacy Shield. To the extent Twilio processes (or causes to be processed) any personal data via the Services originating from Switzerland Twilio represents that it is self-certified to the Privacy Shield Framework and agrees that it will comply with the Privacy Shield Principles when handling any such data. To the extent that Customer is (a) located in the United States of America and is also self-certified to the Swiss-US Privacy Shield Framework or (b) located in Switzerland, Twilio further agrees to (x) provide at least the same level of protection to such data as is required by the Privacy Shield Principles; (y) notify Customer without undue delay if its self-certification to the Swiss-US

Privacy Shield Framework is withdrawn, terminated, revoked, or otherwise invalidated and to cooperate in good faith to put in place such alternative data export mechanisms as are required under Applicable Data Protection Law; and (z) upon notice, to work with Customer to take reasonable and appropriate steps to stop and remediate any unauthorized processing of personal data.

14.4 Standard Contractual Clauses. This Addendum hereby incorporates by reference (a) the Standard Contractual clauses for data controller to data processor transfers approved by the European Commission in decision 2010/593/EU, provided that Appendices 1 and 2 of the Standard Contractual Clauses are set forth in Schedule 2 to this Addendum; and (b) the Standard Contractual Clauses for data controller to data controller transfers approved by the European Commission in decision 2004/915/EC, provided that Annex B of the Standard Contractual Clauses are set forth in Schedule 3 to this Addendum. The parties further agree that the Standard Contractual Clauses will apply to personal data that is transferred via the Services from the European Economic Area, the United Kingdom, and/or Switzerland to outside the European Economic Area, the United Kingdom, and Switzerland, either directly or via onward transfer, to any country or recipient: (x) not recognized by the European Commission as providing an adequate level of protection for personal data (as described in the EU Data Protection Directive) and (y) not covered by the Twilio BCRs or by the Swiss-US Privacy Shield certification.

15. Jurisdiction Specific Terms. To the extent Twilio processes personal data originating from and protected by Applicable Data Protection Law in one of the jurisdictions listed in Schedule 4, then the terms specified in Schedule 4 with respect to the applicable jurisdiction(s) ("***Jurisdiction Specific Terms***") apply in addition to the terms of this Addendum. In case of any conflict or ambiguity between the Jurisdiction Specific Terms and any other terms of this Addendum, the applicable Jurisdiction Specific Terms will take precedence.

VI. Miscellaneous

16. Cooperation and Data Subject Rights. In the event that either party receives: (a) any request from a data subject to exercise any of its rights under Applicable Data Protection Law (including its rights of access, correction, objection, erasure and data portability, as applicable) or (b) any other correspondence, enquiry, or complaint received from a data subject, regulator or other third party, (collectively, "***Correspondence***") then, where such Correspondence relates to processing of Customer Account Data or Customer Usage Data conducted by the other party, it will promptly inform such other party and the parties agree to cooperate in good faith as necessary to respond to such Correspondence and fulfill their respective obligations under Applicable Data Protection Law.

17. Sensitive Data. Customer is responsible for ensuring that suitable safeguards are in place prior to transmitting or processing any Sensitive Data over the Services, or prior to permitting End Users to transmit or process Sensitive Data over the Services.

18. Failure to Perform. In the event that changes in law or regulation render performance of this Addendum impossible or commercially unreasonable, the Parties may renegotiate this Addendum in good faith. If renegotiation would not cure the impossibility, or the Parties cannot reach an agreement, the Parties may terminate the Agreement in accordance with the Agreement's termination provisions.

19. Notification Cooperation. Customer acknowledges that Twilio, as a controller, may be required by Applicable Data Protection Law to notify the regulatory authority of Security Incidents involving Customer Usage Data. If the regulatory authority requires Twilio to notify impacted data subjects with whom Twilio does not have a direct relationship (e.g., Customer's end users), Twilio will notify Customer of this requirement. Customer will provide reasonable assistance to Twilio to notify the impacted data subjects.

20. GDPR Penalties. Notwithstanding anything to the contrary in this Addendum or in the Agreement (including, without limitation, either party's indemnification obligations), neither party will be responsible for any GDPR fines issued or levied under Article 83 of the GDPR against the other party by a regulatory authority or governmental body in connection with such other party's violation of the GDPR.

21. Conflict. If there is any conflict between this Addendum and the Agreement and/or Privacy Policy, then the terms of this Addendum will control. Any claims brought in connection with this Addendum will be subject to the terms and conditions, including but not limited to, the exclusions and limitations set forth in the Agreement.

22. Updates. Twilio may update the terms of this Data Protection Addendum from time to time; provided, however, Twilio will provide at least thirty (30) days prior written notice to Customer when an update is required as a result of (a) changes in Applicable Data Protection Law; (b) a merger, acquisition, or other similar transaction; or (c) the release of new products or services or material changes to any of the existing Services.

SCHEDULE 1
DETAILS OF PROCESSING

1. Nature and Purpose of the Processing. Twilio will process personal data as necessary to provide the Services under the Agreement. Twilio does not sell Customer's personal data or Customer end users' personal data and does not share such end users' information with third parties for compensation or for those third parties' own business interests.

1.1 Customer Content. Twilio will process Customer Content in accordance with Section 5 of the Addendum.

1.2 Customer Account Data. Twilio will process Customer Account Data as a controller (a) in order to manage the relationship with Customer; (b) carry out Twilio's core business operations, such as accounting and filing taxes; and (c) in order to detect, prevent, or investigate security incidents, fraud and other abuse and/or misuse of the Services.

1.3 Customer Usage Data. Twilio will process Customer Usage Data as a controller in order to carry out necessary functions as a communications service provider including, but not limited to, (a) Twilio's accounting, tax, billing, audit, and compliance purposes; (b) to provide, optimize, and maintain the services and platform and security; (c) to investigate fraud, spam, wrongful or unlawful use of the Services; and/or (c) as required by applicable law.

2. Duration of the Processing.

2.1 Customer Content**.**

a. Twilio Services**.** Prior to the termination of the Agreement, Twilio will process stored Customer Content for the Permitted Purposes until Customer elects to delete such Customer Content via the Twilio Services. Prior to the termination of this Agreement, Customer agrees that it is solely responsible for deleting Customer Content via the Twilio Services. Upon termination of the Agreement, Twilio will (i) provide Customer thirty (30) days after the termination effective date to obtain a copy of any stored Customer Content via the Twilio Services; (ii) automatically delete any stored Customer Content thirty (30) days after the termination effective date; and (iii) automatically delete any stored Customer Content on Twilio's back-up systems sixty (60) days after the termination effective date. Any Customer Content archived on Twilio's back-up systems will be securely isolated and protected from any further processing, except as otherwise required by applicable law.
b. SendGrid Services. Upon termination of the Agreement, Twilio will (a) at Customer's election, delete or return to Customer the Customer Content (including copies) stored in the SendGrid Services and (b) automatically delete any stored Customer Content on Twilio's back-up systems one (1) year after the termination effective date.

2.2 Customer Account Data. Twilio will process Customer Account Data as long as needed to provide the Services to Customer as required for Twilio's legitimate business needs, or as required by law. Customer Account Data will be stored in accordance with Twilio's Privacy Policy.

2.3 Customer Usage Data. Upon termination of the Agreement, Twilio may retain, use, and disclose Customer Usage Data for the purposes set forth in Section 1.3 of this Schedule, subject to the confidentiality obligations set forth in the Agreement. Twilio will anonymize or delete Customer Usage Data when Twilio no longer requires it for the purposes set forth in Section 1.3 of this Schedule 1.

3. Categories of Data Subjects.

3.1 Customer Content. Customer's end users.

3.2 Customer Account Data. Customer's employees and individuals authorized by Customer to access Customer's Twilio account or make use of Customer's telephone number assignments received from Twilio.

3.3 Customer Usage Data. Customer's end users.

4. Type of Personal Data. Twilio processes personal data contained in Customer Account Data, Customer Content, and Customer Usage Data as defined in the Addendum.

SCHEDULE 2
APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter

The data exporter is the Customer and the user of the Services.

Data importer

The data importer is Twilio Inc, a provider of (a) business communications services that enable communications features and capabilities to be embedded into web, desktop and mobile software applications; and (b) cloud-based transactional and marketing email delivery, management and analytics services.

Data subjects

The personal data transferred concern the following categories of data subjects:

Data exporter's end-users. The data importer will receive any personal data in the form of Customer Content that the data exporter instructs it to process through its cloud communications products and services. The precise personal data that the data exporter will transfer to the data importer is necessarily determined and controlled solely by the data exporter.

Categories of data

The personal data transferred concern the following categories of data (please specify):

Customer Content: As defined in Section 1 of this Addendum.

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data (please specify):

Twilio does not intentionally collect or process any special categories of data in the provision of its products or services.

However, special categories of data may from time to time be processed through the Services where the data exporter or its end users choose to include this type of data

within the communications it transmits using the Services. As such, the data exporter is solely responsible for ensuring the legality of any special categories of data it or its end users choose to process using the Services.

Processing operations

The personal data transferred will be subject to the following basic processing activities (please specify):

For the Twilio Services, the provision of programmable communication products and services, primarily offered in the form of APIs, on behalf of the data exporter, including transmittal to or from data exporter's software application from or to the publicly-switched telephone network (PSTN) or by way of other communications networks.

For the SendGrid Services, the provision of products and services which allow the sending and delivering email communications on behalf of the data exporter to its recipients. Twilio will also provide the data exporter with analytic reports concerning the email communications it sends on the data exporter's behalf.

Storage on Twilio's network.

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organizational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or documentation/legislation attached):

See Twilio Security Overview available at www.twilio.com/legal/security-overview

SCHEDULE 3
ANNEX B TO THE STANDARD CONTRACTUAL CLAUSES

DESCRIPTION OF THE TRANSFER

This Annex forms part of the Standard Contractual Clauses and must be completed and signed by the parties.

Data Subjects

The personal data transferred concern the following categories of data subjects:

Data exporter and data exporter's end users.

Purposes of the Transfer(s)

The transfer is made for the following purposes:

The provision of cloud communication services.

and

For provision of a portion of the Twilio Services under which data exporter adds an additional factor for verification of data exporter's end users' identity in connection with such end users' use of data exporter's software applications or services ("***2 Factor Authentication Services***")

Categories of data

The personal data transferred concern the following categories of data:

1. Personal data transferred by data exporter to data importer to provide 2 Factor Authentication Services, namely data subjects' telephone numbers and email addresses and any other personal data provided by the data exporter and/or needed for authentication purposes.
2. Customer Account Data: As defined in Section 1 of the Addendum.
3. Customer Usage Data: As defined in Section 1 of the Addendum.

Recipients

The personal data transferred may only be disclosed to the following recipients or categories of recipients:

- Employees, agents, affiliates, advisors and independent contractors of data importer with a reasonable business purpose for needing such personal data
- Vendors of data importer that, in their performance of their obligations to data importer, must process such personal data acting on behalf of and according to instructions from data importer.
- Any person (natural or legal) or organization to whom data importer may be required by applicable law or regulation to disclose personal data, including law enforcement authorities, central and local government.

Sensitive data

N/A

Data protection registration of the data exporter

_____

SCHEDULE 4
JURISDICTION SPECIFIC TERMS

1. **Australia:**

1.1. The definition of "Applicable Data Protection Law" includes the Australian Privacy Principles and the Australian Privacy Act (1988).
1.2. The definition of "personal data" includes "Personal Information" as defined under Applicable Data Protection Law.
1.3. The definition of "Sensitive Data" includes "Sensitive Information" as defined under Applicable Data Protection Law.

2. California:

2.1 The definition of "Applicable Data Protection Law" includes the California Consumer Privacy Act (CCPA).
2.2 The definition of "personal data" includes "Personal Information" as defined under Applicable Data Protection Law and, for clarity, includes any Personal Information contained within Customer Account Data, Customer Content, and Customer Usage Data.
2.3 The definition of "data subject" includes "Consumer" as defined under Applicable Data Protection Law. Any data subject rights, as described in Section 8 of the Addendum, apply to Consumer rights. In regards to data subject requests, Twilio can only verify a request from Customer and not from Customer's end user or any third party.
2.4 The definition of "controller" includes "Business" as defined under Applicable Data Protection Law.
2.5 The definition of "processor" includes "Service Provider" as defined under Applicable Data Protection Law.
2.6 Twilio will process, retain, use, and disclose personal data only as necessary to provide the Services under the Agreement, which constitutes a business purpose. Twilio agrees not to (a) sell (as defined by the CCPA) Customer's personal data or Customer end users' personal data; (b) retain, use, or disclose Customer's personal data for any commercial purpose (as defined by the CCPA) other than providing the Services; or (c) retain, use, or disclose Customer's personal data outside of the scope of the Agreement. Twilio understands its obligations under the Applicable Data Protection Law and will comply with them.
2.7 Twilio certifies that its sub-processors, as described in Section 7 of the Addendum, are Service Providers under Applicable Data Protection Law, with whom Twilio has entered into a written contract that includes terms substantially similar to this Addendum. Twilio conducts appropriate due diligence on its sub-processors.
2.8 Twilio will implement and maintain reasonable security procedures and practices appropriate to the nature of the personal data it processes as set forth in Section 11 of the Addendum.

3. Canada:

3.1. The definition of "Applicable Data Protection Law" includes the Federal Personal Information Protection and Electronic Documents Act (PIPEDA).
3.2. Twilio's sub-processors, as described in Section 7 of the Addendum, are third parties under Applicable Data Protection Law, with whom Twilio has entered into a written contract that includes

terms substantially similar to this Addendum. Twilio has conducted appropriate due diligence on its sub-processors.
3.3. Twilio will implement technical and organizational measures as set forth in Section 11 of the Addendum.

4. Chile:

4.1. The definition of "Applicable Data Protection Law" includes Law 19.628.

5. Israel:

5.1 The definition of "Applicable Data Protection Law" includes the Protection of Privacy Law (PPL).
5.2 The definition of "controller" includes "Database Owner" as defined under Applicable Data Protection Law.
5.3 The definition of "processor" includes "Holder" as defined under Applicable Data Protection Law.
5.4 Twilio will require that any personnel authorized to process Customer Content comply with the principle of data secrecy and have been duly instructed about Applicable Data Protection Law. Such personnel sign confidentiality agreements with Twilio in accordance with Section 6 of the Addendum.
5.5 Twilio must take sufficient steps to ensure the privacy of data subjects by implementing and maintaining the security measures as specified in Section 11 of the Addendum and complying with the terms of the Agreement.
5.6 Twilio must ensure that the personal data will not be transferred to a sub-processor unless such sub-processor has executed an agreement with Twilio pursuant to Section 7.1 of this Addendum.

6. Japan:

6.1 The definition of "Applicable Data Protection Law" includes the Act on the Protection of Personal Information (APPI).
6.2 The definition of "personal data" includes "Personal Information" as defined under Applicable Data Protection Law.
6.3 The definition of "controller" includes "Business Operator" as defined under Applicable Data Protection Law. As a Business Operator, Twilio is responsible for the handling of personal data in its possession.

7. Mexico

7.1. The definition of "Applicable Data Protection Law" includes the Federal Law for the Protection of Personal Data Held by Private Parties and its Regulations (FLPPIPPE).
7.2. When acting as a processor, Twilio will:
(a) treat personal data in accordance with Customer's instructions as outlined in Section 5 of the Addendum;
(b) process personal data only to the extent necessary to provide the Services;
(c) implement security measures in accordance with Applicable Data Protection Law and Section 11 of the Addendum;
(d) keep confidentiality regarding the personal data processed in accordance with the Agreement;

(e) delete all personal data upon termination of the Agreement in accordance with Section 10 of the Addendum; and
(f) only transfer personal data to sub-processors in accordance with Section 7 of the Addendum.

8. Singapore:

8.1 The definition of "Applicable Data Protection Law" includes the Personal Data Protection Act 2012 (PDPA).
8.2 Twilio will process personal data to a standard of protection in accordance with the PDPA by implementing adequate technical and organizational measures as set forth in Section 11 of the Addendum and complying with the terms of the Agreement.

9. United Kingdom:

9.1 The definition of "Applicable Data Protection Law" includes the Data Protection Act 2018.

Bilag E –Google Cloud Platform: EU Model Contract Clauses

Standard Contractual Clauses (processors)

for the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

the non-Google legal entity accepting the Clauses (the "Data Exporter")

And

Google LLC (formerly known as Google Inc.),
1600 Amphitheatre Parkway, Mountain View, California 94043 USA

(the "**Data Importer**")

each a "party"; together "the parties",

HAVE AGREED on the following Contractual Clauses (the "Clauses") in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the Data Exporter to the Data Importer of the personal data specified in Appendix 1.

The Clauses (including Appendices 1 and 2) are effective from the date the Data Exporter has both: (i) executed a valid Google Cloud Platform Agreement with Data Processing and Security Terms (collectively the "Services Agreement") and (ii) clicked to accept these Clauses. In this document: (a) "Google Cloud Platform Agreement" means an agreement under which the Data Importer, Google Ireland Limited, Google Asia Pacific Pte. Ltd., or any other entity that directly or indirectly controls, is controlled by, or is under common control with the Data Importer, has agreed to provide Google Cloud Platform (as described at https://cloud.google.com/terms/services) and related technical support to Data Exporter (whether as a customer, reseller or supplier); and (b) "Data Processing and Security Terms" means terms incorporated by reference into the Google Cloud Platform Agreement or otherwise subsequently agreed between the parties to that agreement that set out certain terms in relation to the protection and processing of personal data.

If you are accepting on behalf of the Data Exporter, you represent and warrant that: (i) you have full legal authority to bind your employer, or the applicable entity, to these terms and conditions; (ii) you have read and understand the Clauses; and (iii) you agree, on behalf of the party that you represent, to the Clauses. If you do not have the legal authority to bind the Data Exporter, please do not click the "I Accept" button below. The Clauses shall automatically expire on the termination or expiry of the Data Processing and Security Terms. The parties agree that where Data Exporter has been presented with these Clauses and clicked to accept these terms electronically, such acceptance shall constitute execution of the entirety of the Clauses by both parties, subject to the effective date described above.

Clause 1

Definitions

For the purposes of the Clauses:

- (a) '***personal data***', '***special categories of data***', '***process/processing***', '***controller***', '***processor***', '***Data Subject***' and '***Supervisory Authority***' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;
- (b) 'the ***Data Exporter***' means the controller who transfers the personal data;
- (c) 'the ***Data Importer***' means the processor who agrees to receive from the Data Exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25 (1) of Directive 95/46/EC;
- (d) 'the ***Subprocessor***' means any processor engaged by the Data Importer or by any other subprocessor of the Data Importer who agrees to receive from the Data Importer or from any

other subprocessor of the Data Importer personal data exclusively intended for processing activities to be carried out on behalf of the Data Exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

- (e) 'the ***applicable data protection law***' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the Data Exporter is established;
- (f) '***technical and organisational security measures***' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.
-

Clause 2

Details of the transfer

- The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

- 1. The Data Subject can enforce against the Data Exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.
- 2. The Data Subject can enforce against the Data Importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the Data Exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the Data Exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the Data Exporter, in which case the Data Subject can enforce them against such entity.
- 3. The Data Subject can enforce against the Subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the Data Exporter and the Data Importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the Data Exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the Data Subject can enforce them against such entity. Such third-party liability of the Subprocessor shall be limited to its own processing operations under the Clauses.
- 4. The parties do not object to a Data Subject being represented by an association or other body if the Data Subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the Data Exporter

The Data Exporter agrees and warrants:

- (a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the Data Exporter is established) and does not violate the relevant provisions of that State
- (b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the Data Exporter's behalf and in accordance with the applicable data protection law and the Clauses;
- (c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;
- (d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation.
- (e) that it will ensure compliance with the security measures;
- (f) that, if the transfer involves special categories of data, the Data Subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;
- (g) to forward any notification received from the data importer or any Subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the Data Exporter decides to continue the transfer or to lift the suspension;
- (h) to make available to the Data Subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;
- (i) that, in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 by a Subprocessor providing at least the same level of protection for the personal data and the rights of Data Subject as the Data Importer under the Clauses; and
- (j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the Data Importer*

The Data Importer agrees and warrants:

- (a) to process the personal data only on behalf of the Data Exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the Data Exporter of its inability to comply, in which case the Data Exporter is entitled to suspend the transfer of data and/or terminate the contract;

- (b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the Data Exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the Data Exporter as soon as it is aware, in which case the Data Exporter is entitled to suspend the transfer of data and/or terminate the contract;
- (c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;
- (d) that it will promptly notify the Data Exporter about:

- (i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;
- (ii) any accidental or unauthorised access; and
- (iii) any request received directly from the Data Subjects without responding to that request, unless it has been otherwise authorised to do so;

- (e) to deal promptly and properly with all inquiries from the Data Exporter relating to its processing of the personal Data Subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;
- (f) at the request of the Data Exporter to submit its data-processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the Data Exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the Data Exporter, where applicable, in agreement with the supervisory authority;
- (g) to make available to the Data Subject upon request a copy of the Clauses, or any existing contract for sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the Data Subject is unable to obtain a copy from the Data Exporter;
- (h) that, in the event of sub-processing, it has previously informed the Data Exporter and obtained its prior written consent;
- (i) that the processing services by the Subprocessor will be carried out in accordance with Clause 11;
- (j) to send promptly a copy of any Subprocessor agreement it concludes under the Clauses to the Data Exporter.

Clause 6

Liability

- 1. The parties agree that any Data Subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or Subprocessor is entitled to receive compensation from the Data Exporter for the damage suffered.
- 2. If a Data Subject is not able to bring a claim for compensation in accordance with paragraph 1 against the Data Exporter, arising out of a breach by the Data Importer or his Subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the

Data Exporter has factually disappeared or ceased to exist in law or has become insolvent, the Data Importer agrees that the Data Subject may issue a claim against the Data Importer as if it were the Data Exporter, unless any successor entity has assumed the entire legal obligations of the Data Exporter by contract or by operation of law, in which case the Data Subject can enforce its rights against such entity.The Data Importer may not rely on a breach by a Subprocessor of its obligations in order to avoid its own liabilities.

- 3. If a Data Subject is not able to bring a claim against the Data Exporter or the Data Importer referred to in paragraphs 1 and 2, arising out of a breach by the Subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the Data Exporter and the Data Importer have factually disappeared or ceased to exist in law or have become insolvent, the Subprocessor agrees that the Data Subject may issue a claim against the data Subprocessor with regard to its own processing operations under the Clauses as if it were the Data Exporter or the Data Importer, unless any successor entity has assumed the entire legal obligations of the Data Exporter or Data Importer by contract or by operation of law, in which case the Data Subject can enforce its rights against such entity. The liability of the Subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

- 1. The Data Importer agrees that if the Data Subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the Data Importer will accept the decision of the Data Subject;

- (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
- (b) to refer the dispute to the courts in the Member State in which the Data Exporter is established.

- 2. The parties agree that the choice made by the Data Subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

- 1. The Data Exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.
- 2. The parties agree that the supervisory authority has the right to conduct an audit of the Data Importer, and of any Subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the Data Exporter under the applicable data protection law.
- 3. The Data Importer shall promptly inform the Data Exporter about the existence of legislation applicable to it or any Subprocessor preventing the conduct of an audit of the Data Importer, or any Subprocessor, pursuant to paragraph 2. In such a case the Data Exporter shall be entitled to take the measures foreseen in Clause 5(b).

-

Clause 9

Governing Law

- The Clauses shall be governed by the law of the Member State in which the Data Exporter is established.

Clause 10

Variation of the contract

- The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.
-

Clause 11

Sub-Processing

- 1. The Data Importer shall not subcontract any of its processing operations performed on behalf of the Data Exporter under the Clauses without the prior written consent of the Data Exporter. Where the Data Importer subcontracts its obligations under the Clauses, with the consent of the Data Exporter, it shall do so only by way of a written agreement with the Subprocessor which imposes the same obligations on the Subprocessor as are imposed on the Data Importer under the Clauses. Where the Subprocessor fails to fulfil its data protection obligations under such written agreement the Data Importer shall remain fully liable to the Data Exporter for the performance of the Subprocessor's obligations under such agreement.
- 2. The prior written contract between the Data Importer and the Subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the Data Subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the Data Exporter or the Data Importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the Data Exporter or Data Importer by contract or by operation of law. Such third-party liability of the Subprocessor shall be limited to its own processing operations under the Clauses.
- 3. The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the Data Exporter is established.
- 4. The Data Exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the Data Importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be available to the Data Exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

- 1. The parties agree that on the termination of the provision of data processing services, the Data Importer and the Subprocessor shall, at the choice of the Data Exporter, return all the personal data transferred and the copies thereof to the Data Exporter or shall destroy all the personal data and certify to the Data Exporter that it has done so, unless legislation imposed upon the Data Importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the Data Importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.
- 2. The Data Importer and the Subprocessor warrant that upon request of the Data Exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

Appendix 1

to the Standard Contractual Clauses

This Appendix forms part of the Clauses

Data Exporter

- The Data Exporter is the non-Google legal entity that is a party to the Clauses.

Data Importer

- The Data Importer is Google LLC, a global provider of a variety of technology services for businesses.

Data Subjects

- The personal data transferred concern the following categories of data subjects: Data subjects include the individuals about whom data is provided to Google via the Services (as defined in the Services Agreement) by (or at the direction of) Data Exporter.

Categories of data

- The personal data transferred concern the following categories of data: Data relating to individuals provided to Google via the Services by (or at the direction of) Data Exporter.

Special categories of data (if appropriate)

- The personal data transferred concern the following special categories of data: Data relating to individuals provided to Google via the Services by (or at the direction of) Data Exporter.

Processing operations

The personal data transferred will be subject to the following basic processing activities:

- Scope of Processing.
- The Clauses reflect the parties' agreement with respect to the processing and transfer of personal data specified in this Appendix pursuant to the provision of the Services. Personal data may be processed only to comply with Instructions (as defined in the Data Processing and Security Terms). The Data Exporter instructs the Data Importer to process personal data in countries in which the Data Importer or its Subprocessors maintain facilities.
- Term of Data Processing.
- Data processing will be for the period specified in the Data Processing and Security Terms. Such period will automatically terminate upon the deletion by the Data Importer of all data as described in the Data Processing and Security Terms.
- Data Deletion.
- During the term of the Services Agreement, the Data Importer will provide the Data Exporter with the ability to delete the Data Exporter's personal data from the Services in accordance with the Services Agreement. After termination or expiry of the Services Agreement, the Data Importer will delete the Data Exporter's personal data in accordance with the Data Processing and Security Terms.
- Access to Data.
- During the term of the Services Agreement, the Data Importer will provide the Data Exporter with access to, and the ability to rectify, restrict processing of, and export the Data Exporter's personal data from the Services in accordance with the Services Agreement.
- Subprocessors.
- The Data Importer may engage Subprocessors to provide parts of the Services and TSS (as defined in the Services Agreement). The Data Importer will ensure Subprocessors only access and use the Data Exporter's personal data to provide the Services and TSS and not for any other purpose.

Appendix 2

to the Standard Contractual Clauses

This Appendix forms part of the Clauses.

Description of the technical and organisational security measures implemented by the Data Importer in accordance with Clauses 4(c) and 5(c) (or document/legislation attached):

The Data Importer currently abides by the security standards in this Appendix 2. The Data Importer may update or modify these security standards from time to time provided such updates and modifications will not result in a degradation of the overall security of the Services during the term of the Services Agreement.

- 1.Data Center & Network Security.

- (a) Data Centers.

- Infrastructure. The Data Importer maintains geographically distributed data centers. The Data Importer stores all production data in physically secure data centers.
- Redundancy. Infrastructure systems have been designed to eliminate single points of failure and minimize the impact of anticipated environmental risks. Dual circuits, switches, networks or other necessary devices help provide this redundancy. The Services are designed to allow the Data Importer to perform certain types of preventative and corrective maintenance without interruption. All environmental equipment and facilities have documented preventative maintenance procedures that detail the process for and frequency of performance in accordance with the manufacturer's or internal specifications. Preventative and corrective maintenance of the data center equipment is scheduled through a standard change process according to documented procedures.
- Power. The data center electrical power systems are designed to be redundant and maintainable without impact to continuous operations, 24 hours a day, 7 days a week. In most cases, a primary as well as an alternate power source, each with equal capacity, is provided for critical infrastructure components in the data center. Backup power is provided by various mechanisms such as uninterruptible power supplies (UPS) batteries, which supply consistently reliable power protection during utility brownouts, blackouts, over voltage, under voltage, and out-of-tolerance frequency conditions. If utility power is interrupted, backup power is designed to provide transitory power to the data center, at full capacity, for up to 10 minutes until the diesel generator systems take over. The diesel generators are capable of automatically starting up within seconds to provide enough emergency electrical power to run the data center at full capacity typically for a period of days.
- Server Operating Systems. The Data Importer servers use a Linux based implementation customized for the application environment. Data is stored using proprietary algorithms to augment data security and redundancy. The Data Importer employs a code review process to increase the security of the code used to provide the Services and enhance the security products in production environments.
- Businesses Continuity. The Data Importer replicates data over multiple systems to help to protect against accidental destruction or loss. The Data Importer has designed and regularly plans and tests its business continuity planning/disaster recovery programs.

- (b) Networks and Transmission.

- Data Transmission. Data centers are typically connected via high-speed private links to provide secure and fast data transfer between data centers.This is designed to prevent data from being read, copied, altered or removed without authorization during electronic transfer or transport or while being recorded onto data storage media. The Data Importer transfers data via Internet standard protocols.

- External Attack Surface. The Data Importer employs multiple layers of network devices and intrusion detection to protect its external attack surface. The Data Importer considers potential attack vectors and incorporates appropriate purpose built technologies into external facing systems.
- Intrusion Detection. Intrusion detection is intended to provide insight into ongoing attack activities and provide adequate information to respond to incidents. The Data Importer intrusion detection involves:

- 1. tightly controlling the size and make-up of the Data Importer's attack surface through preventative measures;
- 2. employing intelligent detection controls at data entry points; and
- 3. employing technologies that automatically remedy certain dangerous situations.

- Incident Response. The Data Importer monitors a variety of communication channels for security incidents, and The Data Importer's security personnel will react promptly to known incidents.
- Encryption Technologies. The Data Importer makes HTTPS encryption (also referred to as SSL or TLS connection) available. Google servers support ephemeral elliptic curve Diffie-Hellman cryptographic key exchange signed with RSA and ECDSA. These perfect forward secrecy (PFS) methods help protect traffic and minimize the impact of a compromised key, or a cryptographic breakthrough.

- 2. Access and Site Controls.

- (a) Site Controls.

- On-site Data Center Security Operation. The Data Importer's data centers maintain an on-site security operation responsible for all physical data center security functions 24 hours a day, 7 days a week. The on-site security operation personnel monitor closed circuit TV (CCTV) cameras and all alarm systems. On-site security operation personnel perform internal and external patrols of the data center regularly.
- Data Center Access Procedures. The Data Importer maintains formal access procedures for allowing physical access to the data centers. The data centers are housed in facilities that require electronic card key access, with alarms that are linked to the on-site security operation. All entrants to the data center are required to identify themselves as well as show proof of identity to on-site security operations. Only authorized employees, contractors and visitors are allowed entry to the data centers. Only authorized employees and contractors are permitted to request electronic card key access to these facilities. Data center electronic card key access requests must be made through e-mail, and require the approval of the requestor's manager and the data center director. All other entrants requiring temporary data center access must: (i) obtain approval in advance from the data center managers for the specific data center and internal areas they wish to visit; (ii) sign in at on-site security operations; and (iii) reference an approved data center access record identifying the individual as approved.
- On-site Data Center Security Devices. The Data Importer's data centers employ an electronic card key and biometric access control system that is linked to a system alarm. The access control system monitors and records each individual's electronic card key and when they access perimeter doors, shipping and receiving, and other critical areas. Unauthorized

activity and failed access attempts are logged by the access control system and investigated, as appropriate. Authorized access throughout the business operations and data centers is restricted based on zones and the individual's job responsibilities. The fire doors at the data centers are alarmed. CCTV cameras are in operation both inside and outside the data centers. The positioning of the cameras has been designed to cover strategic areas including, among others, the perimeter, doors to the data center building, and shipping/receiving. On-site security operations personnel manage the CCTV monitoring, recording and control equipment. Secure cables throughout the data centers connect the CCTV equipment. Cameras record on site via digital video recorders 24 hours a day, 7 days a week. The surveillance records are retained for up to 30 days based on activity.

- (b) Access Control.

- Infrastructure Security Personnel. The Data Importer has, and maintains, a security policy for its personnel, and requires security training as part of the training package for its personnel. The Data Importer's infrastructure security personnel are responsible for the ongoing monitoring of the Data Importer's security infrastructure, the review of the Services, and responding to security incidents.
- Access Control and Privilege Management. The Data Exporter's administrators must authenticate themselves via a central authentication system or via a single sign on system in order to administer the Services.
- Internal Data Access Processes and Policies – Access Policy. The Data Importer's internal data access processes and policies are designed to prevent unauthorized persons and/or systems from gaining access to systems used to process personal data. The Data Importer designs its systems to: (i) only allow authorized persons to access data they are authorized to access; and (ii) ensure that personal data cannot be read, copied, altered or removed without authorization during processing, use and after recording. The systems are designed to detect any inappropriate access.The Data Importer employs a centralized access management system to control personnel access to production servers, and only provides access to a limited number of authorized personnel. LDAP, Kerberos and a proprietary system utilizing SSH certificates are designed to provide the Data Importer with secure and flexible access mechanisms. These mechanisms are designed to grant only approved access rights to site hosts, logs, data and configuration information. The Data Importer requires the use of unique user IDs, strong passwords, two factor authentication and carefully monitored access lists to minimize the potential for unauthorized account use. The granting or modification of access rights is based on: the authorized personnel's job responsibilities; job duty requirements necessary to perform authorized tasks; and a need to know basis. The granting or modification of access rights must also be in accordance with The Data Importer's internal data access policies and training. Approvals are managed by workflow tools that maintain audit records of all changes. Access to systems is logged to create an audit trail for accountability. Where passwords are employed for authentication (e.g., login to workstations), password policies that follow at least industry standard practices are implemented. These standards include restrictions on password reuse and sufficient password strength. For access to extremely sensitive information (e.g., credit card data), the Data Importer uses hardware tokens.

- 3. Data.

- (a) Data Storage, Isolation and Logging.

- The Data Importer stores data in a multi-tenant environment on the Data Importer-owned servers. The data and file system architecture are replicated between multiple geographically dispersed data centers. The Data Importer also logically isolates the Data Exporter's data, and the Data Exporter will be given control over specific data sharing policies. Those policies, in accordance with the functionality of the Services, will enable the Data Exporter to determine the product sharing settings applicable to end users for specific purposes. The Data Exporter may choose to make use of certain logging capability that the Data Importer may make available via the Services.

- (b) Decommissioned Disks and Disk Erase Policy.

- Disks containing data may experience performance issues, errors or hardware failure that lead them to be decommissioned ("Decommissioned Disk"). Every Decommissioned Disk is subject to a series of data destruction processes (the "Disk Erase Policy") before leaving the Data Importer's premises either for reuse or destruction. Decommissioned Disks are erased in a multi-step process and verified complete by at least two independent validators. The erase results are logged by the Decommissioned Disk's serial number for tracking. Finally, the erased Decommissioned Disk is released to inventory for reuse and redeployment. If, due to hardware failure, the Decommissioned Disk cannot be erased, it is securely stored until it can be destroyed. Each facility is audited regularly to monitor compliance with the Disk Erase Policy.

- 4. Personnel Security.

- The Data Importer personnel are required to conduct themselves in a manner consistent with the company's guidelines regarding confidentiality, business ethics, appropriate usage, and professional standards. The Data Importer conducts reasonably appropriate backgrounds checks to the extent legally permissible and in accordance with applicable local labor law and statutory regulations.
- Personnel are required to execute a confidentiality agreement and must acknowledge receipt of, and compliance with, the Data Importer's confidentiality and privacy policies. Personnel are provided with security training. Personnel handling customer data are required to complete additional requirements appropriate to their role (eg., certifications). The Data Importer's personnel will not process customer data without authorization.

- 5. Subprocessor Security.

- Before onboarding Subprocessors, the Data Importer conducts an audit of the security and privacy practices of Subprocessors to ensure Subprocessors provide a level of security and privacy appropriate to their access to data and the scope of the services they are engaged to provide. Once the Data Importer has assessed the risks presented by the Subprocessor, the Subprocessor is required to enter into appropriate security, confidentiality and privacy contract terms as described in Section 11.3 of the Data Processing and Security Terms.

- 6. The Data Importer's Cloud Data Protection Team.

- The Data Importer's Cloud Data Protection Team can be contacted at: https://support.google.com/cloud/contact/dpo (and/or via such other means as Google may provide from time to time).

---

* Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, inter alia, internationally recognised sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

Version 1.6