Addendum voor Cloud-gegevensverwerking (Klanten)

Dit Addendum voor Cloud-gegevensverwerking (inclusief bijbehorende bijlagen, het "*Addendum*") maakt deel uit van de Overeenkomst(en) (zoals hieronder gedefinieerd) tussen Google en Klant. Dit Addendum heette voorheen de "Data Processing and Security Terms" genoemd op grond van een Overeenkomst voor Google Cloud Platform, Looker (original), Google SecOps Diensten of Google Cloud Skills Boost voor organisaties; het "Data Processing Amendment" onder een Overeenkomst voor Google Workspace of Cloud Identity; en het "Data Processing Addendum" een Overeenkomst voor Mandiant Consulting Diensten en Beheerde Diensten.

Algemene voorwaarden

1. Overzicht

Dit Addendum beschrijft de verplichtingen van de partijen, inclusief verplichtingen op grond van privacy-, gegevensbeveiligings- en gegevensbeschermingswetgeving, met betrekking tot de verwerking en beveiliging van Klantgegevens (zoals hieronder gedefinieerd). Dit Addendum gaat in 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 Klantgegevens. 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 Klant dit Addendum heeft aanvaard of waarop de partijen anderszins akkoord zijn gegaan met dit Addendum.
- *"Aanvullende Beveiligingsmechanismen"* betekent middelen, functies, functionaliteiten en mechanismen voor beveiliging die Klant 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 ermee heeft ingestemd de toepasselijke Diensten aan Klant te leveren.
- *"Toepasselijke Privacywetgeving"* betekent, voor zover van toepassing op de verwerking van Persoonsgegevens van Klant, 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 toepasselijke Overeenkomst.

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

- "*Klantgegevens*", indien niet gedefinieerd in de Overeenkomst, heeft de betekenis die is gegeven in Bijlage 4 (Specifieke producten).

- "*Klant-Persoonsgegevens*" betekent de persoonsgegevens die zijn vervat in Klantgegevens, inclusief bijzondere categorieën persoonsgegevens of gevoelige gegevens zoals gedefinieerd onder de Toepasselijke Privacywetgeving.

- *"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 Klantgegevens 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 Klant-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 Klant-Persoonsgegevens); of (c) de wetgeving van Zwitserland (als de Zwitserse FADP van toepassing is op de verwerking van Klant-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 Klant zal bekendmaken.

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

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

- *"Beveiligingsdocumentatie"* betekent de Compliance-certificeringen en 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 Klantgegevens te verwerken om 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 AVG van het Verenigd Koninkrijk 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 toepasselijke Overeenkomst is beëindigd of verlopen, blijft dit Addendum van kracht totdat Google alle Klantgegevens 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 Klant is, indien van toepassingl, verwerkingsverantwoordelijke of verwerker met betrekking tot Klant-Persoonsgegevens.

4.2 *Verwerkingssamenvatting*. Het onderwerp en de details van de verwerking van Klant-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 Klant-Persoonsgegevens onder de Toepasselijke Privacywetgeving naleven.

4.4 *Aanvullende juridische voorwaarden*. Voor zover de verwerking van Klant-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 *Klanten die verwerker zijn*. Indien Klant een verwerker is:

a. garandeert Klant doorlopend dat de derde-verwerkingsverantwoordelijke het volgende heeft geautoriseerd:

i. de Instructies;

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

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

b. zal Klant 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 derde-verwerkingsverantwoordelijke; en

c. kan Klant aan de 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 Klant*. Klant instrueert Google om Klantgegevens uitsluitend te verwerken in overeenstemming met de toepasselijke Overeenkomst (inclusief dit Addendum), als volgt:

a. om de Diensten en TSS (indien van toepassing) te leveren, te beveiligen en te monitoren; en

b. zoals verder gespecificeerd via:

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

ii. alle andere schriftelijke instructies gegeven door Klant 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 Klant*. Google zal Klant in staat stellen om tijdens de Looptijd Klantgegevens te verwijderen op een wijze die in overeenstemming is met de functionaliteit van de Diensten. Indien Klant de Diensten gebruikt om tijdens de Looptijd Klantgegevens te verwijderen en deze Klantgegevens niet door Klant kunnen worden hersteld, vormt dit gebruik een Instructie aan Google om de relevante Klantgegevens 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 is vereist op grond 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.

6.2 *Teruggave of verwijdering wanneer de Looptijd eindigt*. Indien Klant bepaalde Klantgegevens na het einde van de Looptijd wenst te behouden, kan hij Google instrueren in overeenstemming met Artikel 9.1 (Toegang, Rectificatie, Beperkte Verwerking, Portabiliteit) om de gegevens tijdens de Looptijd terug te geven. Behoudens Artikel 6.3 (Instructies voor Uitgestelde Verwijdering), instrueert Klant Google om alle resterende Klantgegevens (inclusief 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 is en binnen een maximale periode van 180 dagen, tenzij opslag is vereist op grond van 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.

6.3. *Instructies voor uitgestelde verwijdering*. Voor zover enige Klantgegevens die vallen onder de verwijderingsinstructie beschreven in Artikel 6.2 (Teruggave of verwijdering wanneer de Looptijd eindigt) ook worden verwerkt zal, wanneer de toepasselijke Looptijd op grond van Artikel 6.2 afloopt, met betrekking tot een Overeenkomst met een doorlopende Looptijd, een dergelijke

verwijderingsinstructie pas van kracht worden met betrekking tot die Klantgegevens wanneer de doorlopende Looptijd afloopt. Ter verduidelijking: dit Addendum blijft van toepassing op die Klantgegevens totdat Google deze heeft verwijderd.

7. Gegevensbeveiliging

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

7.1.1 *Beveiligingsmaatregelen van Google*. Google implementeert en onderhoudt technische, organisatorische en fysieke maatregelen om Klantgegevens te beschermen tegen onbedoelde of onwettige vernietiging, verlies, wijziging en ongeautoriseerde vrijgave van of toegang zoals beschreven in Bijlage 2 (Beveiligingsmaatregelen) (de "*Beveiligingsmaatregelen*"). De Beveiligingsmaatregelen omvatten maatregelen om Klantgegevens 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 Klantgegevens te herstellen na een incident; en voor regelmatige effectiviteitstests. Google kan de Beveiligingsmaatregelen van tijd tot tijd bijwerken, mits deze updates niet leiden tot een materiële vermindering van de beveiliging van de Diensten.

7.1.2 *Toegang en Compliance*. Google zal:

a. haar medewerkers, onderaannemers en Subverwerkers uitsluitend autoriseren om toegang te krijgen tot Klantgegevens voor zover dit strikt noodzakelijk is om aan Instructies te voldoen;

b. passende stappen ondernemen om compliance met Beveiligingsmaatregelen door haar 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 Klantgegevens te verwerken onder een geheimhoudingsverplichting vallen.

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

a. Klant in staat te stellen stappen te ondernemen om Klantgegevens te beveiligen; en

b. Klant te voorzien van informatie over het beveiligen, toegang krijgen tot en gebruiken van Klantgegevens.

7.1.4 *Googles Beveiligingsassistentie*. Google zal (rekening houdend met de aard van de verwerking van Klant-Persoonsgegevens en de informatie waarover Google beschikt) Klant helpen bij het voldoen aan zijn verplichtingen (of, wanneer Klant 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 (Beveiligingsmaatregelen van Google);

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 toepasselijke Overeenkomst (inclusief dit Addendum) te verstrekken; en

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

7.2 *Gegevensincidenten*.

7.2.1 *Kennisgeving van Incidenten*. Google zal Klant 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 minimaliseren en Klantgegevens te beveiligen.

7.2.2 *Details van Gegevensincident*. De kennisgeving door Google van een Gegevensincident zal het volgende beschrijven: de aard van het Gegevensincident, inclusief getroffen bronnen van Klant; 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 Klant 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 Klantgegevens door Google*. Google is niet verplicht om Klantgegevens te beoordelen teneinde 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 van Google van schuld of aansprakelijkheid met betrekking tot het Gegevensincident.

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

7.3.1 *Beveiligingsverantwoordelijkheden van Klant*. 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 toepasselijke Overeenkomst, is Klant verantwoordelijk voor het gebruik van de Diensten en de opslag van kopieën van Klantgegevens 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 Klantgegevens;

b. het beveiligen van de authenticatiegegevens van het account, de systemen en de apparaten die Klant gebruikt om toegang te krijgen tot de Diensten; en

c. het maken van back-ups of het bewaren van kopieën van zijn Klantgegevens, voor zover passend.

7.3.2 *Beoordeling van beveiliging door Klant*. Klant 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 Klantgegevens (rekening houdend met de stand van de techniek, de implementatiekosten, alsmede de aard, omvang, context en doeleinden van de verwerking van Klantgegevens, en de risico's voor individuen).

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

a. certificaten voor ISO 27001 en alle 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 de verplichtingen onder dit Addendum nakomt, zal Google de Beveiligingsdocumentatie beschikbaar stellen ter beoordeling door Klant en, indien Klant een verwerker is, zal Google Klant toestaan om toegang te verzoeken tot de SOC-rapporten voor de derde-verwerkingsverantwoordelijke aan te vragen in overeenstemming met Artikel 7.5.3 (Aanvullende zakelijke voorwaarden voor beoordelingen en audits).

7.5.2 *Auditrechten van Klant*.

a. *Audit door Klant*. Google zal, indien vereist op grond van de Toepasselijke Privacywetgeving, Klant of een door Klant 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 Klant of haar auditor, zoals beschreven in dit Artikel 7.5 (Beoordelingen en audits met betrekking tot Compliance).

b. *Onafhankelijke beoordeling door Klant*. Klant kan een audit uitvoeren om de 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. Klant 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 Klant).

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

i. beveiligings- en vertrouwelijkheidsmechanismen van toepassing op 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 vertrouwelijkheidsmechanismen van toepassing op elke audit op grond van Artikel 7.5.2(a) (Audit door Klant).

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 Klant). Google zal Klant voorafgaand aan een dergelijke audit nader informeren over eventuele toepasselijke vergoeding en de grondslag voor de berekening ervan. Klant is verantwoordelijk voor alle vergoedingen die in rekening worden gebracht door een door Klant aangestelde auditor om een dergelijke audit uit te voeren.

d. Google kan schriftelijk bezwaar maken bij een door Klant aangewezen auditor die een audit uitvoert op grond van Artikel 7.5.2(a) (Audit door Klant), 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 Klant een andere auditor aan te wijzen of de audit zelf uit te voeren.

e. Alle verzoeken van Klant op grond van Bijlage 3 (Specifieke privacywetgeving) of Bijlage 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) Klant helpen om te voldoen aan zijn verplichtingen (of, wanneer Klant 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 toepasselijke Overeenkomst (inclusief dit Addendum) te verstrekken; en

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

9. Toegang; Rechten van betrokkenen; Gegevens exporteren

9.1 *Toegang; Rectificatie; Beperkte verwerking; Portabiliteit*. Gedurende de Looptijd zal Google Klant in staat stellen om, op een wijze in overeenstemming met de functionaliteit van de Diensten, toegang te verkrijgen tot Klantgegevens, Klantgegevens te corrigeren en de verwerking van Klantgegevens te beperken, onder andere via de verwijderfunctie die Google biedt zoals beschreven in Artikel 6.1 (Verwijdering door Klant) en om Klantgegevens te exporteren. Indien Klant constateert dat Klant-Persoonsgegevens onjuist of verouderd zijn, is Klant 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 Klant-Persoonsgegevens en waarbij Klant wordt geïdentificeerd, zal Google:

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

b. Klant prompt op de hoogte stellen; en

c. niet op een andere wijze op het verzoek van die betrokkene reageren zonder toestemming van Klant.

Klant 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 Klant-Persoonsgegevens) Klant assisteren bij het voldoen aan zijn verplichtingen (of, als Klant een verwerker is, 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; Portabiliteit) en 9.2.1 (Verantwoordelijkheid voor Verzoeken) na te leven; en

c. indien bovenstaande subartikelen (a) en (b) voor Klant (of de derde-verwerkingsverantwoordelijke) onvoldoende zijn om aan dergelijke verplichtingen te voldoen, op verzoek van Klant 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 in de Servicespecifieke Voorwaarden en verplichtingen voor gegevensdoorgifte in Bijlage 3 (Specifieke privacywetgeving), indien van toepassing, kunnen Klantgegevens 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*. Klant 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 Klant, onverminderd aan 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 zijn beschreven in Bijlage 4 (Specifieke producten).

11.3 *Vereisten voor het betrekken van Subverwerkers*. Bij de inschakeling van Subverwerkers zal Google:

a. er via een schriftelijk overeenkomst voor zorgen dat:

i. de Subverwerker uitsluitend toegang heeft tot en gebruikmaakt van Klantgegevens voor zover noodzakelijk om de aan hem uitbestede verplichtingen na te komen, en ditdoet in overeenstemming met de toepasselijke 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 mogelijk verder 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, zal Google Klant ten minste 30 dagen voordat de Nieuwe Subverwerker Klantgegevens gaat verwerken in kennis stellen van de betrokkenheid (inclusief de naam, locatie en activiteiten van de Nieuwe Subverwerker).

b. Klant kan, binnen 90 dagen nadat deze op de hoogte is gesteld van de inschakeling van een Nieuwe Subverwerker, bezwaar maken door de toepasselijke 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 in de Overeenkomst; of

ii. indien een dergelijke bepaling ontbreekt, door Google hiervan 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 een Klant over de verwerking van Klantgegevens op grond van de toepasselijke Overeenkomst en er kan contact mee worden opgenomen zoals beschreven in het Artikel Kennisgevingen van de toepasselijke Overeenkomst of in Bijlage 4 (Specifieke producten).

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

12.3 *Verzoeken van verwerkingsverantwoordelijken*. Gedurende de Looptijd, indien het Cloud-gegevensbeschermingsteam van Google een verzoek of instructie beoordeelt van een derde die beweert verwerkingsverantwoordelijke te zijn van Klant-Persoonsgegevens, zal Google deze derde adviseren om contact op te nemen met Klant.

13. Kennisgevingen

Kennisgevingen op grond van dit Addendum (waaronder kennisgevingen van Gegevensincidenten) worden naar het E-mailadres voor Kennisgevingen gestuurd. Het is de verantwoordelijkheid van Klant 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; en

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

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

Voor alle duidelijkheid: als Klant meer dan één Overeenkomst heeft, zal dit Addendum elk van de Overeenkomsten afzonderlijk wijzigen.

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.

Bijlage 1: Onderwerp en details van gegevensverwerking

Onderwerp

Googles levering van Diensten en TSS (indien van toepassing) aan Klant.

Duur van de verwerking

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

Aard en doel van de verwerking

Google zal Klant-Persoonsgegevens verwerken met het doel de Diensten en TSS (indien van toepassing) te leveren aan Klant in overeenstemming met dit Addendum.

Categorieën van gegevens

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

Betrokkenen

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

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 gespreide datacenters. Google slaat alle productiegegevens op in fysiek beveiligde datacenters.

Redundantie. Infrastructuursystemen zijn ontworpen om enkelvoudige storingspunten te elimineren en de impact van voorzienbare omgevingsrisico's te minimaliseren. Dubbele circuits, schakelaars, netwerken en 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 transitorische stroom 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.

Extern aanvalsoppervlak. Google maakt gebruik van meerdere lagen netwerkapparaten en indringingsdetectie om zijn extern 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.

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 het beveiligingspersoneel van Google zal 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 ontvangstzones. 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 Klant 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 Klantgegevens te verwerken. Google ontwerpt systemen zodanig dat (i) alleen geautoriseerde personen toegang hebben tot gegevens waarvoor ze geautoriseerd zijn; en (ii) Klantgegevens 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-tenant omgeving op servers die eigendom zijn van Google. Behoudens eventuele andersluidende Instructies (bijvoorbeeld in de vorm van een selectie van een gegevenslocatie) kopieert Google Klantgegevens naar verschillende datacenters op verschillende locaties. Ook isoleert Google Klantgegevens op een logische wijze. Klant krijgt controle over specifieke beleidsregels inzake gegevensdeling. Die beleidsregels zullen, in overeenstemming met de functionaliteit van de Diensten, Klant in staat stellen om de productdelingsinstellingen te bepalen die van toepassing zijn op Eindgebruikers voor specifieke doeleinden. Klant 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 te maken krijgen met prestatieproblemen, fouten of hardwareproblemen 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 tracering. 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 Klantgegevens verwerkt, moet aanvullende eisen voltooien die passend zijn voor hun rol (bijvoorbeeld certificeringen). Google-personeel zal Klantgegevens 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 geacht worden te leveren. Zodra Google de risico's verbonden aan de Subverwerker heeft beoordeeld, en

onverminderd de vereisten beschreven in Artikel 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 Klant-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 op grond van de Zwitserse FADP;

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

- *"Alternatieve Doorgifteoplossing"* betekent 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.

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

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

- *"SCC's (Verwerker-naar-Verwerkingsverantwoordelijke)"* betekent de voorwaarden zoals opgenomen op: https://cloud.google.com/terms/sccs/eu-p2c
- *"SCC's (Verwerker-naar-Verwerker)"* betekent de voorwaarden zoals opgenomen op: https://cloud.google.com/terms/sccs/eu-p2p
- *"SCC's (Verwerker-naar-Verwerker, Google Exporteur)"* betekent de voorwaarden zoals opgenomen 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 Klant) of andere rechten of verplichtingen van beide partijen op grond van de toepasselijke Overeenkomst, zal Google Klant 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 Klant een verwerker is, stuurt Klant elke door Google verstrekte kennisgeving op grond van dit Artikel onmiddellijk door naar de derde-verwerkingsverantwoordelijke.

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

4.1 *Beperkte doorgiften*. De partijen erkennen dat de Europese Gegevensbeschermingswetgeving geen SCC's of een Alternatieve Doorgifteoplossing vereist voor de verwerking of doorgifte van Klant-Persoonsgegevens in of naar een Adequaat Land. Indien Klant-Persoonsgegevens worden doorgegeven naar enig ander land en de Europese Gegevensbeschermingswetgeving van toepassing is op de doorgifte (zoals gecertificeerd door Klant op grond van Artikel 4.2 (Certificering door niet-EMEA Klanten) van deze voorwaarden van de Europese wetgeving voor gegevensbescherming, als het factuuradres buiten de EMEA valt) ("*Beperkte Doorgiften*"), dan:

a. indien Google een Alternatieve Doorgifteoplossing heeft aangenomen voor Beperkte Doorgiften, stelt Google Klant op de hoogte van de betreffende oplossing en zorgt dat dergelijke Beperkte Doorgiften in overeenstemming daarmee worden uitgevoerd; of

b. Indien Google geen Alternatieve Doorgifteoplossing voor Beperkte Doorgiften heeft aangenomen of Klant informeert dat Google geen Alternatieve Doorgifteoplossing voor Beperkte Doorgiften meer gebruikt (zonder een vervangende Alternatieve Doorgifteoplossing aan te nemen):

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

A. gelden de SCC's (Verwerker-naar-Verwerker, Google Exporteur) voor dergelijke Beperkte Doorgiften van Google naar Subverwerkers; en

B. daarnaast gelden, indien het factuuradres van Klant zich niet in een Adequaat Land bevindt, de SCC's (Verwerker-naar-Verwerkingsverantwoordelijke) (ongeacht of Klant een verwerkingsverantwoordelijke of een verwerker is) met betrekking tot dergelijke Beperkte Doorgiften tussen Google en Klant; of

ii. Indien het adres van Google zich niet in een Adequaat Land bevindt, gelden de SCC's (Verwerkingsverantwoordelijke-naar-Verwerker) of SCC's (Verwerker-naar-Verwerker) (afhankelijk van of Klant een verwerkingsverantwoordelijke of verwerker is) met betrekking tot dergelijke Beperkte Doorgiften tussen Google en Klant.

4.2 *Certificering door niet-EMEA Klanten*. Indien het factuuradres van Klant buiten EMEA ligt en de verwerking van Klant-Persoonsgegevens onderworpen is aan de Europese Gegevensbeschermingswetgeving, dan zal Klant, 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 Klant voorzien van informatie die relevant is voor Beperkte Doorgiften, Aanvullende Beveiligingsmechanismen en andere extra beschermingsmaatregelen:

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

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

c. met betrekking tot de aanname door Google van een Alternatieve Doorgifteoplossing https://cloud.google.com/terms/alternative-transfer-solution.

4.4 *SCC-audits*. Indien er Klant-SCC's van toepassing zijn zoals beschreven in Artikel 4.1 (Beperkte Doorgiften) van deze voorwaarden van Europese Gegevensbeschermingswetgeving, zal Google Klant (of een door Klant 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 Klant een verwerker is, erkent Klant dat Google, als een andere verwerker, mogelijk niet in staat is de derde-verwerkingsverantwoordelijke te identificeren. Klant 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 Klant 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 Klant-Persoonsgegevens, kan Klant 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.

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 Klant-SCC's (door middel van verwijzing opgenomen in dit Addendum) en de rest van de Overeenkomst (inclusief dit Addendum), prevaleren de Klant-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.

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

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

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

a. Klant-Persoonsgegevens verkopen of delen;

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

i. anders dan voor een zakelijke doeleinde (*"business purpose"*) op grond van de CCPA namens Klant en met het specifieke doeleinde van het uitvoeren van de Diensten en TSS (indien van toepassing); of

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

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

3. Compliance. Onverminderd de verplichtingen van Google op grond van Artikel 5.2 (Compliance met de Instructies van Klant) of andere rechten of verplichtingen van een der partijen op grond van de toepasselijke Overeenkomst, zal Google Klant op de hoogte indien Google, naar eigen inzicht, 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 Klant. Indien Google Klant in kennis stelt van enig ongeoorloofd gebruik van Klant-Persoonsgegevens, inclusief op grond van Artikel 3 (Compliance) van dit subartikel of Artikel 7.2.1 (Kennisgeving van incidenten), kan Klant redelijke en passende maatregelen nemen om dergelijk ongeoorloofd gebruik te beëindigen of te verhelpen door:

a. maatregelen te nemen die worden aanbevolen door Google in overeenstemming met Artikel 7.2.2 (Details van gegevensincident), indien van toepassing; of

b. gebruik te maken van zijn rechten op grond van Artikel 7.5.2(a) (Controle door Klant) of 9.1 (Toegang; Rectificatie; Beperkte Verwerking; Portabiliteit) uit te oefenen.

Turkije

1. Aanvullende definities.

- "*Turkse Gegevensbeschermingswetgeving*" betekent de Turkse wetgeving inzake de bescherming 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 Klant zich in Turkije bevindt en Google optionele aanvullende voorwaarden (inclusief Turkse SCC's) beschikbaar stelt voor aanvaarding door Klant met betrekking tot de doorgifte van Klant-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 Klant aan Google aangetoond.

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

2.3 *SCC-audits*. Indien Klant Turkse SCC's aangaat op grond van dit Artikel 2 (Gegevensdoorgiften), staat Google Klant (of een door Klant aangewezen 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 Klant 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 Klant-Persoonsgegevens, kan Klant 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 voorwaarde ontbreekt, door Google hiervan op de hoogte te stellen.

2.5 *Geen aanpassing 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 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 Klant 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 overige verordeningen die hieronder vallen.

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

Brazilie

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 Klant) of enige andere rechten of verplichtingen van beide partijen onder de toepasselijke Overeenkomst, stelt Google de Klant 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 Klant optreedt als verwerker, zal Klant elke door Google verstrekte 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 Klant-Persoonsgegevens te verwerken in of door te geven aan een Adequaat Land. Indien Klant-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 Klant 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 Klant 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 Klant optreedt als verwerkingsverantwoordelijke of verwerker) op dergelijke doorgiften tussen Google en Klant.

3.2. *Informatie over beperkte doorgiften.* Google verstrekt de Klant 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 Klant optreedt als verwerker, erkent Klant dat Google, als andere verwerker, mogelijk niet in staat is de derde verwerkingsverantwoordelijke te identificeren en zal Klant 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 Klant, 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 Klant met de verwerkingsverantwoordelijke.

3.4. *Beëindiging wegens risico's bij gegevensdoorgifte. Indien Klant 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 Klant-Persoonsgegevens, kan Klant 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 SCCs*. 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 Klantgegevens 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 Klant.
- "*Klantgegevens*", indien niet gedefinieerd in de Overeenkomst, betekent gegevens die door Klant of Eindgebruikers aan Google worden verstrekt via Google Cloud Platform onder het Account, en gegevens die Klant of Eindgebruikers uit die gegevens afleiden door hun gebruik van Google Cloud Platform.
- *"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 bevatten 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 beveiligingsmaatregelen 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 aldus gewijzigd met betrekking tot Bare Metal Solution:

- De definitie voor 'Externe controleur van Google wordt vervangen door:
    - *"Externe Auditor van Google"* betekent een gekwalificeerde en onafhankelijke externe auditor aangewezen door Google of door een Bare Metal Solution Subverwerker, van wie Google de identiteit op verzoek aan Klant zal bekendmaken.
- De volgende voorwaarden worden verwijderd:
    - Uit Artikel 7.1.1 (Beveiligingsmaatregelen van Google), het gedeelte 'Klantgegevens 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 'Blootstelling aan aanvallen van buitenaf', 'Intrusion detection' en 'Versleutelingstechnologieën' en
    - Uit Bijlage 2, deze zinnen van Artikel 3(a):
        - Google slaat gegevens op in een multi-tenant omgeving op servers die in eigendom zijn van Google. Behoudens eventuele andersluidende instructies van Klant (bijvoorbeeld in de vorm van een selectie van een gegevenslocatie), repliceert Google Klantgegevens naar verschillende datacenters op verschillende locaties.

2. Compliance-certificeringen en SOC-rapporten. Google of Subverwerker onderhoudt ten minste het volgende (of een vergelijkbaar of verbeterd alternatief) voor Bare Metal Solution oom 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 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 Klant en, indien Klant een verwerker is, Klant in staat stellen 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 Klant. Onverminderd de uitdrukkelijke verplichtingen van Google met betrekking tot Bare Metal Solution, zal Klant redelijke stappen ondernemen om de beveiliging van Klantgegevens en alle andere content opgeslagen op of verwerkt via Bare Metal Solution te beschermen en te handhaven.

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.

Klant 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, Klantgegevens, software en applicaties die Klant 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 bedoeld om cyberbeveiligingsrisico's te beperken en heeft, als zodanig, bepaalde onderscheidende kenmerken.

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

- Artikel 6.1 (Verwijdering door Klant) 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 Klant-Persoonsgegevens bevatten.

Google Distributed Cloud connected (Google Cloud Platform)

Google Distributed Cloud connected is niet geïmplementeerd bij 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 Klantgegevens 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 Klant.

- 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 afloopt*. Klant instrueert Google om in overeenstemming met de toepasselijke wetgeving alle resterende Klantgegevens te verwijderen (met inbegrip van bestaande kopieën) van de Apparatuur aan het einde van de Looptijd. Indien Klant Klantgegevens na het einde van de Looptijd wil bewaren, kan Klant 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 zijn toegevoegd aan het einde van Artikel 10.1 (Gegevenopslag en verwerkingsfaciliteiten): "of waar de Klantlocatie zich bevindt".

- Artikel 1 (Datacenter en netwerkbeveiliging) van Bijlage 2 (Beveiligingsmaatregelen) wordt vervangen door het volgende:

  - **1. Lokale machines en netwerkbeveiliging**

Lokale machines. Klantgegevens worden uitsluitend opgeslagen op de Apparatuur die op de Klantlocatie wordt ingezet.

Serverbesturingssystemen. Google-servers gebruiken een Linux-gebaseerde implementatie aangepast voor de applicatie-omgeving. Google gebruikt een code-beoordelingsproces om de beveiliging van de code die wordt gebruikt om Google Distributed Cloud connected te leveren en 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 Klant toe om een sterke, versleutelde interconnectie te gebruiken en te configureren tussen de Apparatuur en de Virtual Private Cloud van Klant met Cloud VPN via een IPSEC VPN-verbinding.

Gebonden opslag. Gegevensopslag van Klant 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. 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 Klant of kan mogelijk geen persoonsgegevens versleutelen in de VMware-omgeving van Klant.

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 aangewezen door Google of een NetApp Volumes-subverwerker, van wie Google de identiteit op verzoek aan Klant bekend maakt.

- 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-tenant omgeving op de servers van NetApp, Inc. Behoudens eventuele andersluidende Instructies (bijvoorbeeld in de vorm van een selectie van een gegevenslocatie) repliceert Google Klantgegevens tussen meerdere geografisch verspreide datacenters. Ook isoleert Google Klantgegevens op logische wijze. Klant krijgt controle over specifieke beleidsregels inzake gegevensdeling. Die beleidsregels zullen, in overeenstemming met de functionaliteit van de Diensten, Klant in staat stellen om de productdelingsinstellingen te bepalen die van toepassing zijn op zijn Eindgebruikers voor specifieke doeleinden. Klant 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 Subverwerker verkrijgt ten minste het volgende (of een gelijkwaardig of verbeterd alternatief) 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 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 Klant en, indien Klant een verwerker is, Klant 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).

Google Workspace en Cloud Identity

1. Aanvullende definities.

- *"Account"*, indien niet gedefinieerd in de Overeenkomst, betekent het Google Workspace- of Cloud Identity-account van Klant.

- *"Cloud Identity"*, indien gekocht onder een zelfstandige Overeenkomst en niet als onderdeel van Google Cloud Platform of Google Workspace, betekent de Cloud Identity Diensten zoals beschreven op https://cloud.google.com/terms/identity/user-features.

- *"Klantgegevens"*, indien niet gedefinieerd in de Overeenkomst, betekent gegevens die door of namens Klant of Eindgebruikers van Klant worden ingediend, opgeslagen, verzonden of ontvangen via Google Workspace of Cloud Identity.

- "*Google Workspace"* betekent de Google Workspace- of Google Workspace for Education-diensten beschreven op https://workspace.google.com/terms/user_features.html, naargelang van toepassing.

2. Aanvullende Producten. Indien Google naar eigen keuze Aanvullende Producten beschikbaar stelt aan Klant voor gebruik met Google Workspace of Cloud Identity in overeenstemming met toepasselijke voorwaarden voor Aanvullende Producten:

a. kan Klant Aanvullende producten in- of uitschakelen via de Admin Console en hoeft Klant geen Aanvullende Producten te gebruiken om Google Workspace of Cloud Identity te gebruiken; en

b. indien Klant ervoor kiest om Aanvullende Producten te installeren of deze te gebruiken met Google Workspace of Cloud Identity, kunnen de Aanvullende Producten toegang krijgen tot Klantgegevens voor zover vereist om te interopereren met Google Workspace of Cloud Identity, naargelang van toepassing.

Ter verduidelijking: dit Addendum is niet van toepassing op de verwerking van persoonsgegevens in verband met de levering van Aanvullende Producten die door Klant zijn geïnstalleerd of gebruikt, inclusief persoonsgegevens die naar of vanuit dergelijke Aanvullende Producten worden verzonden.

3. Compliance-certificeringen. De Compliance-certificeringen voor Gecontroleerde Diensten van Google Workspace en Cloud Identity omvatten ook certificaten voor ISO 27017 en ISO 27018.

4. Locaties van datacenters. De locaties van Google Workspace- en Cloud Identity-datacenters worden beschreven op https://www.google.com/about/datacenters/locations/.

5. Informatie over Subverwerkers. Namen, locaties en activiteiten van Google Workspace en Cloud Identity Subverwerkers worden beschreven op https://workspace.google.com/intl/en/terms/subprocessors.html.

6. Cloud-gegevensbeschermingsteam. Er kan contact worden opgenomen met het gegevensbeschermingsteam voor Google Workspace en Cloud Identity (terwijl Beheerders zijn aangemeld bij hun Beheerdersaccount) via https://support.google.com/a/contact/googlecloud_dpr.

7. Aanvullende Beveiligingsmaatregelen. Voor Google Workspace en Cloud Identity:

a. scheidt Google de gegevens van elke Eindgebruiker op logische wijze van de gegevens van andere Eindgebruikers; en

b. zullen gegevens voor een geauthenticeerde Eindgebruiker niet worden getoond aan een andere Eindgebruiker (tenzij de eerste Eindgebruiker of een Beheerder toestaat dat de gegevens worden gedeeld).

8. Informatie over Beperkte Doorgiften. Aanvullende informatie die relevant is voor Beperkte Doorgiften, Aanvullende Beveiligingsmechanismen en andere aanvullende beschermingsmaatregelen is beschikbaar op cloud.google.com/privacy/.

9. Addendum voor Servicegegevens. Indien Google een optioneel Addendum voor Servicegegevens beschikbaar stelt ter acceptatie door Klant in verband met dit Addendum, vormt de beschikbaarheid van dat optionele Addendum een "DPA-update" indien een dergelijke term is gedefinieerd in enig Addendum voor Servicegegevens dat eerder door Klant is aangegaan.

10. Servicespecifieke Voorwaarden.

AppSheet (Google Workspace)

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

- De paragraaf getiteld "Serverbesturingssystemen" in Artikel 1(a) van Bijlage 2 (Beveiligingsmaatregelen) wordt vervangen door het volgende:
    - *Serverbesturingssystemen*. Google-servers gebruiken een op Linux gebaseerde implementatie die is aangepast aan de applicatie-omgeving.

2. Aanvullende datacenterlocaties. Aanvullende datacenterlocaties voor AppSheet worden beschreven op https://cloud.google.com/about/locations/.

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 Klant 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 Klant een aankoop heeft gedaan via een wederverkoper 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 Klant 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)*" betekent de voorwaarden op: https://cloud.google.com/terms/looker/legal/sccs/eu-p2p-intra-group.
- De volgende woorden zijn toegevoegd aan het einde van Artikel 10.1 (Gegevensopslag en -verwerkingsfaciliteiten): "of waar Multi-Cloud Service Third-Party Providers faciliteiten hebben".

3. Aanvullende beveiligingsverantwoordelijkheden van Klant. Klant is verantwoordelijk voor de beveiliging van de eigen 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 Looker (original) Gecontroleerde Diensten 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 Klanten. Klant is niet verplicht te certificeren of zijn bevoegde Toezichthoudende Autoriteit te identificeren zoals beschreven in Artikel 4.2 (Certificering door niet-EMEA Klanten) 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 (original) is beschikbaar op https://docs.looker.com.

8. Informatie over Subverwerkers. Namen, locaties en activiteiten van Subverwerkers voor Looker (original) 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 Google-Managed Multi-Cloud Diensten voor Looker (original).

10. Cloud-gegevensbeschermingsteam. Er kan contact worden opgenomen met 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 Klant verzamelt en bijhoudt, zal Klant 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 Klant 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 voor de apps van Google beveiligen de toegang tot Looker door een enkel punt te bieden om aanvallen te filteren via IP-denylisting en beperking van verbindingssnelheden.

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

SecOps Diensten

1. Aanvullende definities.

- *"Account"*, indien niet gedefinieerd in de Overeenkomst, betekent het SecOps Dienstenof Google Cloud Platform-account van Klant, indien van toepassing.

- *"Klantgegevens"*, indien niet gedefinieerd in de Overeenkomst, betekent (i) gegevens die door Klant of Eindgebruikers aan Google zijn verstrekt via SecOps Diensten onder het Account, en gegevens die Klant of Eindgebruikrs uit die gegevens afleiden door hun gebruik van de SecOps Diensten, of (ii) uitsluitend voor Mandiant Consulting Diensten en Managed Diensten, gegevens die door Klant of Eindgebruikers aan Google zijn verstrekt in verband met het ontvangen van SecOps Diensten.

- *"Door Klant Ingeschakelde Aanbieder"* betekent een dienstverlener (waaronder een verwerker of subverwerker kan vallen) die rechtstreeks door Klant is ingeschakeld onder een afzonderlijke Overeenkomst tussen Klant en deze aanbieder.

- "*SecOps Diensten*" betekent de SecOps Diensten beschreven op https://cloud.google.com/terms/secops/services, exclusief alle Aanbiedingen van Derden.

- "*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 aanwezig) voor beveiliging die Klant naar eigen keuze en/of naar eigen inzicht kan gebruiken, inclusief (indien aanwezig) versleuteling, logging en monitoring, 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; en

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

- Artikel 6.1 (Verwijdering door Klant) wordt gewijzigd en luidt als volgt:

  - 6.1 **Verwijdering door Klant**. Google zal Klant in staat stellen Klantgegevens te verwijderen tijdens de Looptijd op een manier die in overeenstemming is met de functionaliteit van de Diensten of op verzoek. Indien Klant de Diensten gebruikt om Klantgegevens tijdens de Looptijd te verwijderen en die Klantgegevens niet door Klant kunnen worden hersteld, of indien Klant verzoekt om Klantgegevens te verwijderen tijdens de Looptijd, zal dit gebruik of verzoek (naargelang van toepassing) een Instructie aan Google vormen om de relevante Klantgegevens te verwijderen van de systemen van Google in overeenstemming met toepasselijk recht. 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.

- Artikel 9.1 (Toegang; Rectificatie; Beperkte Verwerking; Portabiliteit) is aldus aangepast:

  9.1 **Toegang; Rectificatie; Beperkte verwerking; Portabiliteit**. Gedurende de Looptijd zal Google Klant in staat stellen om, op een wijze die in overeenstemming is met de functionaliteit van de Diensten, toegang te verkrijgen tot Klantgegevens, Klantgegegevens te corrigeren en de verwerking van Klantgegevens te beperken, inclusief zoals beschreven in Artikel 6.1 (Verwijdering door Klant) en om Klantgegevens op verzoek te exporteren. Indien Klant constateert dat Klant-Persoonsgegevens onjuist of verouderd zijn, is Klant ervoor verantwoordelijk om Google op de hoogte te stellen en zal Google Klant assisteren bij het rectificeren van deze gegevens als de Toepasselijke privacywetgeving dit vereist.

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

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

5. Informatie over Subverwerkers. 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 Klant verzamelt en bijhoudt, zal Klant 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 Klant dergelijke informatie op een andere manier verstrekt en bijwerkt.

8. Servicespecifieke Voorwaarden.

Mandiant Consulting Diensten en Managed Diensten

Mandiant Consulting Diensten en Managed Diensten bieden advies- en implementatiediensten (waaronder incidentrespons, strategische paraatheid en technische waarborgen om dreigingen te mitigeren en incidentgerelateerde risico's te verminderen) en beheerde detectie- en reactiediensten, en hebben, door ontwerp, bepaalde onderscheidendekenmerken.

1. Wijzigingen. Het Addendum wordt als volgt gewijzigd uitsluitend met betrekking tot Mandiant Consulting Diensten en Managed Diensten:

- De definitie van “Gegevensincident” wordt aangevuld met:
    - Ter verduidelijking: Gegevensincident omvat geen incidenten die onderworpen zijn aan de Mandiant Consulting Diensten en/of Managed Diensten, naargelang van toepassing.
- Artikel 5.2(b)(i) (Compliance met de Instructies van Klant) wordt vervangen door het volgende:
    - i. Gebruik van de Diensten door Klant; en
- De tweede zin van Artikel 7.1.1 (Beveiligingsmaatregelen van Google) wordt gewijzigd en luidt als volgt:
    - De Beveiligingsmaatregelen kunnen (indien passend) maatregelen omvatten om Klantgegevens 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 Klantgegevens te herstellen na een incident; en voor regelmatige effectiviteitstests.
- Artikel 7.3.1(b) wordt gewijzigd en luidt als volgt:
    - b. het beheren van, het beheren van toegang tot en het beveiligen van de inloggegevens voor account-authenticatie, systemen, software, netwerken en apparaten die Klant gebruikt om de Mandiant Consulting Diensten en/of Managed Diensten, naargelang van toepassing, te ontvangen, of waartoe Klant Google autoriseert toegang te krijgen om de Mandiant Consulting Diensten en/of Managed Diensten te leveren, naargelang van toepassing;

- De nieuwe Artikelen 7.3.1(d) en (e) worden toegevoegd en luiden als volgt:
    - d. het minimaliseren van de hoeveelheid Klantgegevens die door of namens Klant aan Google worden verstrekt; en
    - e. voor zover de toegang van Google tot Klantgegevens onder controle van Klant valt, het intrekken van die toegang zodra Google de Mandiant Consulting Diensten en/of Managed Diensten heeft voltooid, naargelang van toepassing.
- Bijlage 2 (Beveiligingsmaatregelen) wordt vervangen door het volgende:
    - Bijlage 2: Aanvullende technische en organisatorische maatregelen

1. Door Klant beheerde omgeving. Google zal alleen toegang hebben tot en Klantgegevens verwerken die door of namens Klant aan Google worden verstrekt via een door Klant beheerd of goedgekeurd account of omgeving.

2. Processen en beleidsregels voor gegevenstoegang – Toegangsbeleid. De processen en beleidsregels van Google voor gegevenstoegang zijn ontworpen om te voorkomen dat ongeautoriseerde personen en/of systemen toegang krijgen tot systemen die worden gebruikt om Klantgegevens te verwerken. Google (i) staat personen alleen toe om toegang te krijgen tot gegevens waartoe zij zijn geautoriseerd, en (ii) neemt stappen om ervoor te zorgen dat persoonsgegevens niet kunnen worden gelezen, gekopieerd, gewijzigd of verwijderd zonder autorisatie tijdens verwerking en gebruik. Het toekennen of wijzigen van toegangsrechten door Google is gebaseerd op de verstrekking door Klant van eindgebruikertoegang tot zijn account of omgeving.

3. Personeelsbeveiliging. Van Google-personeel wordt vereist dat zij zich gedragen in overeenstemming met de richtlijnen van het bedrijf inzake vertrouwelijkheid, bedrijfsethiek, passend gebruik en professionele standaarden. Google voert redelijke antecedentenonderzoeken uit, voor zover wettelijk toegestaan en in overeenstemming met toepasselijke lokale arbeidswetgeving en wettelijke voorschriften.

Personeel is verplicht een geheimhoudingsverklaring te ondertekenen en moet de ontvangst van en compliance met de vertrouwelijkheids- en privacybeleidsregels van Google bevestigen. Personeel krijgt beveiligingstraining. Personeel dat Klantgegevens verwerkt, moet aanvullende vereisten voltooien die passend zijn voor hun rol (bijv. certificeringen). Google-personeel zal Klantgegevens niet verwerken zonder autorisatie.

4. Aanvullende Beveiligingsmaatregelen. Google en Klant kunnen aanvullende beveiligingsmaatregelen overeenkomen in het toepasselijke Bestelformulier, inclusief eventuel bijgevoegde Statement of Work, voor de Mandiant Consulting Diensten en/of Managed Diensten, naargelang van toepassing.

2. Door Klant Ingeschakelde Aanbieder. Ter verduidelijking, en onverminderd de verplichtingen van Google op grond van Artikel 7 (Gegevensbeveiliging) of 11 (Subverwerkers), beschrijft Bijlage 2

(Beveiligingsmaatregelen) niet de beveiligingsmaatregelen of -mechanismen die worden geïmplementeerd of geleverd door Klant of door Klant Ingeschakelde Aanbieders.

Implementatiediensten

1. Aanvullende definities.

- "*Klantgegevens*" betekent gegevens waarvoor Klant Google-personeel autoriseert toegang te krijgen op door Klant Beheerde Systemen.
- "*Door Klant Beheerde Systemen*" betekent het volgende, zoals gebruikt door Klant om Implementatiediensten te ontvangen: (a) door Klant beheerde instanties van Google Cloud Diensten of clouddiensten van derden; en (b) hardware of software gehost of beheerd in de on-premises omgeving van Klant.
- *"Google Cloud Diensten*" betekent alle Diensten beschreven in deze Bijlage 4 (Specifieke producten), met uitzondering van Implementatiediensten, Mandiant Consulting Diensten en Managed Diensten.
- "*Google-personeel*" betekent Google-medewerkers en -onderaannemers zijn betrokken bij het leveren van Implementatiediensten.
- "*Implementatiediensten*" betekent advies-, consultancy- en implementatiediensten geleverd door medewerkers en -onderaannemers van Google ter ondersteuning van Google Cloud Diensten zoals beschreven in de Overeenkomst, waaronder in een Bestelformulier of een Statement of Work.

2. Wijzigingen. Dit Addendum is aldus gewijzigd met betrekking tot Implementatiediensten:

- De definitie voor "Aanvullende Beveiligingsmechanismen" wordt verwijderd.
- De definitie voor "Gegevensincident" wordt vervangen door het volgende:
    - "*Gegevensincident*" betekent een schending van Artikel 7.1 (Googles Beveiligingsmaatregelen, -mechanismen en -assistentie) door Google-personeel, die onbedoeld of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging, of de ongeoorloofde verstrekking van of toegang tot Klant-Persoonsgegevens.
- Behoudens de rest van dit artikel, wordt de term "Klantgegevens" vervangen door "Klant-Persoonsgegevens" wanneer gebruikt in (a) Artikel 2 (Definities) in de definitie van "Subverwerker" en (b) in andere artikelen van dit Addendum. Ter verduidelijking: andere definities in Artikel 2 (Definities) blijven ongewijzigd.
- Artikel 3 (Duur) wordt vervangen door het volgende:

- **3. Duur**. Ongeacht of de toepasselijke Overeenkomst is beëindigd of verlopen, blijft dit Addendum van kracht totdat en verloopt het automatisch wanneer Google geen toegang meer heeft tot Klant-Persoonsgegevens.

- Artikel 6 (Gegevensverwijdering) is vervangen door het volgende:

    - **6. Gegevensverwijdering.** Aan het einde van de Looptijd zal Klant (a) bepalen of Klant-Persoonsgegevens moeten worden verwijderd, en (b) verantwoordelijk zijn voor een dergelijke verwijdering.

- De tweede zin van Artikel 7.1.1 (Beveiligingsmaatregelen van Google) wordt vervangen door het volgende:

    - "De Beveiligingsmaatregelen kunnen (indien passend) maatregelen omvatten om Klantgegevens te versleutelen; om de voortdurende vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van Googles systemen en diensten te waarborgen; om te helpen bij het tijdig herstellen van toegang tot Klantgegevens na een incident; en voor regelmatige effectiviteitstests."

- Artikel 7.1.3 (Aanvullende Beveiligingsmechanismen) wordt verwijderd, evenals alle overige verwijzingen naar dat artikel.

- Artikel 9.1 (Toegang; Rectificatie; Beperkte verwerking; Portabiliteit) wordt vervangen door het volgende:

    - 9.1 *Toegang; Rectificatie; Beperkte verwerking; Portabiliteit*. Klant is verantwoordelijk voor het gebruik van de functionaliteit van de Door Klant Beheerde Systemen om toegang te krijgen tot, rectificatie en beperking van de verwerking van Klant-Persoonsgegevens uit te voeren, onder meer indien Klant constateert dat Klant-Persoonsgegevens onjuist of verouderd zijn en Klant op grond van Toepasselijke verplicht is die gegevens te rectificeren of te verwijderen.

- Artikel 11.4 (Mogelijkheid om bezwaar te maken tegen Subverwerkers) wordt vervangen door het volgende:

    - 11.4 *Mogelijkheid om bezwaar te maken tegen Subverwerkers*. Wanneer tijdens de Looptijd een Nieuwe Subverwerker wordt ingeschakeld, dan zal Google Klant op de hoogte stellen van de inschakeling van de Nieuwe Subverwerker voordat deze Klant-Persoonsgegevens verwerkt. Klant kan bezwaar maken tegen de Nieuwe Subverwerker door Google hiervan in kennis te stellen en, indien Klant dit doet, zullen de partijen te goeder trouw samenwerken om een wederzijds aanvaardbaar alternatief vast te stellen.

- Bijlage 1 (Onderwerp en details van gegevensverwerking) wordt als volgt gewijzigd:

    - Het Artikel "Duur van de verwerking" wordt vervangen door het volgende:

- *"Duur van de verwerking*. De Looptijd plus (indien van toepassing) de periode vanaf het einde van de Looptijd tot het verstrijken van de toegang van Google tot Klant-Persoonsgegevens."

- De woorden "aan Google verstrekt via de Diensten" in de Artikelen "Categorieën van gegevens" en "Betrokkenen" worden vervangen door "toegankelijk gemaakt voor Google in verband met de Diensten".

- Bijlage 2 (Beveiligingsmaatregelen) wordt vervangen door het volgende:

  - **Bijlage 2: Beveiligingsmaatregelen**

1. Door Klant Beheerde Systemen. Google-personeel zal enkel toegang krijgen tot en Klant-Persoonsgegevens verwerken op Door Klant Beheerde Systemen. Indien die systemen Google Cloud Diensten omvatten, blijft het gebruik van Klant van Google Cloud Diensten onderworpen aan de overeenkomst die van toepassing is op die diensten.

2. Toegangsbeheer. De interne processen en beleidsregels van Google zijn ontworpen om te voorkomen dat ongeautoriseerde personen en systemen toegang krijgen tot Google Cloud Diensten die worden gebruikt om persoonsgegevens te verwerken. Het beleid van Google (i) staat Google-personeel alleen toe toegang te krijgen tot gegevens waartoe zij zijn geautoriseerd; en (ii) vereist dat Google-personeel Klant-Persoonsgegevens niet leest, kopieert, wijzigt of verwijdert zonder autorisatie tijdens verwerking, gebruik en na vastlegging. Klant beheert het toekennen of wijzigen van toegangsrechten voor eindgebruikers tot Door Klant Beheerde Systemen. Indien die systemen Google Cloud Diensten omvatten, worden details met betrekking tot workflowtools die auditrecords van wijzigingen en systeemtoegangslogs bijhouden, behandeld in de overeenkomst voor de toepasselijke Google Cloud Diensten.

3. Personeelsbeveiliging. Van Google-personeel wordt vereist dat zij zich gedragen in overeenstemming met de richtlijnen van het bedrijf met betrekking tot vertrouwelijkheid, bedrijfsethiek, passend gebruik en professionele standaarden. Google voert redelijke en passende antecedentenonderzoeken uit voor zover deze wettelijk zijn toegestaan en in overeenstemming met toepasselijke lokale arbeidswetgeving en wettelijke voorschriften.

Google-personeel is verplicht een geheimhoudingsverklaring te ondertekenen en moet de ontvangst en compliance met de vertrouwelijkheids- en privacybeleidsregels van Google bevestigen. Google-personeel krijgt beveiligingstraining. Google-personeel dat Klant-Persoonsgegevens verwerkt, moet aanvullende vereisten voltooien die passend zijn voor hun rol (bijv. certificeringen).

4. Aanvullende Beveiligingsmaatregelen. Google en Klant kunnen aanvullende beveiligingsmaatregelen overeenkomen in de Overeenkomst, inclusief in een Bestelformulier of een Statement of Work.

5. Beveiliging van Subverwerkers. Voordat Subverwerkers worden ingeschakelt, voert Google een audit uit van de beveiligings- en privacypraktijken van Subverwerkers om te waarborgen dat de Subverwerkers een niveau van beveiliging en privacy bieden dat passend is bij hun toegang tot

gegevens en de omvang van de diensten die zij geacht worden te leveren. Zodra Google de risico's die de Subverwerker met zich meebrengt heeft beoordeeld, wordt Subverwerker, onder voorbehoud van de vereisten in Artikel 11.3 (Vereisten voor inschakeling van Subverwerkers), verplicht passende beveiligings-, vertrouwelijkheids- en privacycontractvoorwaarden aan te gaan.

3. Beveiligingsverantwoordelijkheden van Klant. Naast de verplichtingen van Klant onder Artikel 7.3.1 (Beveiligingsmaatregelen van Klant), is Klant verantwoordelijk voor het volgende:

- het beheren, het beheren van toegang tot en het beveiligen van Door Klant Beheerde Systemen, inclusief het minimaliseren van de toegang van Google-personeel tot Klant-Persoonsgegevens voor zover redelijkerwijs haalbaar en het beëindigen van die toegang na voltooiing van de Implementatiediensten; en

- het implementeren van eventuele beveiligingsaanbevelingen die door Google schriftelijk aan Klant worden verstrekt met betrekking tot Door Klant Beheerde Systemen.

4. Compliance-certificering. Google zal certificaten voor ISO 27001, ISO 27017 en ISO 27018 onderhouden voor Implementatiediensten die worden geleverd ter ondersteuning van Google Cloud Platform en Google Workspace (de "*Compliance-certificeringen voor Implementatiediensten*"). Google kan te allen tijde standaarden toevoegen. Google kan een Compliance-certificeringen voor Implementatiediensten vervangen door een gelijkwaardig of verbeterd alternatief.

5. Beoordelingen van Compliance-certificering. Om compliance met haar verplichtingen onder dit Addendum aan te tonen, zal Google de Compliance-certificering voor Implementatiediensten beschikbaar stellen voor beoordeling door Klant en, indien Klant een verwerker is, Klant toestaan om toegang te vragen voor de derde-verwerkingsverantwoordelijke tot de Compliance-certificering voor Implementatiediensten.

6. Gegevensverwerkingslocaties. Klant-Persoonsgegevens kunnen in elk land worden verwerkt waar Google Implementatiediensten levert of waar Klant Door Klant Beheerde Systemen onderhoudt.

7. Geen certificering door niet-EMEA Klanten. Klant is niet verplicht te certificeren of zijn bevoegde Toezichthoudende Autoriteit te identificeren zoals beschreven in Artikel 4.2 (Certificering door niet-EMEA Klanten) van de Europese voorwaarden voor gegevensbescherming in Bijlage 3 (Specifieke privacywetgeving) voor Implementatiediensten.

8. Informatie over Subverwerkers. Subverwerkers voor Implementatiediensten worden (als subcontractors) geïdentificeerd in een toepasselijk Bestelformulier, Statement of Work, of andere bevestiging die vóór aanvang van de Implementatiediensten aan Klant worden verstrekt, of zullen Google-entiteiten zijn. Google zal op verzoek namen, locaties en activiteiten van Subverwerkers voor Implementatiediensten beschikbaar stellen aan Klant.

9. Verwerkingsregisters van Google. Voor zover enige Toepasselijke Privacywetgeving vereist dat Google bepaalde informaite met betrekking tot Klant verzamelt en bijhoudt, zal Klant dergelijke informatie op verzoek aan Google verstrekken, en Google op de hoogte stellen van van updates die

nodig zijn om dergelijke informatie accuraat en up-to-date te houden, tenzij Google verzoekt dat Klant dergelijke informatie op een andere manier aanlevert en bijwerkt.

Google Cloud Skills Boost voor organisaties

1. Aanvullende definities.

- *"Account"*, indien niet gedefinieerd in de Overeenkomst, betekent het Klant-account voor Google Cloud Skills Boost voor organisaties van Klant.

- *"GCSBO"* betekent educatieve, training- en leerdiensten en inhoud die wordt geleverd via https://www.cloudskillsboost.google/ (of een andere website die door Google wordt beheerd of gecontroleerd en gebruikt voor Google Cloud Skills Boost voor organisaties).

- *"TSS"* betekent technische ondersteuningsdiensten die Google naar eigen inzicht aan Klant kan leveren.

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

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

    - "*Aanvullende Beveiligingsmechanismen*" betekent middelen, functies, functionaliteiten en/of mechanismen (indien aanwezig) voor beveiliging die Klant naar eigen keuze en/of naar eigen inzicht kan gebruiken, waaronder (indien aanwezig) versleuteling, logging en monitoring, identiteits- en toegangsbeheer en beveiligingsscans.

- 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 de volgende:

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

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

    - "SCC's (Verwerker-naar-Verwerker)" betekent de voorwaarden zoals opgenomen op: https://cloud.google.com/terms/skillsboost-organizations/sccs/eu-p2p; en

    - "SCC's (Verwerker-naar-Verwerker, Google Exporteur)" betekent de voorwaarden zoals opgenomen op: https://cloud.google.com/terms/skillsboost-organizations/sccs/eu-p2p-intra-group.

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

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

5. Informatie over Subverwerkers. Namen, locaties en activiteiten van GCSBO Subverwerkers worden beschreven op:

a. https://cloud.google.com/terms/skillsboost-organizations/subprocessors; en

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

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

7. Verwerkingsregisters van Google. Voor zover enige Toepasselijke Privacywetgeving vereist dat Google bepaalde informatie met beterkking tot Klant verzamelt en bijhoudt, zal Klant 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 Klant dergelijke informatie via een andere methode aanlevert en bijwerkt.

Eerdere versies van Gegevensverwerkings- en Beveiligingsvoorwaarden:

9 april 2024 *30 juni 2022* *24 september 2021* *19 augustus 2020* *10 augustus 2020* *17 juli 2020* *11 oktober 2019* *1 oktober 2019* *25 mei 2018* *13 maart 2018* *9 november 2017* *11 oktober 2017* *7 februari 2017* *6 oktober 2016*

Eerdere versies van het Amendement Gegevensverwerking:

7 juli 2022 *24 september 2021* *27 mei 2021* *29 oktober 2019* *25 mei 2018* *25 april 2018* *11 juli 2017* *28 november 2016* *7 januari 2016* *24 april 2015* *1 april 2014* *14 november 2012*

Eerdere versies van het Addendum Gegevensverwerking voor Diensten van Looker (original) (Klanten):

14 februari 2023 4 januari 2023 20 september 2022 30 juni 2022 16 maart 2022 24 september 2021 1 april 2021 15 januari 2021 17 december 2020 28 augustus 2020 1 juni 2020 9 maart 2020

Eerdere versies van SecOps Diensten DPST (Klanten):

6 februari 2023 28 november 2022 27 september 2021 1 oktober 2020

Eerdere versies van het Addendum Gegevensverwerking voor SecOps Consulting Diensten en Managed Diensten.

5 oktober 2023 19 september 2023 15 juni 2023 22 februari 2023 6 februari 2023

Eerdere versies *(Laatst gewijzigd 15 oktober 2024)*

26 september 2024 9 september 2024 5 augustus 2024 23 mei 2024 9 april 2024 8 november 2023 15 augustus 2023 20 september 2022