Addendum voor Cloud-gegevensverwerking (Partners)

Dit Addendum voor Cloud-gegevensverwerking (inclusief bijbehorende bijlagen, het "*Addendum*") maakt deel uit van de Overeenkomst (zoals hieronder gedefinieerd) tussen Google en Partner. Dit Addendum heette voorheen de "Gegevensverwerkings- en Beveiligingsvoorwaarden" voor Google Cloud Platform, en "Addendum Gegevensverwerking" of "Gegevensverwerkings- en Beveiligingsdiensten" voor Looker- (oorspronkelijk) of Google SecOps Diensten.

Algemene voorwaarden

1. Overzicht

Dit Addendum beschrijft de verplichtingen van de partijen, met inbegrip van maar niet beperkt tot, verplichtingen op grond van de toepasselijke privacy-, gegevensbeveiligings- en gegevensbeschermingswetgeving, met betrekking tot de verwerking en beveiliging van Partnergegevens. Dit Addendum treedt in werking op de Ingangsdatum van het Addendum (zoals hieronder gedefinieerd) en zal alle voorwaarden vervangen die eerder van toepassing waren op de verwerking en beveiliging van Partnergegevens. Termen met een hoofdletter die in dit Addendum worden gebruikt maar niet gedefinieerd, hebben de betekenis die daaraan in de Overeenkomst is gegeven.

2. Definities

2.1 In dit Addendum:

- *"Ingangsdatum van het Addendum"* betekent de datum waarop Partner dit Addendum heeft geaccepteerd, of waarop de partijen anderszins akkoord zijn gegaan met dit Addendum.
- *"Aanvullende Beveiligingsmechanismen"* betekent hulpmiddelen, functies, functionaliteiten en opties voor beveiliging die Partner naar eigen keuze en inzicht kan gebruiken, inclusief de Admin Console, versleuteling, logging en monitoring, identiteits- en toegangsbeheer, beveiligingsscans en firewalls.
- *"Overeenkomst"* betekent de overeenkomst op grond waarvan Google heeft ingestemd de toepasselijke Diensten aan Partner te leveren.
- *"Toepasselijke Privacywetgeving"* betekent, voor zover van toepassing op de verwerking van Persoonsgegevens van Partner, alle nationale, federale, EU-, staats-, provinciale of overige wet- of regelgeving voor privacy, gegevensbeveiliging of gegevensbescherming.
- *"Gecontroleerde Diensten"* betekent de op dat moment geldende Diensten die binnen de reikwijdte vallen van de relevante certificering of het relevante rapport op

https://cloud.google.com/security/compliance/services-in-scope. Google mag geen Diensten verwijderen van deze URL, tenzij ze zijn beëindigd in overeenstemming met de Overeenkomst.

- *"Compliance-certificeringen"* heeft de betekenis die is gegeven in Artikel 7.4 (Compliance-certificeringen en SOC-rapporten).

- *"Gegevensincident"* betekent een inbreuk op de beveiliging van Google die onbedoeld of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging, of de ongeoorloofde verstrekking van of toegang tot Partnergegevens op systemen die door Google worden beheerd of anderszins door Google worden gecontroleerd.

- *"EMEA"* betekent Europa, het Midden-Oosten en Afrika.

- *"EU-AVG"* betekent Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens, en tot intrekking van Richtlijn 95/46/EG.

- *"Europese Gegevensbeschermingswetgeving"* betekent, voor zover van toepassing: (a) de AVG; of (b) de Zwitserse FADP.

- *"Europees Recht"* betekent, voor zover van toepassing: (a) EU-wetgeving of wetgeving van een EU-lidstaat (als de EU-AVG van toepassing is op de verwerking van Partner-Persoonsgegevens); (b) de wetgeving van het Verenigd Koninkrijk of een deel van het Verenigd Koninkrijk (als de VK-AVG van toepassing is op de verwerking van Partner-Persoonsgegevens); of (c) de wetgeving van Zwitserland (als de Zwitserse FADP van toepassing is op de verwerking van Partner-Persoonsgegevens).

- *"AVG"* betekent, voor zover van toepassing: (a) de EU-AVG; of (b) de AVG van het Verenigd Koninkrijk (VK-AVG).

- *"Externe Auditor van Google"* betekent een door Google aangestelde, gekwalificeerde en onafhankelijke externe auditor, van wie Google de op dat moment geldende identiteit aan Partner zal bekendmaken.

- *"Instructies"* heeft de betekenis die is gegeven in Artikel 5.2 (Compliance van de Instructies van Partner).

- *"E-mailadres voor Kennisgevingen"* betekent het e-mailadres/de e-mailadressen die door Partner in de Admin Console of op het Bestelformulier zijn opgegeven om bepaalde kennisgevingen van Google te ontvangen.

- *"Eindgebruikers van Partner"* heeft de betekenis die is gegeven in de Overeenkomst, of, indien een dergelijke betekenis niet is gegeven, de betekenis die in de Overeenkomst is gegeven aan "Eindgebruikers".

- *"Partner-Persoonsgegevens"* betekent de persoonsgegevens die zijn vervat in Partnergegevens, waaronder eventuele bijzondere categorieën persoonsgegevens of gevoelige gegevens gedefinieerd onder de Toepasselijke Privacywetgeving.

- *"Beveiligingsdocumentatie"* betekent de Compliance-certificeringen en de SOC-rapporten.

- *"Beveiligingsmaatregelen"* heeft de betekenis die is gegeven in Artikel 7.1.1 (Googles Beveiligingsmaatregelen).

- *"Diensten"* betekent de toepasselijke diensten die zijn beschreven in Bijlage 4 (Specifieke producten).

- *"SOC-rapporten"* heeft de betekenis die is gegeven in Artikel 7.4 (Compliance-certificeringen en SOC-rapporten).

- *"Subverwerker"* betekent een derde die als andere verwerker onder dit Addendum is gemachtigd om Partnergegevens te verwerken teneinde onderdelen van de Diensten en TSS (indien van toepassing) te leveren.

- *"Toezichthoudende Autoriteit"* betekent, voor zover van toepassing: (a) een "toezichthoudende autoriteit" zoals gedefinieerd in de EU-AVG; of (b) de "Commissioner" zoals gedefinieerd in de VK-AVG of de Zwitserse FADP.

- *"Zwitserse FADP"* betekent, voor zover van toepassing, de Federal Act on Data Protection van 19 juni 1992 (Zwitserland) (met de Ordinance to the Federal Act on Data Protection van 14 juni 1993) of de herziene Federal Act on Data Protection van 25 september 2020 (Zwitserland) (met de Ordinance to the Federal Act on Data Protection van 31 augustus 2022).

- *"Looptijd"* betekent de periode vanaf de Ingangsdatum van het Addendum tot het einde van Googles levering van de Diensten, met inbegrip van, indien van toepassing, iedere periode waarin levering van de Diensten kan worden opgeschort en iedere periode na beëindiging waarin Google de Diensten kan blijven leveren voor overgangsdoeleinden.

- *"VK-AVG"* (*UK GDPR*) betekent de AVG van de EU zoals gewijzigd en opgenomen in de wetgeving van het Verenigd Koninkrijk krachtens de European Union (Withdrawal) Act 2018 van het Verenigd Koninkrijk, en toepasselijke secundaire wetgeving vastgesteld krachtens die wet.

2.2 De termen "persoonsgegevens", "betrokkene", "verwerking", "verwerkingsverantwoordelijke" en "verwerker" zoals gebruikt in dit Addendum hebben de betekenissen die daaraan worden gegeven door de Toepasselijke Privacywetgeving of, bij gebreke van een dergelijke betekenis of wetgeving, door de EU-AVG.

2.3 De termen "betrokkene", "verwerkingsverantwoordelijke" en "verwerker" omvatten respectievelijk "consument", "bedrijf" en "aanbieder", zoals vereist door de Toepasselijke Privacywetgeving.

3. Duur

Ongeacht of de Overeenkomst is beëindigd of verlopen, blijft dit Addendum van kracht totdat Google alle Partnergegevens heeft verwijderd zoals beschreven in dit Addendum, waarna het Addendum automatisch afloopt.

4. Rollen; Compliance met wet- en regelgeving

4.1 *Rollen van partijen.* Google is een verwerker en Partner is, naargelang het geval, verwerkingsverantwoordelijke of verwerker met betrekking tot Partner-Persoonsgegevens.

4.2 *Verwerkingssamenvatting.* Het onderwerp en de details van de verwerking van Partner-Persoonsgegevens worden beschreven in Bijlage 1 (Onderwerp en details van gegevensverwerking).

4.3 *Compliance met wetgeving.* Elke partij zal haar verplichtingen met betrekking tot de verwerking van Partner-Persoonsgegevens onder de Toepasselijke Privacywetgeving naleven.

4.4 *Aanvullende juridische voorwaarden*. Voor zover de verwerking van Partner-Persoonsgegevens onderworpen is aan Toepasselijke Privacywetgeving zoals beschreven in Bijlage 3 (Specifieke privacywetgeving), zijn de overeenkomstige voorwaarden in Bijlage 3 van toepassing naast deze Algemene voorwaarden en hebben voorrang zoals beschreven in Artikel 14.1 (Voorrang).

5. Gegevensverwerking

5.1 *Partners die verwerker zijn*. Indien Partner een verwerker is:

a. garandeert Partner doorlopend dat de relevante Klant en derde-verwerkingsverantwoordelijke het volgende hebben geautoriseerd:

i. de Instructies;

ii. de inschakeling van Google als andere verwerker door Partner; en

iii. de inschakeling door Google van Subverwerkers zoals beschreven in Artikel 11 (Subverwerkers);

b. zal Partner alle door Google verstrekte kennisgevingen op grond van Artikel 7.2.1 (Kennisgeving van incidenten), 9.2.1 (Verantwoordelijkheid voor Verzoeken) of 11.4 (Mogelijkheid om bezwaar te maken tegen Subverwerkers) prompt en zonder onnodige vertraging doorsturen naar de relevante Klant en derde-verwerkingsverantwoordelijke; en

c. kan Partner aan de relevante Klant en derde-verwerkingsverantwoordelijke alle eventuele andere informatie beschikbaar stellen die door Google onder dit Addendum beschikbaar wordt gesteld over de locaties van Google-datacenters of de namen, locaties en activiteiten van Subverwerkers.

5.2 *Compliance met Instructies van Partner*. Partner instrueert Google om Partnergegevens uitsluitend te verwerken in overeenstemming met de Overeenkomst (inclusief dit Addendum), als volgt:

a. om de Diensten en TSS te leveren, te beveiligen en te monitoren; en

b. zoals verder gespecificeerd via:

i. het gebruik van de Diensten door Partner (inclusief via de Admin Console) en TSS; en

ii. alle andere schriftelijke instructies gegeven door Partner en door Google erkend als zijnde instructies onder dit Addendum

(gezamenlijk de "*Instructies*").

Google zal zich houden aan de Instructies, tenzij dit is verboden op grond van Europees Recht wanneer Europese Gegevensbeschermingswetgeving van toepassing is, of dit verboden is op grond van toepasselijk recht in geval dat andere Toepasselijke Privacywetgeving van toepassing is.

6. Gegevensverwijdering

6.1 *Verwijdering door Partner*. Google zal Partner in staat stellen om tijdens de Looptijd Partnergegevens te verwijderen op een wijze die in overeenstemming is met de functionaliteit van de Diensten. Indien Partner de Diensten gebruikt om tijdens de Looptijd Partnergegevens te verwijderen en deze Partnergegevens niet door Partner kunnen worden hersteld, vormt dit gebruik een Instructie aan Google om de relevante Partnergegevens te verwijderen uit de systemen van Google. Google zal aan deze Instructie voldoen zo snel als redelijkerwijs mogelijk is en uiterlijk binnen 180 dagen, tenzij opslag vereist is op grond van Europees Recht wanneer Europese Gegevensbeschermingswetgeving van toepassing is, of opslag vereist is op grond van toepasselijk recht wanneer enige andere Toepasselijke Privacywetgeving van toepassing is.

6.2 *Teruggave of verwijdering wanneer de Looptijd eindigt*. Indien Partner bepaalde Partnergegevens na het einde van de Looptijd wenst te behouden, kan hij Google instrueren in overeenstemming met Artikel 9.1 (Toegang, Rectificatie, Beperkte verwerking, Overdraagbaarheid) om de gegevens tijdens de Looptijd terug te geven. Partner instrueert Google om alle resterende Partnergegevens (met inbegrip van bestaande kopieën) aan het einde van de Looptijd uit de systemen van Google te verwijderen. Na een herstelperiode van maximaal 30 dagen vanaf die datum, zal Google aan deze Instructie voldoen zo snel als redelijkerwijs mogelijk en binnen een maximale periode van 180 dagen, tenzij opslag is vereist op grond van het Europees Recht wanneer Europese Gegevensbeschermingswetgeving van toepassing is, of opslag is vereist op grond van toepasselijk recht wanneer enige andere Toepasselijke Privacywetgeving van toepassing is.

7. Gegevensbeveiliging

7.1 *Googles Beveiligingsmaatregelen, -mechanismen en -assistentie*.

7.1.1 *Beveiligingsmaatregelen van Google*. Google zal technische, organisatorische en fysieke maatregelen implementeren en onderhouden om Partnergegevens te beschermen tegen onbedoelde of onrechtmatige vernietiging, verlies, wijziging, ongeoorloofde verstrekking of toegang zoals beschreven in Bijlage 2 (Beveiligingsmaatregelen) (de "*Beveiligingsmaatregelen*"). De Beveiligingsmaatregelen omvatten maatregelen om Partnergegevens te versleutelen; om te helpen bij het waarborgen van de voortdurende vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de systemen en diensten van Google; om te helpen tijdig toegang tot Partnergegevens te herstellen na een incident; en voor regelmatige effectiviteitstests. Google kan de Beveiligingsmaatregelen van tijd tot tijd bijwerken, mits dergelijkeupdates niet leiden tot een materiële vermindering van de beveiliging van de Diensten.

7.1.2 *Toegang en Compliance*. Google zal:

a. Zijn medewerkers, onderaannemers en Subverwerkers alleen machtigen om toegang te hebben tot Partnergegevens voor zover dit strikt noodzakelijk is om aan de Instructies te voldoen;

b. passende stappen ondernemen om compliance met de Beveiligingsmaatregelen door zijn medewerkers, onderaannemers en Subverwerkers te garanderen voor zover van toepassing binnen de reikwijdte van hun werkzaamheden; en

c. ervoor zorgen dat alle personen die gemachtigd zijn om Partnergegevens te verwerken onder een geheimhoudingsverplichting vallen.

7.1.3 *Aanvullende Beveiligingsmechanismen.* Google zal Aanvullende Beveiligingsmechanismen beschikbaar stellen om:

a. Partner in staat te stellen stappen te ondernemen om Partnergegevens te beveiligen; en

b. Partner te voorzien van informatie over het beveiligen, toegang krijgen tot en gebruiken van Partnergegevens.

7.1.4 *Googles Beveiligingsassistentie*. Google zal (rekening houdend met de aard van de verwerking van Partner-Persoonsgegevens en de informatie waarover Google beschikt) Partner helpen bij het waarborgen van de compliance met zijn verplichtingen (of, wanneer Partner een verwerker is, de verplichtingen van de derde-verwerkingsverantwoordelijke) met betrekking tot beveiliging en inbreuken in verband met persoonsgegevens op grond van de Toepasselijke Privacywetgeving, door:

a. Beveiligingsmaatregelen te implementeren en te onderhouden in overeenstemming met Artikel 7.1.1 (Googles Beveiligingsmaatregelen);

b. Aanvullende Beveiligingsmechanismen beschikbaar te stellen in overeenstemming met Artikel 7.1.3 (Aanvullende Beveiligingsmechanismen);

c. de voorwaarden in Artikel 7.2 (Gegevensincidenten) na te leven;

d. de Beveiligingsdocumentatie beschikbaar te stellen in overeenstemming met Artikel 7.5.1 (Beoordelingen van Beveiligingsdocumentatie) en de informatie opgenomen in de Overeenkomst (inclusief dit Addendum) te verstrekken; en

e. indien de hierboven genoemde subartikelen (a)-(d) onvoldoende zijn voor Partner (of de derde-verwerkingsverantwoordelijke) om aan dergelijke verplichtingen te voldoen, op verzoek van Partner, Partner aanvullende redelijke samenwerking en ondersteuning te bieden.

7.2 *Gegevensincidenten*.

7.2.1 *Kennisgeving van Incidenten*. Google zal Partner prompt en zonder onnodige vertraging op de hoogte stellen nadat Google kennis heeft gekregen van een Gegevensincident, en zal prompt redelijke stappen ondernemen om schade te beperken en Partnergegevens te beveiligen.

7.2.2 *Details van het Gegevensincident*. De kennisgeving door Google van een Gegevensincident zal het volgende beschrijven: de aard van het Gegevensincident, inclusief getroffen bronnen van Partner; de maatregelen die Google heeft genomen of van plan is te nemen om het Gegevensincident aan te pakken en mogelijke risico's te beperken; de maatregelen, indien van toepassing, die Google Partner aanbeveelt om het Gegevensincident aan te pakken; en details van een contactpersoon voor meer informatie. Indien het niet mogelijk is om al deze informatie tegelijk te leveren, bevat de eerste kennisgeving van Google de dan beschikbare informatie en wordt nadere informatie zonder onnodige vertraging geleverd zodra deze beschikbaar is.

7.2.3 *Geen beoordeling van Partnergegevens door Google*. Google is niet verplicht om Partnergegevens te beoordelen om informatie te identificeren die onderworpen is aan specifieke wettelijke vereisten.

7.2.4 *Geen erkenning van schuld door Google*. Kennisgeving van of reactie op een Gegevensincident door Google op grond van dit Artikel 7.2 (Gegevensincidenten) zal niet worden opgevat als een erkenning door Google van schuld of aansprakelijkheid met betrekking tot het Gegevensincident.

7.3 *Verantwoordelijkheden en beoordeling van de beveiliging door Partner*.

7.3.1 *Beveiligingsverantwoordelijkheden van Partner*. Onverminderd de verplichtingen van Google op grond van Artikel 7.1 (Googles Beveiligingsmaatregelen, -mechanismen en -assistentie) en Artikel 7.2 (Gegevensincidenten) en elders in de Overeenkomst, zoals overeengekomen tussen Google en Partner, is Partner verantwoordelijk zijn gebruik en het gebruik van diens Klanten van de Diensten en de opslag van kopieën van Partnergegevens buiten de systemen van Google of Subverwerkers van Google, waaronder begrepen:

a. het gebruik van de Diensten en Aanvullende Beveiligingsmechanismen om een beveiligingsniveau te waarborgen dat passend is bij het risico voor de Partnergegevens;

b. het beveiligen van de accountauthenticatiegegevens, de systemen en de apparaten die Partner en haar Klanten gebruiken om toegang te krijgen tot de Diensten; en

c. het maken van back-ups van zijn Partnergegevens, indien passend.

7.3.2 *Beoordeling van beveiliging door Partner*. Partner stemt ermee in dat de Diensten, Beveiligingsmaatregelen, Aanvullende Beveiligingsmechanismen en verplichtingen van Google op grond van dit Artikel 7 (Gegevensbeveiliging) een beveiligingsniveau bieden dat passend is bij het risico voor Partnergegevens (rekening houdend met de stand van de techniek, de implementatiekosten, alsmede de aard, omvang, context en doeleinden van de verwerking van Partnergegevens en de risico's voor individuen).

7.4 *Compliance-certificeringen en SOC-rapporten*. Google zal ten minste het volgende onderhouden voor de Gecontroleerde Diensten om de blijvende effectiviteit van de Beveiligingsmaatregelen te verifiëren:

a. certificaten voor ISO 27001 en eventuele aanvullende certificeringen beschreven in Bijlage 4 (Specifieke Producten) (de *"Compliance-certificeringen"*); en

b. SOC 2- en SOC 3-rapporten opgesteld door de Externe Auditor van Google en jaarlijks bijgewerkt op basis van een audit die ten minste eenmaal per 12 maanden wordt uitgevoerd (de "*SOC-rapporten*").

Google kan te allen tijde standaarden toevoegen. Google kan een Compliance-certificering of SOC-rapport vervangen door een gelijkwaardig of verbeterd alternatief.

7.5 *Beoordelingen en audits met betrekking tot compliance*.

7.5.1 *Beoordelingen van Beveiligingsdocumentatie*. Om aan te tonen dat Google haar verplichtingen onder dit Addendum nakomt, zal Google de Beveiligingsdocumentatie beschikbaar stellen ter beoordeling door Partner en, indien Partner een verwerker is, zal Google Partner toestaan om toegang te verzoeken tot de SOC-rapporten voor de relevante Klant en derde-verwerkingsverantwoordelijke in overeenstemming met Artikel 7.5.3 (Aanvullende zakelijke voorwaarden voor beoordelingen en audits).

7.5.2 *Auditrechten van Partner*.

a. *Audit door Partner*. Google zal, indien vereist op grond van de Toepasselijke Privacywetgeving, Partner of een door Partner aangestelde onafhankelijke auditor toestaan om audits (inclusief inspecties) uit te voeren om Googles compliance met haar verplichtingen onder dit Addendum te controleren in overeenstemming met Artikel 7.5.3 (Aanvullende zakelijke voorwaarden voor beoordelingen en audits). Tijdens een audit zal Google redelijkerwijs samenwerken met Partner of haar auditor, zoals beschreven in dit Artikel 7.5 (Beoordelingen en audits met betrekking tot compliance).

b. *Onafhankelijke beoordeling door Partner*. Partner kan een audit uitvoeren om Googles compliance met haar verplichtingen uit hoofde van dit Addendum te verifiëren door de Beveiligingsdocumentatie te beoordelen (die de uitkomsten weergeeft van audits uitgevoerd door de Externe Auditor van Google).

7.5.3 *Aanvullende zakelijke voorwaarden voor beoordelingen en audits*.

a. Partner moet contact opnemen met het Cloud-gegevensbeschermingsteam van Google voor:

i. toegang tot de SOC-rapporten voor een derde-verwerkingsverantwoordelijke op grond van Artikel 7.5.1 (Beoordelingen van Beveiligingsdocumentatie); of

ii. een audit op grond van Artikel 7.5.2(a) (Audit door Partner).

b. Naar aanleiding van een verzoek van Partner op grond van Artikel 7.5.3(a), zullen Google en Partner vooraf overleg voeren en overeenstemming bereiken over:

i. beveiligings- en vertrouwelijkheidsmaatregelen die van toepassing zijn op elke toegang tot de SOC-rapporten door een derde-verwerkingsverantwoordelijke op grond van Artikel 7.5.1 (Beoordelingen van Beveiligingsdocumentatie); en

ii. de redelijke startdatum, reikwijdte en duur van beveiligings- en vertrouwelijkheidsmaatregelen die van toepassing zijn op elke audit op grond van Artikel 7.5.2(a) (Audit door Partner).

c. Google kan een vergoeding in rekening brengen (op basis van de redelijke kosten van Google) voor elke audit op grond van Artikel 7.5.2(a) (Audit door Partner). Google zal Partner voorafgaand aan een dergelijke audit nader informeren over eventuele toepasselijke vergoeding en de grondslag voor de

berekening ervan. Partner is verantwoordelijk voor alle vergoedingen die in rekening worden gebracht door een door Partner aangestelde auditor voor het uitvoeren van een dergelijke audit.

d. Google kan schriftelijk bezwaar maken tegen een door Partner aangestelde auditor die een audit uitvoert op grond van Artikel 7.5.2(a) (Audit door Partner), indien de auditor naar het redelijke oordeel van Google niet voldoende gekwalificeerd of onafhankelijk is, een concurrent van Google is, of anderszins kennelijk ongeschikt is. In dat geval dient Partner een andere auditor aan te wijzen of de audit zelf uit te voeren.

e. Alle verzoeken van Partner op grond van Artikel 3 (Specifieke Privacywetgeving) of Artikel 4 (Specifieke Producten) met betrekking tot toegang tot SOC-rapporten voor een derde-verwerkingsverantwoordelijke of voor audits zijn tevens onderworpen aan dit Artikel 7.5.3 (Aanvullende zakelijke voorwaarden voor beoordelingen en audits).

8. Impact Assessments en Raadplegingen

Google zal (rekening houdend met de aard van de verwerking en de informatie waarover Google beschikt) Partner helpen bij het waarborgen van de compliance met haar verplichtingen (of, wanneer Partner een verwerker is, de verplichtingen van de derde-verwerkingsverantwoordelijke) met betrekking tot gegevensbeschermingsbeoordelingen, risicobeoordelingen, voorafgaande raadplegingen met toezichthouders of vergelijkbare procedures op grond van Toepasselijke Privacywetgeving, door:

a. Aanvullende Beveiligingsmechanismen beschikbaar te stellen in overeenstemming met Artikel 7.1.3 (Aanvullende Beveiligingsmechanismen) en de beschikbare Beveiligingsdocumentatie beschikbaar te stellen in overeenstemming met Artikel 7.5.1 (Beoordelingen van Beveiligingsdocumentatie);

b. de informatie in de Overeenkomst (inclusief dit Addendum) te verstrekken; en

c. indien bovenstaande subartikelen (a) en (b) voor Partner (of de derde-verwerkingsverantwoordelijke) onvoldoende zijn om aan dergelijke verplichtingen te voldoen, op verzoek van Partner aanvullende redelijke samenwerking en ondersteuning te bieden.

9. Toegang etc.; Rechten van betrokkenen; Gegevensexport

9.1 *Toegang; Rectificatie; Beperkte verwerking; Overdraagbaarheid*. Gedurende de Looptijd zal Google Partner in staat stellen om, op een wijze in overeenstemming met de functionaliteit van de Diensten, toegang te verkrijgen tot Partnergegevens, Partnergegevens te corrigeren en de verwerking van Partnergegevens te beperken, waaronder via de verwijderfunctie die Google biedt zoals beschreven in Artikel 6.1 (Verwijdering door Partner) en om Partnergegevens te exporteren. Indien Partner constateert dat Partner-Persoonsgegevens onjuist of verouderd zijn, is Partner verantwoordelijk voor het gebruik van een dergelijke functionaliteit om die gegevens te corrigeren of te verwijderen indien de Toepasselijke Privacywetgeving dit vereist.

9.2 *Verzoeken van betrokkenen*.

9.2.1 *Verantwoordelijkheid voor verzoeken*. Gedurende de Looptijd, als het Cloud-gegevensbeschermingsteam van Google een verzoek ontvangt van een betrokkene dat betrekking heeft op Partner-Persoonsgegevens en waarbij Partner wordt geïdentificeerd, zal Google:

a. de betrokkene adviseren om het verzoek bij Partner in te dienen;

b. Partner prompt in kennis stellen; en

c. niet anderszins op het verzoek van die betrokkene reageren zonder toestemming van Partner.

Partner zal verantwoordelijk zijn voor de reactie op dergelijke verzoeken, onder meer, indien nodig, door de functionaliteit van de Diensten te gebruiken.

9.2.2 *Ondersteuning van Google bij verzoeken van betrokkenen*. Google zal (rekening houdend met de aard van de verwerking van Partner-Persoonsgegevens) Partner assisteren bij het voldoen aan zijn verplichtingen (of, als Partner een verwerker is, die van de derde-verwerkingsverantwoordelijke) op grond van Toepasselijke Privacywetgeving om te reageren op verzoeken tot uitoefening van de rechten van betrokkenen door:

a. Aanvullende Beveiligingsmechanismen beschikbaar te stellen in overeenstemming met Artikel 7.1.3 (Aanvullende Beveiligingsmechanismen);

b. Artikel 9.1 (Toegang; Rectificatie; Beperkte verwerking; Overdraagbaarheid) en 9.2.1 (Verantwoordelijkheid voor verzoeken) na te leven; en

c. indien bovenstaande subartikelen (a) en (b) voor Partner (of de derde-verwerkingsverantwoordelijke) onvoldoende zijn om aan dergelijke verplichtingen te voldoen, op verzoek van Partner aanvullende redelijke samenwerking en ondersteuning te bieden.

10. Locaties van gegevensverwerking

10.1 *Opslag- en verwerkingsfaciliteiten voor gegevens*. Behoudens de toezeggingen van Google met betrekking tot gegevenslocaties onder de Servicespecifieke Voorwaarden en de toezeggingen inzake gegevensdoorgifte in Bijlage 3 (Specifieke privacywetgeving), indien van toepassing, kunnen Partnergegevens worden verwerkt in elk land waar Google of zijn Subverwerkers faciliteiten onderhouden.

10.2 *Informatie over datacenters*. De locaties van datacenters van Google worden beschreven in Bijlage 4 (Specifieke producten).

11. Subverwerkers

11.1 *Toestemming voor de inschakeling van Subverwerkers*. Partner geeft Google specifiek toestemming voor de inschakeling door Google als Subverwerkers van die entiteiten die zijn bekendgemaakt zoals beschreven in Artikel 11.2 (Informatie over Subverwerkers), vanaf de Ingangsdatum van het Addendum. Daarnaast geeft Partner, onverminderd het bepaalde in Artikel 11.4 (Mogelijkheid om bezwaar te maken tegen Subverwerkers), in algemene zin toestemming voor de inschakeling door Google van andere derden als Subverwerkers ("*Nieuwe Subverwerkers*").

11.2 *Informatie over Subverwerkers*. Namen, locaties en activiteiten van Subverwerkers worden beschreven in Bijlage 4 (Specifieke producten).

11.3 *Vereisten voor inschakeling van Subverwerkers*. Bij de inschakeling van een Subverwerker, zal Google:

a. via een schriftelijke overeenkomst waarborgen dat:

i. de Subverwerker uitsluitend toegang heeft tot en gebruikmaakt van Partnergegevens voor zover noodzakelijk om de aan hem uitbestede verplichtingen na te komen, en dit doet in overeenstemming met de Overeenkomst (inclusief dit Addendum); en

ii. indien vereist op grond van Toepasselijke Privacywetgeving, de in dit Addendum beschreven gegevensbeschermingsverplichtingen worden opgelegd aan de Subverwerker (zoals nader kan worden beschreven in Bijlage 3 (Specifieke privacywetgeving)); en

b. volledig aansprakelijk blijven voor alle aan Subverwerker uitbestede verplichtingen, alsmede voor alle handelingen en nalatigheden van de Subverwerker.

11.4 *Mogelijkheid om bezwaar te maken tegen Subverwerkers*.

a. Wanneer Google gedurende de Looptijd Nieuwe Subverwerkers inschakelt, stelt Google Partner ten minste 30 dagen voordat de Nieuwe Subverwerker Partnergegevens gaat verwerken op de hoogte van de inschakeling (inclusief de naam, locatie en activiteiten van de Nieuwe Subverwerker).

b. Partner kan, binnen 90 dagen nadat deze op de hoogte is gesteld van de inschakeling van een Nieuwe Subverwerker, bezwaar maken door de Overeenkomst met onmiddellijke ingang en zonder opgave van redenen (*for convenience*) te beëindigen:

i. in overeenstemming met de bepaling inzake beëindiging zonder opgave van redenen (*for convenience*) in de Overeenkomst; of

ii. indien een dergelijke bepaling ontbreekt, door Google in kennis te stellen.

12. Cloud-gegevensbeschermingsteam; Verwerkingsregisters

12.1 *Cloud-gegevensbeschermingsteam*. Het Cloud-gegevensbeschermingsteam van Google zal prompte en redelijke ondersteuning bieden bij elke vraag van Partner met betrekking tot de verwerking van Partnergegevens op grond van de Overeenkomst en kan worden gecontacteerd op de wijze zoals beschreven in het Artikel 'Kennisgevingen' van de Overeenkomst of in Bijlage 4 (Specifieke producten).

12.2 *Verwerkingsregisters van Google*. Google zal passende documentatie bijhouden over verwerkingsactiviteiten zoals vereist door de Toepasselijke Privacywetgeving. Voor zover Google op grond van Toepasselijke Privacywetgeving verplicht is bepaalde gegevens met betrekking tot Partner en zijn Klanten te verzamelen en bij te houden, gebruikt Partner de Admin Console of andere middelen zoals aangegeven in Bijlage 4 (Specifieke producten) om dergelijke gegevens te verstrekken en deze nauwkeurig en up-to-date te houden. Google kan dergelijke informatie beschikbaar stellen aan bevoegde toezichthouders, waaronder een Toezichthoudende Autoriteit, indien vereist door Toepasselijke Privacywetgeving.

12.3 *Verzoeken van verwerkingsverantwoordelijken*. Gedurende de Looptijd, als het Cloud-gegevensbeschermingsteam van Google een verzoek of instructie beoordeelt van een derde die

beweert verwerkingsverantwoordelijke te zijn van Partner-Persoonsgegevens, adviseert Google deze derde om contact op te nemen met Partner.

13. Kennisgevingen

Kennisgevingen op grond van dit Addendum (inclusief kennisgevingen van Gegevensincidenten) zullen worden verzonden naar het E-mailadres voor Kennisgevingen. Het is de verantwoordelijkheid van Partner via de Admin Console, of door Google anderszins in kennis te stellen, ervoor te zorgen dat zijn E-mailadres voor Kennisgevingen actueel en geldig blijft.

14. Uitleg

14.1 *Voorrang*. Voor zover er een conflict bestaat tussen:

a. Bijlage 3 (Specifieke privacywetgeving) en de rest van het Addendum (inclusief Bijlage 4 (Specifieke producten)), prevaleert Bijlage 3;

b. Bijlage 4 (Specifieke producten) en de rest van het Addendum (exclusief Bijlage 3), prevaleert Bijlage 4; en

c. dit Addendum en de rest van de Overeenkomst, prevaleert dit Addendum.

14.2 *Verwijzingen naar Artikelen*. Tenzij anders aangegeven, zijn alle verwijzingen naar Artikelen in een Bijlage van dit Addendum verwijzingen naar Artikelen in de Algemene voorwaarden van het Addendum.

14.3 *Klanten*. Voor alle duidelijkheid: Klanten zijn geen derden die rechten kunnen ontlenen aan dit Addendum.

Bijlage 1: Onderwerp en details van gegevensverwerking

Onderwerp

Googles levering van Diensten en TSS aan Partner.

Duur van de verwerking

De Looptijd plus de periode vanaf het einde van de Looptijd tot aan de verwijdering van alle Partnergegevens door Google in overeenstemming met dit Addendum.

Aard en doel van de verwerking

Google zal Partner-Persoonsgegevens verwerken met het doel de Diensten en TSS te leveren aan Partner in overeenstemming met dit Addendum.

Categorieën van gegevens

Gegevens betreffende aan individuen die via de Diensten aan Google worden verstrekt, door (of in opdracht van) Partner of de Eindgebruikers van Partner.

Betrokkenen

Betrokkenen omvatten de personen over wie gegevens aan Google worden verstrekt via de Diensten, door (of in opdracht van) Partner of diens Klanten, of door Eindgebruikers van Partner.

Bijlage 2: Beveiligingsmaatregelen

Vanaf de Ingangsdatum van het Addendum zal Google de in deze Bijlage 2 beschreven Beveiligingsmaatregelen implementeren en onderhouden.

1. Datacenter- en netwerkbeveiliging

(a) Datacenters.

Infrastructuur. Google onderhoudt geografisch verspreide datacenters. Google slaat alle productiegegevens op in fysiek beveiligde datacenters.

Redundantie. De infrastructuursystemen zijn ontworpen om enkelvoudige storingspunten te elimineren en de impact van voorzienbare omgevingsrisico's te minimaliseren. Dubbele circuits, switches, netwerken of andere noodzakelijke apparaten helpen deze redundantie te bieden. De Diensten zijn ontworpen om Google in staat te stellen bepaalde soorten preventief en correctief onderhoud zonder uit te voeren zonder onderbreking. Alle omgevingsapparatuur en -faciliteiten beschikken over schriftelijk vastgelegde procedures voor preventief onderhoud, waarin het proces voor en de frequentie van de uitvoering wordt beschreven in overeenstemming met de specificaties van de fabrikant of interne specificaties. Preventief en correctief onderhoud van de datacenterapparatuur wordt gepland via een standaard wijzigingsproces volgens gedocumenteerde procedures.

Stroomvoorziening. De elektriciteitssystemen van de datacenters zijn ontworpen om redundant en onderhoudbaar te zijn zonder impact op de continue bedrijfsvoering, 24 uur per dag, 7 dagen per week. In de meeste gevallen wordt zowel een primaire als een alternatieve stroombron, elk met gelijke capaciteit, voorzien voor kritieke infrastructuurcomponenten in het datacenter. Noodstroom wordt geleverd door verschillende mechanismen zoals UPS-batterijen (Uninterruptible Power Supplies, UPS), die consistent betrouwbare stroombeveiliging bieden tijdens elektriciteitsstoringen, stroomuitval, overspanning, onderspanning en frequentiecondities buiten tolerantie. Indien de netstroom wordt onderbroken, is de noodstroom ontworpen om tot maximaal 10 minuten stroom transitorische te leveren aan het datacenter, op volle capaciteit, totdat de noodgeneratoren het overnemen. De noodgeneratoren kunnen automatisch binnen enkele seconden opstarten en voldoende noodstroom leveren om het datacenter doorgaans gedurende een aantal dagen op volle capaciteit te laten draaien.

Serverbesturingssystemen. Google-servers gebruiken een Linux-gebaseerde implementatie aangepast voor de toepassingsomgeving. Gegevens worden opgeslagen met behulp van algoritmes die eigendom zijn van Google om de gegevensbeveiliging en redundantie te vergroten.

Codekwaliteit. Google hanteert een beoordelingsproces voor codes om de beveiliging van de code die wordt gebruikt om de Diensten te leveren te vergroten en de beveiligingsproducten in productieomgevingen te verbeteren.

Bedrijfscontinuïteit. Google heeft bedrijfscontinuïteitsplannen/rampherstelprogramma's ontworpen en plant en test deze regelmatig.

(*b) Netwerken en transmissie.*

Gegevensoverdracht. Datacenters zijn doorgaans verbonden via privéverbindingen met hoge snelheid die zorgen voor een beveiligde en snelle gegevensoverdracht tussen datacenters. Dit is ontworpen om te voorkomen dat de gegevens tijdens de elektronische overdracht of transport, of wanneer ze worden opgeslagen op gegevensdragers, zonder autorisatie kunnen worden gelezen, gekopieerd, gewijzigd of verwijderd. Google draagt gegevens over via internet-standaardprotocollen.

Externe aanvalsoppervlak. Google maakt gebruik van meerdere lagen netwerkapparaten en indringingsdetectie om zijn externe aanvalsoppervlak te beschermen. Google houdt rekening met potentiële aanvalsvectoren en past passende, speciaal ontwikkelde technologieën toe in extern gerichte systemen.

Indringingsdetectie. Indringingsdetectie is bedoeld om inzicht te verschaffen in lopende aanvalsactiviteiten en om toereikende informatie te bieden om op incidenten te reageren. De indringingsdetectie van Google omvat (i) het strikt beheersen van de omvang en samenstelling van het aanvalsoppervlak van Google door middel van preventieve maatregelen; (ii) het toepassen van intelligente detectiecontroles op gegevensinvoerpunten; en (iii) het toepassen van technologieën die bepaalde gevaarlijke situaties automatisch verhelpen.

Incidentrespons. Google monitort verschillende communicatiekanalen op beveiligingsincidenten en de veiligheidsmedewerkers van Google zullen prompt reageren op bekende incidenten.

Versleutelingstechnologieën. Google stelt HTTPS-versleuteling (ook wel SSL- of TLS-verbinding genoemd) ter beschikking. De servers van Google ondersteunen efemere elliptische-curve Diffie-Hellman cryptografische sleuteluitwisseling ondertekend met RSA en ECDSA. Deze Perfect Forward Secrecy-methoden (PFS) helpen om het verkeer te beschermen en de impact van een gecompromitteerde sleutel of een cryptografische doorbraak te minimaliseren.

2. Toegangs- en locatiecontroles

(a) Locatiecontroles.

Beveiligingsactiviteiten voor datacenters op de locatie. De datacenters van Google beschikken over een beveiligingsoperatie ter plaatse die verantwoordelijk is voor alle fysieke beveiligingsfuncties van het datacenter, 24 uur per dag, 7 dagen per week. Het beveiligingspersoneel bewaakt CCTV-camera's (gesloten circuit van beveiligingscamera's) en alle alarmsystemen. Het beveiligingspersoneel op locatie voert regelmatig interne en externe patrouilles bij het datacenter uit.

Toegangsprocedures voor datacenters. Google maakt gebruik van formele toegangsprocedures voor het toestaan van fysieke toegang tot de datacenters. De datacenters bevinden zich in faciliteiten waarvoor toegang met behulp van een elektronische toegangspas vereist is en die zijn voorzien van alarmen die met de beveiligingsoperatie op locatie zijn verbonden. Iedereen die het datacenter betreedt, is verplicht om zich te identificeren en een identiteitsbewijs te tonen aan de beveiliging op locatie. Alleen geautoriseerde medewerkers, onderaannemers en bezoekers hebben toegang tot datacenters. Alleen geautoriseerde medewerkers en onderaannemers kunnen toegang tot deze faciliteiten met behulp van een elektronische toegangspas aanvragen. Elektronische toegangspassen voor datacenters moeten via e-mail worden aangevraagd en vereisen de goedkeuring van de manager

van de aanvrager en de directeur van het datacenter. Alle overige bezoekers die tijdelijk toegang willen krijgen tot het datacenter moeten: (i) vooraf goedkeuring krijgen van de managers van het datacenter voor het specifieke datacenter en de interne zones die ze willen bezoeken; (ii) zich aanmelden bij de beveiligingsoperatie op locatie; en (iii) een erkend bewijs van toegang tot het datacenter tonen waarin staat dat de persoon is goedgekeurd.

Beveiligingsapparaten voor datacenters op de locatie. De datacenters van Google gebruiken een toegangscontrolesysteem met dubbele authenticatie dat gekoppeld is aan een alarmsysteem. Dit systeem bewaakt en registreert het gebruik van toegangskaarten bij buitendeuren, verzend- en ontvangstzones en andere kritieke zones. Ongeautoriseerde activiteiten en mislukte toegangspogingen worden door het toegangscontrolesysteem vastgelegd en, indien passend, onderzocht. Toegang tot de bedrijfsactiviteiten en datacenters is beperkt op basis van zones en de functieverantwoordelijkheden van de persoon. De branddeuren van de datacenters zijn voorzien van een alarm. CCTV-camera's bewaken binnen- en buitengebieden van het datacenter. De camera's zijn zo geplaatst dat ze strategische gebieden beslaan, waaronder de omheining, deuren tot het datacentergebouw en de verzend- en ontvagstzones. Het beveiligingspersoneel op locatie beheert de bewakings-, opname- en besturingsapparatuur. Beveiligde kabels verbinden de bewakingsapparatuur in alle datacenters. Camera's maken 24 uur per dag en 7 dagen per week op locatie opnamen via digitale videorecorders. De bewakingsopnames worden tot wel 30 dagen bewaard, afhankelijk van de activiteit.

(b) Toegangscontrole.

Beveiligingspersoneel voor infrastructuur. Google beschikt over een beveiligingsbeleid en handhaaft dit beleid, en vereist beveiligingstraining als onderdeel van het opleidingspakket voor haar personeel. Het beveiligingspersoneel voor infrastructuur van Google is verantwoordelijk voor het continu monitoren van de beveiligingsinfrastructuur van Google, het beoordelen van de Diensten en het reageren op beveiligingsincidenten.

Toegangscontrole en beheer van rechten. Beheerders en Eindgebruikers van Partner moeten zich authenticeren via een centraal verificatiesysteem of via een single sign-on-systeem om de Diensten te gebruiken.

Interne processen en beleidsregels voor gegevenstoegang – Toegangsbeleid. Googles interne processen en beleidsregels voor gegevenstoegang zijn ontworpen om te voorkomen dat onbevoegde personen en systemen toegang krijgen tot systemen die worden gebruikt om Partnergegevens te verwerken. Google ontwerpt de systemen zodanig dat (i) alleen geautoriseerde personen toegang hebben tot gegevens waarvoor ze geautoriseerd zijn; en (ii) Partnergegevens tijdens verwerking, gebruik en na opslag niet zonder autorisatie kunnen worden gelezen, gekopieerd, gewijzigd of verwijderd. De systemen zijn ontworpen om ongepaste toegang te detecteren. Google maakt gebruik van een centraal toegangsbeheersysteem om de toegang van personeel tot productieservers te controleren en geeft alleen toegang aan een beperkt aantal geautoriseerde medewerkers. De verificatie- en autorisatiesystemen van Google gebruiken SSH-certificaten en beveiligingssleutels en zijn ontworpen om Google van beveiligde en flexibele toegangsmechanismen te voorzien. Deze mechanismen zijn ontworpen om alleen goedgekeurde toegangsrechten te verstrekken tot site-hosts, logbestanden, gegevens en configuratie-informatie. Google vereist het gebruik van unieke gebruikers-ID's, sterke wachtwoorden, tweefactorauthenticatie en zorgvuldig gemonitorde

toegangslijsten om het risico op ongeautoriseerd accountgebruik te minimaliseren. Het toekennen of wijzigen van toegangsrechten is gebaseerd op: de functie en verantwoordelijkheden van de geautoriseerde medewerker; de functieverplichtingen die nodig zijn om de geautoriseerde taken uit te voeren; en het *need-to-know*-principe. Het toekennen of wijzigen van toegangsrechten moet bovendien in overeenstemming zijn met de interne toegangsbeleidsregels en trainingen van Google. Goedkeuringen worden beheerd via workflowtools die auditrecords bijhouden van alle wijzigingen. Toegang tot systemen wordt gelogd om een audittrail te creëren voor verantwoording. Waar wachtwoorden worden gebruikt voor authenticatie (bijv. inlog op werkstations), wordt een wachtwoordbeleid toegepast dat ten minste voldoet aan de geldende industriestandaarden. Deze standaarden omvatten beperkingen op wachtwoordhergebruik en vereisten voor voldoende wachtwoordsterkte. Voor toegang tot uiterst gevoelige informatie (bijv. creditcardgegevens) gebruikt Google hardwaretokens.

3. Gegevens

(a) *Gegevensopslag, isolatie en logging*. Google slaat gegevens op in een multi-tenantomgeving op servers die eigendom zijn van Google. Behoudens eventuele andersluidende Instructies (bijvoorbeeld in de vorm van een selectie van een gegevenslocatie) repliceert Google Partnergegevens tussen meerdere geografisch verspreide datacenters. Ook isoleert Google Partnergegevens op logische wijze. Partner krijgt controle over specifieke beleidsregels inzake gegevensdeling. Die beleidsregels zullen, in overeenstemming met de functionaliteit van de Diensten, Partner in staat stellen om de productdelingsinstellingen te bepalen die van toepassing zijn op Eindgebruikers van Partner voor specifieke doeleinden. Partner kan ervoor kiezen om de loggingsfunctionaliteit te gebruiken die Google beschikbaar stelt via de Diensten.

(b) *Uitgefaseerde schijven en beleid voor het wissen van schijven*. Schijven die gegevens bevatten kunnen prestatieproblemen, fouten of hardwareproblemen ondervinden die ertoe leiden dat ze worden uitgefaseerd ("Uitgefaseerde Schijf"). Elke Uitgefaseerde Schijf is onderworpen aan een reeks processen voor gegevensvernietiging (het "Beleid voor het wissen van schijven") voordat deze de gebouwen van Google verlaat voor hergebruik of vernietiging. Uitgefaseerde Schijven worden gewist in een proces dat uit meerdere stappen bestaat en de voltooiing hiervan wordt geverifieerd door ten minste twee onafhankelijke validators. De wisresultaten worden in een logbestand vastgelegd op basis van het serienummer van de Uitgefaseerde Schijf voor tracking. Tot slot wordt de gewiste Uitgefaseerde Schijf vrijgegeven voor hergebruik en nieuwe inzet. Indien de Uitgefaseerde Schijf niet kan worden gewist als gevolg van een hardwareprobleem, wordt de schijf beveiligd opgeslagen totdat deze kan worden vernietigd. Elke faciliteit wordt regelmatig gecontroleerd op compliance met het Beleid voor het wissen van schijven.

4. Personeelsbeveiliging

Google-personeel is verplicht zich te gedragen in overeenstemming met de richtlijnen van het bedrijf inzake vertrouwelijkheid, bedrijfsethiek, passend gebruik en professionele standaarden. Google voert, voor zover wettelijk toegestaan en in overeenstemming met de toepasselijke lokale arbeidswetgeving en wettelijke voorschriften, redelijk passende antecedentenonderzoeken uit.

Google-personeel is verplicht een geheimhoudingsovereenkomst te ondertekenen en dient de ontvangst van en compliance met Googles vertrouwelijkheids- en privacybeleid te bevestigen.

Personeel krijgt beveiligingstraining. Personeel dat Partnergegevens verwerkt, moet aanvullende eisen voltooien die passend zijn voor hun rol (bijvoorbeeld certificeringen). Google-personeel zal Partnergegevens niet verwerken zonder autorisatie.

5. Beveiliging bij Subverwerkers

Voordat Subverwerkers worden ingeschakeld, voert Google een audit uit van hun beveiligings- en privacypraktijken om te waarborgen dat de Subverwerkers een beveiligings- en privacyniveau bieden dat passend is bij hun toegang tot gegevens en de reikwijdte van de diensten die zij geact worden te leveren. Zodra Google de risico's verbonden aan de Subverwerker heeft beoordeeld, en onverminderd de vereisten beschreven in Sectie 11.3 (Vereisten voor de inschakeling van Subverwerkers), is de Subverwerker verplicht passende contractuele bepalingen inzake beveiliging, vertrouwelijkheid en privacy aan te gaan.

Bijlage 3: Specifieke privacywetgeving

De voorwaarden in ieder onderdeel van deze Bijlage 3 zijn uitsluitend van toepassing wanneer de overeenkomstige wetgeving van toepassing is op de verwerking van Partner-Persoonsgegevens.

Europese Gegevensbeschermingswetgeving

1. Aanvullende definities.

- *"Adequaat Land"* betekent:

(a) voor verwerkte gegevens onderworpen aan de EU-AVG: de Europese Economische Ruimte, of een land of gebied dat erkend is als een land dat een adequaat beschermingsniveau garandeert op grond van de EU-AVG;

(b) voor verwerkte gegevens onderworpen aan de VK-AVG: het Verenigd Koninkrijk of een land of gebied dat erkend is als een land dat een adequaat beschermingsniveau garandeert op grond van de VK-AVG en de Data Protection Act 2018; of

(c) voor verwerkte gegevens onderworpen aan de Zwitserse FADP: Zwitserland, of een land of gebied dat: (i) vermeld staat op de lijst met staten waarvan de wetgeving adequate beveiliging garandeert zoals gepubliceerd door de Zwitserse Federal Data Protection and Information Commissioner, indien van toepassing; of (ii) erkend is als een land dat adequate beveiliging garandeert door de Zwitserse Bondsraad onder de Zwitserse FADP;

in elk geval, anders dan op basis van een optioneel gegevensbeschermingskader.

- *"Alternatieve Doorgifteoplossing"* betekent, voor de doeleinden van deze voorwaarden inzake Europese Gegevensbeschermingswetgeving, een oplossing, anders dan SCC's, die de rechtmatige doorgifte van persoonsgegevens naar een derde land mogelijk maakt in overeenstemming met de Europese Gegevensbeschermingswetgeving, bijvoorbeeld een gegevensbeschermingskader dat wordt erkend als waarborgend dat de deelnemende entiteiten een adequaat beschermingsniveau bieden.

- *"Partner-SCC's"* betekent de SCC's (Verwerkingsverantwoordelijke-naar-Verwerker), de SCC's (Verwerker-naar-Verwerker) of de SCC's (Verwerker-naar-Verwerkingsverantwoordelijke), naar gelang van toepassing.

- *"SCC's"* betekent de SCC's van Partner of de SCC's (Verwerker-naar-Verwerker, Google Exporteur), naargelang van toepassing.

- *"SCC's (Verwerkingsverantwoordelijke-naar-Verwerker)"* betekent de voorwaarden op: https://cloud.google.com/terms/sccs/eu-c2p

- *"SCC's (Verwerker-naar-Verwerkingsverantwoordelijke)"* betekent de voorwaarden op: https://cloud.google.com/terms/sccs/eu-p2c

- *"SCC's (Verwerker-naar-Verwerker)"* betekent de voorwaarden op: https://cloud.google.com/terms/sccs/eu-p2p

- *"SCC's (Verwerker-naar-Verwerker, Google Exporteur)"* betekent de voorwaarden op: https://cloud.google.com/terms/sccs/eu-p2p-google-exporter

2. Kennisgevingen over Instructies. Onverminderd de verplichtingen van Google op grond van Artikel 5.2 (Compliance met de Instructies van Partner) of andere rechten of verplichtingen van beide partijen op grond van de Overeenkomst, zal Google Partner onmiddellijk in kennis stellen indien, naar mening van Google:

a. Europees Recht Google verbiedt om een Instructie op te volgen;

b. een Instructie niet voldoet aan Europese Gegevensbeschermingswetgeving; of

c. Google anderszins niet in staat is om een Instructie op te volgen;

en in ieder geval tenzij een dergelijke kennisgeving verboden is op grond van Europees Recht.

Indien Partner een verwerker is, stuurt Partner elke door Google verstrekte kennisgeving op grond van dit Artikel onmiddellijk door naar de derde-verwerkingsverantwoordelijke.

3. Auditrechten van Partner. Google zal Partner of een door Partner aangestelde onafhankelijke auditor toestaan audits (inclusief inspecties) uit te voeren zoals beschreven in Artikel 7.5.2(a) (Audit door Partner). Tijdens een dergelijke audit zal Google alle informatie beschikbaar stellen die nodig is om de verplichtingen op grond van dit Addendum na te komen en zal Google meewerken aan de Audit zoals beschreven in Artikel 7.5 (Beoordelingen en controles met betrekking tot compliance) en dit artikel.

4. Gegevensdoorgiften.

4.1 *Beperkte doorgiften*. De partijen erkennen dat de Europese Gegevensbeschermingswetgeving geen SCC's of een Alternatieve Doorgifteoplossing vereist om Partner-Persoonsgegevens te verwerken in of door te geven naar een Adequaat Land. Indien Partner-Persoonsgegevens worden doorgegeven naar enig ander land en de Europese Gegevensbeschermingswetgeving van toepassing is op de doorgifte

(zoals gecertificeerd door Partner op grond van Artikel 4.2 (Certificering door niet EMEA-Partners) van deze bepalingen van Europese Gegevensbeschermingswetgeving, als het factuuradres buiten de EMEA valt) ("*Beperkte Doorgiften*"), dan geldt het volgende:

a. indien Google een Alternatieve Doorgifteoplossing heeft aangenomen voor Beperkte Doorgiften, zal Google Partner informeren over de relevanteoplossing en zal Google ervoor zorgen dat dergelijke Beperkte Doorgiften in overeenstemming daarmee plaatsvinedn; of

b. indien Google geen Alternatieve Doorgifteoplossing voor Beperkte Doorgiften heeft aangenomen voor enige Beperkte Doorgifte of indien Google Partner informeert dat Google geen Alternatieve Doorgifteoplossing voor Beperkte Doorgiften meer gebruikt (zonder een vervangende Alternatieve Doorgifteoplossing aan te nemen), geldt het volgende:

i. indien het adres van Google zich bevindt in een Adequaat Land:

A. zijn de SCC's (Verwerker-naar-Verwerker, Google Exporteur) van toepassing met betrekking tot dergelijke Beperkte Doorgiften van Google naar Subverwerkers; en

B. bovendien, indien het factuuradres van Partner niet in een Adequaat Land is gelegen, zijn de SCC's (Verwerker-naar-Verwerkingsverantwoordelijke) van toepassing (ongeacht of Partner een verwerkingsverantwoordelijke of een verwerker is) met betrekking tot dergelijke Beperkte Doorgiften tussen Google en Partner; of

ii. als het adres van Google niet in een Adequaat Land is gelegen, zijn de SCC's (Verwerkingsverantwoordelijke-naar-Verwerker) of SCC's (Verwerker-naar-Verwerker) van toepassing (afhankelijk van of Partner een verwerkingsverantwoordelijke of verwerker is) met betrekking tot dergelijke Beperkte Doorgiften tussen Google en Partner.

4.2 *Certificering door niet-EMEA Partners*. Indien het factuuradres van Partner buiten de EMEA ligt en de verwerking van Partner-Persoonsgegevens onderworpen is aan de Europese Gegevensbeschermingswetgeving, dan zal Partner, tenzij anders bepaald in Bijlage 4 (Specifieke Producten) van dit Addendum, dit certificeren en zijn bevoegde Toezichthoudende Autoriteit identificeren via de Admin Console voor de toepasselijke Diensten.

4.3 *Informatie over Beperkte Doorgiften*. Google zal Partner voorzien van informatie die relevant is voor Beperkte Doorgiften, Aanvullende Beveiligingsmechanismen en andere extra beveiligingsmaatregelen:

a. zoals beschreven in Artikel 7.5.1 (Beoordelingen van Beveiligingsdocumentatie);

b. op eventuele aanvullende locaties beschreven in Bijlage 4 (Specifieke producten); en

c. met betrekking tot het in gebruik nemen van een Alternatieve Doorgifteoplossing door Google, op https://cloud.google.com/terms/alternative-transfer-solution.

4.4 *SCC-audits*. Indien er Partner-SCC's van toepassing zijn zoals beschreven in Artikel 4.1 (Beperkte Doorgiften) van deze voorwaarden inzake Europese Gegevensbeschermingswetgeving, zal Google Partner (of een door Partner aangestelde onafhankelijke auditor) toestaan om audits uit te voeren zoals beschreven in die SCC's en tijdens een audit alle informatie beschikbaar stellen die door die SCC's

wordt vereist, beide in overeenstemming met Artikel 7.5.3 (Aanvullende zakelijke voorwaarden voor beoordelingen en audits).

4.5 *SCC's en derde-verwerkingsverantwoordelijken*. Indien Partner een verwerker is, erkent Partner dat Google, als een andere verwerker, mogelijk niet in staat is de derde-verwerkingsverantwoordelijke te identificeren. Partner zal daarom iedere kennisgeving met betrekking tot SCC's prompt en zonder onnodige vertraging doorsturen naar de derde-verwerkingsverantwoordelijke.

4.6 *Beëindiging wegens risico's bij gegevensdoorgifte*. Indien Partner op basis van het huidige of beoogde gebruik van de Diensten tot de conclusie komt dat er geen passende waarborgen worden geboden voor de doorgifte van Partner-Persoonsgegevens, kan Partner de Overeenkomst met onmiddelijke ingang beëindigen in overeenstemming met de bepaling inzake beëindiging zonder opgave van redenen (*for convenience*) in de Overeenkomst; of, indien een dergelijke bepaling ontbreekt, door Google hiervan op de hoogte te stellen.

4.7 *Geen wijziging van SCC's*. Niets in de Overeenkomst (inclusief dit Addendum) is bedoeld om SCC's te wijzigen of tegen te spreken, of om afbreuk te doen aan de fundamentele rechten of vrijheden van betrokkenen op grond van Europese Gegevensbeschermingswetgeving.

4.8 *Voorrang van SCC's*. Voor zover er een conflict of inconsistentie bestaat tussen Partner-SCC's (door middel van verwijzing opgenomen in dit Addendum) en de rest van de Overeenkomst (inclusief dit Addendum), prevaleren de Partner-SCC's.

5. Vereisten voor de inschakeling van Subverwerkers.

De Europese Gegevensbeschermingswetgeving vereist dat Google, via een schriftelijke overeenkomst, waarborgt dat de in dit Addendum beschreven verplichtingen inzake gegevensbescherming, en die worden bedoeld in Artikel 28(3) van de AVG, indien van toepassing, worden opgelegd aan iedere door Google ingeschakelde Subverwerker.

CCPA

1. Aanvullende definities.

- *"CCPA"* betekent de *California Consumer Privacy Act* van 2018, zoals gewijzigd, inclusief de wijzigingen aangebracht door de *California Privacy Rights Act* van 2020, samen met alle uitvoeringsregelingen.

- *"Partner-Persoonsgegevens"* omvat 'persoonlijke informatie'.

- De termen 'bedrijf', 'zakelijk doel', 'consument', 'persoonlijke informatie', 'verwerking', 'verkoop', 'verkopen', 'aanbieder', en 'delen' hebben de betekenis zoals vermeld in de CCPA.

2. Verboden. Onverminderd de verplichtingen van Google op grond van Artikel 5.2 (Compliance met de Instructies van Partner), met betrekking tot de verwerking van Partner-Persoonsgegevens in overeenstemming met de CCPA, zal Google het volgende niet doen, tenzij toegestaan onder de CCPA:

a. Partner-Persoonsgegevens verkopen of delen;

b. Partner-Persoonsgegevens bewaren, gebruiken of openbaar maken:

i. anders dan voor een zakelijke doeleinde (*"business purpose"*) op grond van de CCPA namens Partner en met het specifieke doel de Diensten en TSS te leveren; of

ii. buiten de directe zakelijke relatie tussen Google en Partner om; of

c. Partner-Persoonsgegevens combineren of bijwerken met persoonlijke informatie (*"personal information"*) die Google van of namens een derde ontvangt of verzamelt via eigen interacties met de consument.

3. Compliance. Onverminderd de verplichtingen van Google op grond van Artikel 5.2 (Compliance met de Instructies van Partner) of andere rechten of verplichtingen van een der partijen op grond van de Overeenkomst, zal Google Partner op de hoogte stellen indien Google, naar eigen mening, niet in staat is om haar verplichtingen op grond van de CCPA na te komen, tenzij een dergelijke kennisgeving op grond van de toepasselijke wetgeving niet is toegestaan.

4. Interventie door Partner. Indien Google Partner in kennis stelt van enig ongeoorloofd gebruik van Partner-Persoonsgegevens, waaronder op grond van Artikel 3 (Compliance) van dit onderdeel of Artikel 7.2.1 (Kennisgeving van incidenten), kan Partner redelijke en passende maatregelen nemen om dergelijk ongeoorloofd gebruik te beëindigen of te verhelpen door:

a. maatregelen te nemen die door Google worden aanbevolen krachtens Artikel 7.2.2 (Details van Gegevensincident), indien van toepassing; of

b. zijn rechten uit te oefenen onder Artikel 7.5.2(a) (Audit door Partner) of 9.1 (Toegang; Rectificatie; Beperkte verwerking; Overdraagbaarheid).

Turkije

1. Aanvullende definities.

- "*Turkse Gegevensbeschermingswetgeving*" betekent de Turkse wetgeving inzake de escherming van persoonsgegevens nr. 6698 van 7 april 2016.
- "*Turkse Gegevensbeschermingsautoriteit*" betekent de Kişisel Verileri Koruma Kurumu.
- "*Turkse SCC's*" betekent de standaardcontractbepalingen op grond van de Turkse Gegevensbeschermingswetgeving.

2. Gegevensdoorgiften.

2.1 *Aanvullende voorwaarden.* Indien het factuuradres van Partner zich in Turkije bevindt en Google optionele aanvullende voorwaarden (inclusief Turkse SCC's) beschikbaar stelt voor aanvaarding door Partner met betrekking tot de doorgifte van Partner-Persoonsgegevens op grond van de Turkse Gegevensbeschermingswetgeving, vormen deze voorwaarden een aanvulling op dit Addendum vanaf de datum waarop ze aan de Turkse Gegevensbeschermingsautoriteit worden gemeld in overeenstemming met Artikel 2.2 (Kennisgeving aan de bevoegde autoriteit), zoals door Partner aan Google aangetoond.

2.2 *Kennisgeving aan de bevoegde autoriteit*. Indien Partner Turkse SCC's aangaat op grond van dit Artikel 2 (Gegevensdoorgiften), is Partner verantwoordelijk voor het op de hoogte stellen van desbetreffende Turkse Gegevensbeschermingsautoriteit van Turkse SCC's binnen vijf (5) werkdagen na ondertekening van de Turkse SCC's zoals vereist door de Turkse Gegevensbeschermingswetgeving.

2.3 *SCC-audits*. Indien Partner Turkse SCC's aangaat op grond van dit Artikel 2 (Gegevensdoorgiften), staat Google Partner (of een door Partner aangestelde onafhankelijke auditor) toe om audits uit te voeren zoals beschreven in die SCC's en, stelt Google tijdens een audit alle door die SCC's vereiste informatie beschikbaar, beide in overeenstemming met Artikel 7.5.3 (Aanvullende zakelijke voorwaarden voor beoordelingen en audits).

2.4 *Beëindiging wegens risico's bij gegevensdoorgifte*. Indien Partner op basis van het huidige of beoogde gebruik van de Diensten tot de conclusie komt dat er geen passende waarborgen worden geboden voor de doorgifte van Partner-Persoonsgegevens, kan Partner de Overeenkomst met onmiddellijke ingang beëindigen in overeenstemming met de bepaling inzake beëindiging zonder opgave van redenen in de Overeenkomst; of, indien een dergelijke voorwaarde ontbreekt, door Google hiervan in kennis te stellen.

2.5 *Geen wijziging van Turkse SCC's*. Niets in de Overeenkomst (inclusief dit Addendum) is bedoeld om de Turkse SCC's te wijzigen of tegen te spreken, of om afbreuk te doen aan de fundamentele rechten of vrijheden van betrokkenen op grond van de Turkse Gegevensbeschermingswetgeving.

2.6 *Voorrang van SCC's*. Voor zover er een conflict of inconsistentie bestaat tussen de Turkse SCC's (door middel van verwijzing opgenomen in dit Addendum, indien Partner deze aangaat) en de rest van de Overeenkomst (inclusief dit Addendum), prevaleren de Turkse SCC's.

Israël

1. Aanvullende definitie.

- *"Israëlische Privacybeschermingswetgeving"* betekent de Israëlische Wet inzake Privacybescherming van 1981 en alle daarop gebaseerde regelingen.

2. Equivalente termen. Alle termen die gelijkwaardig zijn aan "verwerkingsverantwoordelijke", "persoonsgegevens", "verwerking" en "verwerker", zoals gebruikt in dit Addendum, hebben de betekenis die daaraan is gegeven in de Israëlische Privacybeschermingswetgeving.

3. Auditrechten van Partner. Google zal Partner of een door Partner aangestelde onafhankelijke auditor toestaan om audits (inclusief inspecties) uit te voeren zoals beschreven in Artikel 7.5.2(a) (Audit door Partner).

Brazilië

1. **Aanvullende definities**
   - "Adequaat Land" betekent, voor gegevens die worden verwerkt krachtens de LGPD, Brazilië of een land of internationale organisatie die door de Braziliaanse Gegevensbeschermingsautoriteit (ANPD, volgens de Portugese afkorting) wordt erkend als zijnde van een passend beschermingsniveau krachtens de LGPD.

- "Alternatieve doorgifteoplossing" betekent, voor de doeleinden van deze Braziliaanse voorwaarden, een oplossing, anders dan de BR SCC's, die een rechtmatige internationale doorgifte van persoonsgegevens mogelijk maakt in overeenstemming met de LGPD.
- BR SCC's" betekent de BR SCC's (Verwerkingsverantwoordelijke-naar-Verwerker), de BR SCC's (Verwerker-naar-Verwerker) of de BR SCC's (Verwerker-naar-Verwerker, Google Exporter), indien van toepassing.
- "BR SCC's (Verwerkingsverantwoordelijke-naar-Verwerker)" betekent de voorwaarden op https://cloud.google.com/sccs/br-c2p?hl=pt-br.
- "BR SCC's (Verwerker-naar-Verwerker)" betekent de voorwaarden op https://cloud.google.com/sccs/br-p2p?hl=pt-br.
- "BR SCC's (Verwerker-naar-Verwerker, Google Exporter)" betekent de voorwaarden op https://cloud.google.com/sccs/br-p2p-intra-group?hl=pt-br.
- "LGPD" betekent de Braziliaanse Wet nr. 13.709/2018, zoals gewijzigd.

2. Kennisgevingen met betrekking tot instructies.

Onverminderd Googles verplichtingen krachtens Artikel 5.2 (Naleving van de instructies van Partner) of enige andere rechten of verplichtingen van beide partijen onder de toepasselijke Overeenkomst, stelt Google de Partner onmiddellijk op de hoogte indien Google van mening is dat:

a. De Braziliaanse wet Google verbiedt een Instructie na te leven;
b. Een instructie niet in overeenstemming is met de LGPD; of
c. Google om een andere reden niet in staat is een Instructie na te leven,

En dit in elk geval tenzij een dergelijke kennisgeving verboden is op grond van de Braziliaanse wet.

Indien Partner optreedt als verwerker, zal Partner elke door Google vastgestelde kennisgeving krachtens dit Artikel onmiddellijk doorsturen naar de derde-verwerkingsverantwoordelijke.

3. **Data Transfers.**

3.1. *Beperkte doorgiften*. De partijen erkennen dat de LGPD niet vereist dat BR SCC's of een Alternatieve doorgifteoplossing worden toegepast om Partner-Persoonsgegevens te verwerken in of door te geven aan een Adequaat Land. Indien Partner-Persoonsgegevens worden doorgegeven aan enig ander land en de LGPD van toepassing is op die doorgiften ("BR Beperkte Doorgiften"), dan geldt het volgende:

a. indien Google een Alternatieve doorgifteoplossing heeft aangenomen voor enige BR Beperkte Doorgiften, informeert Google de Partner over de desbetreffende oplossing en zorgt Google ervoor dat dergelijke doorgiften plaatsvinden in overeenstemming daarmee; of

b. indien Google geen Alternatieve doorgifteoplossing heeft aangenomen voor enige BR Beperkte Doorgiften, of de Partner informeert dat Google niet langer een Alternatieve doorgifteoplossing toepast voor enige BR Beperkte Doorgiften (zonder een vervangende Alternatieve doorgifteoplossing aan te nemen):

i. indien Googles adres zich in een Adequaat Land bevindt, zijn de BR SCC's (Verwerker-naar-Verwerker, Google Exporter) van toepassing op dergelijke doorgiften van Google naar Subverwerkers; of

ii. indien Googles adres zich niet in een Adequaat Land bevindt, zijn de BR SCC's (Verwerkingsverantwoordelijke-naar-Verwerker) of BR SCC's (Verwerker-naar-Verwerker) van toepassing (afhankelijk van of Partner optreedt als verwerkingsverantwoordelijke of verwerker) op dergelijke doorgiften tussen Google en Partner.

3.2. *Informatie over beperkte doorgiften*. Google verstrekt de Partner informatie met betrekking tot BR Beperkte Doorgiften, Aanvullende Beveiligingsmaatregelen en andere aanvullende beschermingsmaatregelen:

a. zoals beschreven in Artikel 7.5.1 (Beoordeling van beveiligingsdocumentatie);

b. op eventuele aanvullende locaties beschreven in Bijlage 4 (Specifieke Producten); en

c. met betrekking tot Googles toepassing van een Alternatieve doorgifteoplossing, op https://cloud.google.com/terms/alternative-transfer-solution.

3.3. *SCC's en derde-verwerkingsverantwoordelijken*. Indien Partner optreedt als verwerker, erkent Partner dat Google, als andere verwerker, mogelijk niet in staat is de derde-verwerkingsverantwoordelijke te identificeren en zal Partner daarom:

a. elke kennisgeving die betrekking heeft op de BR SCC's onverwijld en zonder onnodige vertraging doorsturen naar de derde-verwerkingsverantwoordelijke;

b. als enige verantwoordelijk zijn, tussen Google en Partner, voor de naleving door de derde-verwerkingsverantwoordelijke van de transparantieverplichtingen onder de BR SCC's; en

c. op schriftelijk verzoek van Google onverwijld de volgende informatie verstrekken over de derde-verwerkingsverantwoordelijke: naam, bedrijfsgegevens (zoals rechtsvorm, statutaire zetel, fiscaal identificatienummer), hoofdadres, e-mailadres, contactpunt voor betrokkenen en alle gegevens die vereist zijn door de BR SCC's in verband met het contract van Partner met de verwerkingsverantwoordelijke.

3.4. *Beëindiging wegens risico's bij gegevensdoorgifte*. Indien Partner op basis van het huidige of beoogde gebruik van de Diensten tot de conclusie komt dat er geen passende waarborgen worden geboden voor de doorgifte van Partner-Persoonsgegevens, kan Partner de toepasselijke Overeenkomst met onmiddellijke ingang beëindigen in overeenstemming met de bepaling inzake beëindiging zonder opgave van redenen (for convenience) in de Overeenkomst; of, indien een dergelijke bepaling ontbreekt, door Google hiervan op de hoogte te stellen.

3.5. *Geen aanpassing van SCC's*. Niets in de Overeenkomst (inclusief dit Addendum) is bedoeld om de BR SCC's te wijzigen of tegen te spreken.

3.6. *Voorrang van SCC's*. Voor zover er een conflict of inconsistentie bestaat tussen de BR SCC's (Verwerkingsverantwoordelijke-naar-Verwerker) en de BR SCC's (Verwerker-naar-Verwerker) (die als

bijlagen in dit Addendum zijn opgenomen, indien van toepassing) en de rest van de Overeenkomst (inclusief dit Addendum), prevaleren de toepasselijke SCC's.

Bijlage 4: Specifieke producten

De voorwaarden in ieder subartikel van deze Bijlage 4 zijn uitsluitend van toepassing met betrekking tot de verwerking van Partnergegevens door de bijbehorende Dienst(en).

Google Cloud Platform

1. Aanvullende definities.

- *"Account"*, indien niet gedefinieerd in de Overeenkomst, betekent het Google Cloud Platform-account van Partner.
- *"Google Cloud Platform"* betekent de Google Cloud Platform-diensten beschreven op https://cloud.google.com/terms/services, met uitzondering van Aanbiedingen van Derden.
- *"Aanbiedingen van Derden"*, indien niet gedefinieerd in de Overeenkomst, betekent (a) diensten, software, producten en andere aanbiedingen van derden die niet zijn geïntegreerd in Google Cloud Platform of Software, (b) aanbiedingen geïdentificeerd in het artikel 'Voorwaarden van Derden' van de Servicespecifieke Voorwaarden van de Overeenkomst, en (c) besturingssystemen van derden.

2. Compliance-certificeringen. De Compliance-certificeringen voor Google Cloud Platform Gecontroleerde Diensten omvatten tevens certificaten voor ISO 27017 en ISO 27018 en een PCI DSS-attest voor compliance.

3. Locaties van datacenters. De locaties van Google Cloud Platform-datacenters worden beschreven op https://cloud.google.com/about/locations/.

4. Informatie over Subverwerkers. Namen, locaties en activiteiten van Google Cloud Platform Subverwerkers worden beschreven op https://cloud.google.com/terms/subprocessors.

5. Cloud-gegevensbeschermingsteam. Er kan contact worden opgenomen met het gegevensbeschermingsteam voor Google Cloud Platform via https://support.google.com/cloud/contact/dpo.

6. Informatie over Beperkte Doorgiften. Aanvullende informatie met betrekking tot Beperkte Doorgiften, Aanvullende Beveiligingsmechanismen en andere aanvullende beschermingsmaatregelen is beschikbaar op cloud.google.com/privacy/.

7. Servicespecifieke voorwaarden.

Bare Metal Solution (Google Cloud Platform)

Bare Metal Solution biedt niet-gevirtualiseerde toegang tot onderliggende infrastructuurbronnen en heeft, door ontwerp, bepaalde onderscheidende kenmerken.

1. Wijzigingen. Dit Addendum wordt als volgt gewijzigd met betrekking tot Bare Metal Solution:

- De definitie van "Externe Auditor van Google" wordt vervangen door het volgende:
    - *"Externe Auditor van Google"* betekent een gekwalificeerde en onafhankelijke externe auditor aangesteld door Google of door een Bare Metal Solution Subverwerker, van wie Google de op dat moment geldende identiteit op verzoek aan Partner zal bekendmaken.
- De volgende voorwaarden worden verwijderd:
    - Uit Artikel 7.1.1 (Googles Beveiligingsmaatregelen), de zinsnede "Partnergegevens versleutelen";
    - Uit Bijlage 2 (Beveiligingsmaatregelen), de subartikelen van Artikel 1(a) getiteld "Serverbesturingssystemen" en "Bedrijfscontinuïteit";
    - Uit Bijlage 2, de subartikelen van Artikel 1(b) getiteld "Externe aanvalsoppervlak", "Indringingsdetectie" en "Versleutelingstechnologieën"; en
    - Uit Bijlage 2, de volgende zinnen van Artikel 3(a):
        - Google slaat gegevens op in een multi-tenantomgeving op servers die in eigendom zijn van Google. Behoudens eventuele andersluidende instructies van Partner (bijvoorbeeld in de vorm van een selectie van een gegevenslocatie), repliceert Google Partnergegevens tussen meerdere geografisch verspreide datacenters.

2. Compliance-certificeringen en SOC-rapporten. Google of zijn Subverwerker onderhoudt ten minste het volgende (of een vergelijkbaar of verbeterd alternatief) voor Bare Metal Solution om de voortdurende effectiviteit van de Beveiligingsmaatregelen te verifiëren:

a. een certificaat voor ISO 27001 en een PCI DSS-attest voor compliance (de "*BMS-Compliance-certificeringen*"); en

b. SOC 1- en SOC 2-rapporten die jaarlijks worden geüpdatet op basis van een audit die ten minste eenmaal per 12 maanden wordt uitgevoerd (de "*BMS SOC-rapporten*").

3. Beoordelingen van Beveiligingsdocumentatie. Om Googles compliance met haar verplichtingen onder dit Addendum aan te tonen, zal Google de BMS-Compliance-certificeringen en BMS SOC-rapporten beschikbaar stellen ter beoordeling door Partner en, indien Partner een verwerker is, Partner toestaan om toegang tot de BMS SOC-rapporten aan te vragen voor de derde-verwerkingsverantwoordelijke in overeenstemming met Artikel 7.5.3 (Aanvullende zakelijke voorwaarden voor beoordelingen en audits).

4. Verplichtingen van Partner. Onverminderd de uitdrukkelijke verplichtingen van Google met betrekking tot Bare Metal Solution, zal Partner redelijke stappen ondernemen om de beveiliging van

Partnergegevens en alle andere inhoud opgeslagen op of verwerkt via Bare Metal Solution te beschermen en te onderhouden.

5. Disclaimer. Niettegenstaande enige andersluidende bepaling in de Overeenkomst (inclusief dit Addendum), is Google niet verantwoordelijk voor het volgende met betrekking tot Bare Metal Solution:

a. niet-fysieke beveiliging, zoals toegangsbeheer, versleuteling, firewalls, antivirusbescherming, dreigingsdetectie en beveiligingsscans;

b. logging en monitoring;

c. niet-hardware onderhoud of -ondersteuning;

d. gegevensback-up, inclusief redundantie- of hoge-beschikbaarheidsconfiguratie; of

e. beleidsregels of procedures voor bedrijfscontinuïteit en herstel na rampen.

Partner is als enige verantwoordelijk voor het beveiligen (met uitzondering van de fysieke beveiliging van Bare Metal Solution-servers), loggen en monitoren, onderhouden en ondersteunen en back-ups maken van alle Besturingssystemen, Partnergegevens, software en applicaties die Partner gebruikt met, uploadt naar, of host op Bare Metal Solution.

Cloud NGFW (Google Cloud Platform)

De editie van Cloud NGFW getiteld "Cloud NGFW Enterprise" ("CNE") is ontworpen om cyberbeveiligingsrisico's te beperken en heeft, als zodanig, bepaalde onderscheidende kenmerken.

1. Wijzigingen. Het Addendum wordt als volgt gewijzigd met betrekking tot CNE:

- Artikelen 6.1 (Verwijdering door Partner) en 6.2 (Teruggave of verwijdering wanneer de Looptijd eindigt) zullen Google of Subverwerkers niet verhinderen om een bestand of netwerkverkeer-packet capture, dat voor TSS-doeleinden is ingediend en door CNE is aangemerkt als een beveiligingsdreiging, te bewaren, mits het bestand of de packet capture geen Partner-Persoonsgegevens bevatten.

Google Distributed Cloud connected (Google Cloud Platform)

Google Distributed Cloud connected is niet geïmplementeerd in een Google-datacenter en heeft, door ontwerp, bepaalde onderscheidende kenmerken.

1. Wijzigingen. Dit Addendum wordt als volgt gewijzigd met betrekking tot Google Distributed Cloud connected:

- De definitie van "Gegevensincident" wordt vervangen door:

  > "*Gegevensincident*" betekent een inbreuk op de beveiliging van Google die onbedoeld of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging, of de ongeoorloofde verstrekking van of toegang tot Partnergegevens op systemen die door Google worden beheerd door of anderszins door Google worden gecontroleerd, maar, ter verduidelijking, met uitsluiting van inbreuken die verband houden met hardware of

infrastructuur die wordt beheerd, gehost of geëxploiteerd door, of anderszins de verantwoordelijkheid is van Partner.

- Verwijzingen naar "Systemen van Google" worden vervangen door "de Apparatuur".
- Artikel 6.2 (Teruggave of verwijdering wanneer de Looptijd eindigt) wordt vervangen door het volgende:
    - 6.2 *Teruggave of verwijdering wanneer de Looptijd eindigt*. Partner instrueert Google om in overeenstemming met de toepasselijke wetgeving alle resterende Partnergegevens te verwijderen (met inbegrip van bestaande kopieën) van de Apparatuur aan het einde van de Looptijd. Indien Partner Partnergegevens na het einde van de Looptijd wil bewaren, kan Partner deze gegevens exporteren of er kopieën van maken vóór het einde van de Looptijd. Google zal aan de Instructie in dit Artikel 6.2 voldoen zodra dit redelijkerwijs mogelijk is en binnen een maximale periode van 180 dagen, tenzij opslag vereist is op grond van het Europees Recht, wanneer Europese Gegevensbeschermingswetgeving van toepassing is, of opslag vereist is op grond van toepasselijk recht, wanneer enige andere Toepasselijke Privacywetgeving van toepassing is.
- De volgende woorden worden toegevoegd aan het einde van Artikel 10.1 (Opslag- en verwerkingsfaciliteiten voor gegevens): "of waar de Partnerlocatie zich bevindt".
- Artikel 1 (Datacenter en netwerkbeveiliging) van Bijlage 2 (Beveiligingsmaatregelen) wordt vervangen door het volgende:
    - **1. Lokale machines en netwerkbeveiliging**

Lokale machines. Partnergegevens worden uitsluitend opgeslagen op de Apparatuur die op de Partnerlocatie wordt ingezet.

Serverbesturingssystemen. Google-servers gebruiken een Linux-gebaseerde implementatie aangepast voor de toepassingsomgeving. Google gebruikt een code-beoordelingsproces om de beveiliging van de code die wordt gebruikt om Google Distributed Cloud connected te leveren te vergroten en om de beveiligingsproducten in productieomgevingen van Google Distributed Cloud connected te verbeteren.

Versleutelingstechnologieën. Google stelt HTTPS-versleuteling (ook wel SSL- of TLS-verbinding genoemd) ter beschikking en maakt versleuteling van gegevens tijdens overdracht mogelijk ('data in transit'). De servers van Google ondersteunen de uitwisseling van tijdelijke elliptische curves van de cryptografische sleutel van Diffie-Hellman ondertekend met RSA en ECDSA. Deze Perfect Forward Secrecy-methoden (PFS) helpen om het verkeer te beschermen en de impact van een gecompromitteerde sleutel of een cryptografische doorbraak te minimaliseren. Google maakt ook versleuteling van gegevens in rust ('data at rest') mogelijk door ten minste AES128 of vergelijkbaar te gebruiken. Google Distributed Cloud connected heeft een CMEK-integratie; meer informatie is te vinden op https://cloud.google.com/kms/docs/cmek.

Verbinding met Cloud VPN. Google staat Partner toe om een sterke, versleutelde interconnectie te gebruiken en te configureren tussen de Apparatuur en de Virtual Private Cloud van Partner met Cloud VPN via een IPSEC VPN-verbinding.

Gebonden opslag. Gegevensopslag van Partner is gebonden aan de server. Indien een schijf in rust wordt gestolen of gekopieerd, dan zal de inhoud van die schijf buiten de server onherstelbaar zijn.

- Artikel 2 (Toegangs- en locatiecontroles) en 3 (Gegevens) van Bijlage 2 (Beveiligingsmaatregelen) worden verwijderd.

2. Niet-toepasselijke bepalingen. Alle verplichtingen van Google in de Overeenkomst (inclusief dit Addendum) of verklaringen in bijbehorende beveiligingsdocumentatie (inclusief whitepapers) die afhankelijk zijn van de exploitatie door Google van een Google-datacenter, zijn niet van toepassing op Google Distributed Cloud connected.

Google-Managed Multi-Cloud (Google Cloud Platform)

Google-Managed Multi-Cloud Diensten maken gebruik van infrastructuur van derden en hebben, door ontwerp, bepaalde onderscheidende kenmerken.

1. Aanvullende definitie.

- "*Google-Managed MCS Data Processing Amendment*" betekent de voorwaarden op https://cloud.google.com/terms/mcs-data-processing-terms.

2. Voorwaarden voor Multi-Cloud-gegevensverwerking. De Google-Managed MCS Data Processing Amendment vult dit Addendum aan en wijzigt deze met betrekking tot Google-Managed Multi-Cloud Diensten voor Google Cloud Platform.

Google Cloud VMware Engine (Google Cloud Platform)

Google heeft mogelijk geen toegang tot de VMware-omgeving van Partner en kan mogelijk geen persoonsgegevens versleutelen in de VMware-omgeving van Partner.

NetApp Volumes (Google Cloud Platform)

1. Wijzigingen. Dit Addendum wordt als volgt gewijzigd met betrekking tot NetApp Volumes:

- De definitie van "Externe Auditor van Google" wordt vervangen door:
    - "*Externe Auditor van Google*" betekent een gekwalificeerde en onafhankelijke externe auditor aangesteld door Google of een NetApp Volumes-subverwerker, van wie Google de op dat moment geldende identiteit op verzoek aan Partner zal bekendmaken.
- Artikel 3(a) (Gegevensopslag, isolatie en logging) van Bijlage 2 (Beveiligingsmaatregelen) wordt vervangen door het volgende:
    - (a) *Gegevensopslag, isolatie en logging*. Google slaat gegevens op in een multi-tenantomgeving op de servers van NetApp, Inc. Behoudens eventuele

andersluidende Instructies (bijvoorbeeld in de vorm van een selectie van een gegevenslocatie) repliceert Google Partnergegevens tussen meerdere geografisch verspreide datacenters. Ook isoleert Google Partnergegevens op logische wijze. Partner krijgt controle over specifieke beleidsregels inzake gegevensdeling. Die beleidsregels zullen, in overeenstemming met de functionaliteit van de Diensten, Partner in staat stellen om de productdelingsinstellingen te bepalen die van toepassing zijn op Eindgebruikers van Partner voor specifieke doeleinden. Partner kan ervoor kiezen om gebruik te maken van de loggingsfunctionaliteit die Google via de Diensten beschikbaar stelt.

2. Compliance-certificeringen en SOC-rapporten. Google of een Subverwerker zal ten minste het volgende (of een gelijkwaardig of verbeterd alternatief) verkrijgen voor NetApp Volumes:

a. een certificaat voor ISO 27001 en een PCI DSS-attest voor compliance(de "*NetApp-Compliance-certificeringen*"); en

b. SOC 1- en SOC 2-rapporten die jaarlijks worden bijgewerkt op basis van een audit die ten minste één keer per 12 maanden wordt uitgevoerd (de "*NetApp SOC-rapporten*").

3. Beoordelingen van Beveiligingsdocumentatie. Om Googles compliance met haar verplichtingen onder dit Addendum aan te tonen, zal Google de NetApp-Compliance-certificeringen en NetApp SOC-rapporten beschikbaar stellen ter beoordeling door Partner en, indien Partner een verwerker is, Partner in staat stellen om toegang tot de NetApp SOC-rapporten aan te vragen voor de derde-verwerkingsverantwoordelijke in overeenstemming met Artikel 7.5.3 (Aanvullende zakelijke voorwaarden voor beoordelingen en audits).

Looker (origineel)

1. Aanvullende definities.

- *"Admin Console"* betekent elke beheerdersconsole van toepassing op iedere Instantie.
- *"Google-Managed MCS Data Processing Amendment"* betekent, indien van toepassing, de voorwaarden op https://cloud.google.com/terms/mcs-data-processing-terms.
- *"Google-Managed Multi-Cloud Diensten"* betekent, indien van toepassing, gespecificeerde Google-diensten, -producten en -functies die worden gehost op de infrastructuur van een derde cloudprovider.
- *"Looker (origineel)"* betekent een geïntegreerd platform (inclusief cloudgebaseerde infrastructuur, indien van toepassing, en softwarecomponenten inclusief alle bijbehorende API's) dat bedrijven in staat stelt gegevens te analyseren en bedrijfsstatistieken te definiëren over meerdere gegevensbronnen, beschikbaar gesteld door Google aan Partner op grond van de Overeenkomst. Looker (origineel) is exclusief Aanbiedingen van Derden.
- *"Multi-Cloud Service Third-Party Provider"* heeft de betekenis zoals beschreven in het Google-Managed MCS Data Processing Agreement.

- *"Bestelformulier"* heeft de betekenis zoals beschreven in de Overeenkomst, tenzij Partner een aankoop heeft gedaan via een reseller of online marktplaats of Looker alleen gebruikt voor proef- of evaluatiedoeleinden onder een proef- of evaluatieovereenkomst, in welk geval Bestelformulier een ander schriftelijk formulier kan betekenen (e-mail of andere toegestane elektronische manieren) zoals geautoriseerd door Google.

2. Wijzigingen. Dit Addendum wordt als volgt gewijzigd met betrekking tot Looker (origineel):

- De definitie van "E-mailadres voor Kennisgevingen" wordt vervangen door het volgende:
    - *"E-mailadres voor Kennisgevingen"* betekent het e-mailadres/de e-mailadressen die door Partner in het Bestelformulier of via Looker (indien van toepassing) zijn opgegeven om bepaalde kennisgevingen van Google te ontvangen.
- De definities van "SCC's (Verwerkingsverantwoordelijke-naar-Verwerker)", "SCC's (Verwerker-naar-Verwerkingsverantwoordelijke)", "SCC's (Verwerker-naar-Verwerker)" en "SCC's (Verwerker-naar-Verwerker, Google Exporteur)" in Bijlage 3 (Specifieke privacywetgeving) worden vervangen door het volgende:
    - "*SCC's (Verwerkingsverantwoordelijke-naar-Verwerker)*" betekent de voorwaarden op: https://cloud.google.com/terms/looker/legal/sccs/eu-c2p;
    - "*SCC's (Verwerker-naar-Verwerkingsverantwoordelijke)*" betekent de voorwaarden op: https://cloud.google.com/terms/looker/legal/sccs/eu-p2c;
    - "*SCC's (Verwerker-naar-Verwerker)*" betekent de voorwaarden op: https://cloud.google.com/terms/looker/legal/sccs/eu-p2p; en
    - "*SCC's (Verwerker-naar-Verwerker, Google Exporteur)" beteke*nt de voorwaarden op: https://cloud.google.com/terms/looker/legal/sccs/eu-p2p-intra-group.
- De volgende woorden worden toegevoegd aan het einde van Artikel 10.1 (Opslag- en verwerkingsfaciliteiten voor gegevens): "of waar Multi-Cloud Service Third-Party Providers faciliteiten hebben".

3. Aanvullende beveiligingsverantwoordelijkheden van Partner. Partner is verantwoordelijk voor de beveiliging van Partners omgeving, databases en configuratie voor Looker (origineel), met uitzondering van systemen die door Google worden beheerd en gecontroleerd.

4. Compliance-certificeringen en SOC-rapporten. De Compliance-certificeringen en SOC-rapporten voor de Gecontroleerde Diensten van Looker (origineel) kunnen variëren afhankelijk van de hostingomgeving waarin de relevante Diensten worden gebruikt. Google zal op verzoek details verstrekken van de Compliance-certificeringen en SOC-rapporten die beschikbaar zijn voor specifieke hostingomgevingen.

5. Locaties van datacenters. De locaties van datacenters voor Looker (origineel) zullen worden beschreven op het toepasselijke Bestelformulier of anderszins worden geïdentificeerd door Google.

6. Geen certificering door niet-EMEA Partners. Partner is niet verplicht te certificeren of om zijn bevoegde Toezichthoudende Autoriteit te identificeren zoals beschreven in Artikel 4.2 (Certificering door niet-EMEA Partners) van de Europese voorwaarden voor gegevensbescherming in Bijlage 3 (Specifieke privacywetgeving) voor Looker (origineel).

7. Informatie over Beperkte Doorgiften. Aanvullende informatie die relevant is voor Beperkte Doorgiften, Aanvullende Beveiligingsmechanismen en overige aanvullende beveiligingsmaatregelen voor Looker (origineel) is beschikbaar op https://docs.looker.com.

8. Informatie over Subverwerkers. Namen, locaties en activiteiten van Subverwerkers voor Looker (origineel) worden beschreven op:

a. https://cloud.google.com/terms/looker/privacy/lookeroriginal-subprocessors; en

b. https://cloud.google.com/terms/subprocessors.

9. Google-Managed Multi-Cloud (Looker (origineel))

Google-Managed Multi-Cloud Diensten maken gebruik van infrastructuur van derden en hebben, door ontwerp, bepaalde onderscheidende kenmerken.

9.1 *Voorwaarden voor Multi-Cloud-gegevensverwerking*. Het Google-Managed MCS Data Processing Amendment is een aanvulling op dit Addendum en wijzigt het met betrekking tot door Google-Managed Multi-Cloud Diensten voor Looker (origineel).

10. Cloud-gegevensbeschermingsteam. Er kan contact worden opgenomen met het gegevensbeschermingsteam voor Looker (origineel) via https://support.google.com/cloud/contact/dpo.

11. Verwerkingsregisters van Google. Voor zover Toepasselijke Privacywetgeving vereist dat Google bepaalde informatie met betrekking tot Partner of zijn Klanten verzamelt en bijhoudt, zal Partner dergelijke informatie op verzoek aan Google verstrekken, en Google op de hoogte stellen van eventuele updates die nodig zijn om dergelijke informatie accuraat en up-to-date te houden, tenzij Google verzoekt dat Partner dergelijke informatie via een andere manier verstrekt en bijwerkt.

12. Aanvullende beveiligingsmaatregelen voor applicaties. Google zal de onderstaande aanvullende Beveiligingsmaatregelen implementeren en onderhouden voor Looker (origineel):

a. Google volgt ten minste de industriestandaarden voor beveiligingsarchitectuur.. Proxyservers die worden gebruikt voor de applicaties van Google helpen de toegang tot Looker te beveiligen door een enkel punt te bieden om aanvallen te filteren via IP-denylisting en beperking van verbindingssnelheden.

b. Beheerders van Partner beheren de toegang van Google-personeel tot applicaties om technische ondersteuning te bieden die door Partner of Eindgebruikers van Partner is verzocht.

SecOps Diensten

1. Aanvullende definities.

- *"Account"*, indien niet gedefinieerd in de Overeenkomst, betekent SecOps Diensten- of Google Cloud Platform-account van Partner, indien van toepassing.

- *"SecOps Diensten"* betekent Chronicle SIEM, Chronicle SOAR en Mandiant Solutions, elk zoals beschreven op https://cloud.google.com/terms/secops/services, met uitzondering van eventueel Aanbiedingen van Derden. Ter verduidelijking: SecOps Diensten sluiten Mandiant Consulting Diensten en Managed Services uit.

- *"Aanbiedingen van Derden"*, indien niet gedefinieerd in de Overeenkomst, betekent (a) diensten, software, producten en overige aanbiedingen van derden die niet zijn verwerkt in SecOps Diensten of Software, en (b) besturingssystemen van derden.

2. Wijzigingen. Dit Addendum wordt als volgt gewijzigd met betrekking tot SecOps Diensten:

- De definitie van "Aanvullende Beveiligingsmechanismen" wordt vervangen door het volgende:

    - *"Aanvullende Beveiligingsmechanismen"* betekent middelen, functies, functionaliteiten en/of mechanismen (indien van toepassing) voor beveiliging die Partner naar eigen keuze en/of naar eigen inzicht kan gebruiken, inclusief (indien van toepassing) versleuteling, logging en controle, identiteits- en toegangsbeheer en beveiligingsscans.

- De definities van "SCC's (Verwerkingsverantwoordelijke-naar-Verwerker)", "SCC's (van Verwerker-naar-Verwerkingsverantwoordelijke)", "SCC's (Verwerker-naar-Verwerker)" en "SCC's (Verwerker-naar-verwerker, Google Exporteur)" in Bijlage 3 (Specifieke privacywetgeving) worden vervangen door de volgende:

    - "*SCC's (Verwerkingsverantwoordelijke-naar-Verwerker)*" betekent de voorwaarden op: https://cloud.google.com/terms/secops/sccs/eu-c2p.

    - *"SCC's (Verwerker-naar-Verwerkingsverantwoordelijke)"* betekent de voorwaarden op: https://cloud.google.com/terms/secops/sccs/eu-p2c.

    - *"SCC's (Verwerker-naar-Verwerker)"* betekent de voorwaarden op: https://cloud.google.com/terms/secops/sccs/eu-p2p.

    - "SCC's (Verwerker-naar-verwerker, Google Exporteur)" betekent de voorwaarden op: https://cloud.google.com/terms/secops/sccs/eu-p2p-google-exporter.

3. Locaties van datacenters. De locaties van de datacenters voor SecOps Diensten worden beschreven op https://cloud.google.com/terms/secops/data-residency.

4. Geen certificering door niet-EMEA Partners. Partner is niet verplicht te certificeren of om zijn bevoegde Toezichthoudende Autoriteit te identificeren zoals beschreven in Artikel 4.2 (Certificering door niet-EMEA Partners) van de Europese voorwaarden voor gegevensbescherming in Bijlage 3 (Specifieke privacywetgeving) voor SecOps Diensten.

5. Informatie over Subverwerkers. De namen, locaties en activiteiten van Subverwerkers voor SecOps Diensten worden beschreven op https://cloud.google.com/terms/secops/subprocessors.

6. Cloud-gegevensbeschermingsteam. Er kan contact worden opgenomen met het gegevensbeschermingsteam voor SecOps Diensten via https://support.google.com/cloud/contact/dpo (en/of op andere manieren die Google van tijd tot tijd kan bieden).

7. Verwerkingsregisters van Google. Voor zover Toepasselijke Privacywetgeving vereist dat Google bepaalde informatie met betrekking tot Partner verzamelt en bijhoudt, zal Partner dergelijke informatie op verzoek aan Google verstrekken, en Google op de hoogte stellen van updates die nodig zijn om dergelijke informatie accuraat en up-to-date te houden, tenzij Google verzoekt dat Partner dergelijke informatie op een andere manier verstrekt en bijwerkt.

Eerdere versies van de Gegevensverwerkings- en Beveiligingsvoorwaarden (Partners):

30 juni 2022 24 september 2021 20 augustus 2020 10 augustus 2020 17 juli 2020 1 oktober 2019 28 februari 2019 25 mei 2018 13 maart 2018

Eerdere versies van SecOps Diensten DPST (Partners):

6 februari 2023 31 oktober 2022 27 september 2021

Eerdere versies *(Laatst gewijzigd 30 oktober 2024)*

15 oktober 2024 26 september 2024 9 september 2024 9 april 2024 8 november 2023 15 augustus 2023 20 september 2022