

Google Ads Voorwaarden voor Gegevensverwerking

Google en de wederpartij die instemt met deze voorwaarden ("**Klant**") zijn een overeenkomst aangegaan voor de levering van de Verwerkingsdiensten (zoals van tijd tot tijd gewijzigd, de "**Overeenkomst**").

De Google Ads Voorwaarden voor gegevensverwerking (met inbegrip van de bijlagen, "**Voorwaarden voor Gegevensverwerking**") worden door Google en Klant aangegaan en vormen een aanvulling op de Overeenkomst. Deze Voorwaarden voor Gegevensverwerking gaan van kracht, en vervangen eventuele eerder toepasselijke voorwaarden met betrekking tot het onderwerp hiervan, (met inbegrip van eventuele wijzigingen inzake gegevensverwerking of addenda inzake gegevensverwerking met betrekking tot de Verwerkingsdiensten) op de Ingangsdatum Voorwaarden.

Als u namens Klant deze Voorwaarden voor Gegevensverwerking accepteert, garandeert u dat: (a) u volledige juridische bevoegdheid heeft om Klant te binden aan deze Voorwaarden voor Gegevensverwerking ; (b) u deze Voorwaarden voor Gegevensverwerking heeft gelezen en begrepen; en (c) u, namens Klant, instemt met deze Voorwaarden voor Gegevensverwerking. Als u niet de juridische bevoegdheid hebt om Klant te binden, stem dan niet in met deze Voorwaarden voor Gegevensverwerking.

1. Inleiding

Deze Voorwaarden voor Gegevensverwerking geven uitdrukking aan de overeenstemming van partijen over de voorwaarden van de verwerking van bepaalde gegevens in het kader van de Europese Wetgeving inzake gegevensbescherming en bepaalde niet-Europese Wetgeving inzake gegevensbescherming.

2. Definities en interpretatie

2.1 In deze Voorwaarden voor Gegevensverwerking hebben de volgende begrippen de volgende betekenissen:

“Extra product”: een door Google of een derde geleverd(e) product, dienst of toepassing die of dat: (a) geen deel uitmaakt van de Verwerkingsdiensten; en (b) toegankelijk is voor gebruik binnen de gebruikersinterface van de Verwerkingsdiensten of op een andere wijze geïntegreerd is met de Verwerkingsdiensten.

“Aanvullende Voorwaarden voor niet-Europese Wetgeving inzake gegevensbescherming”: de aanvullende voorwaarden als opgenomen in Bijlage 3, die uitdrukking geven aan de overeenstemming van partijen over de voorwaarden die van toepassing zijn op de verwerking van bepaalde gegevens in verband met bepaalde niet-Europese Wetgeving inzake gegevensbescherming.

“Aangeslotene”: een entiteit die direct of indirect zeggenschap uitoefent over, waarover zeggenschap wordt uitgeoefend door, of onder gezamenlijke zeggenschap staat met, een partij.

“Persoonsgegevens van Klant”: persoonsgegevens die in het kader van het leveren door Google van de Verwerkingsdiensten door Google namens Klant worden verwerkt.

“Data-incident”: een inbreuk op de beveiliging van Google die resulteert in de/het onvoorziene of onrechtmatige vernietiging, verlies, wijziging, ongeoorloofde openbaarmaking van, of toegang tot, Persoonsgegevens van Klant op systemen die door Google beheerd of anderszins gecontroleerd worden. “Data-incidenten” omvatten geen mislukte pogingen of activiteiten die de beveiliging van de Persoonsgegevens van Klant niet in gevaar brengen, met inbegrip van mislukte inlogpogingen, pings, poortscans, denial-of-service-aanvallen en andere netwerkaanvallen op firewalls of netwerksystemen.

“Betrokkene-instrument”: een instrument (indien van toepassing) dat door een Google Entiteit aan betrokkenen beschikbaar wordt gesteld en dat Google in staat stelt om direct en op gestandaardiseerde wijze te reageren op bepaalde verzoeken van betrokkenen met betrekking tot Persoonsgegevens van Klant (bijvoorbeeld instellingen voor online advertentie instellingen of een opt-out browser-plugin).

“EER”: de Europese Economische Ruimte.

“EU AVG”: 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 Wetgeving inzake gegevensbescherming": naargelang het toepasselijke geval (a) de AVG; en/of (b) de Federale Wet Bescherming Persoonsgegevens van 19 Juni 1992 (Zwitserland).

"Europese of nationale wetgeving": naargelang het geval: (a) EU-wetgeving of wetgeving van EU-lidstaten (als de EU AVG van toepassing is op de verwerking van Persoonsgegevens van Klant); en/of (b) de wetgeving van het Verenigd Koninkrijk ('VK') of een deel van het Verenigd Koninkrijk (als de VK AVG van toepassing is op de verwerking van Persoonsgegevens van Klant).

"AVG": naargelang het toepasselijke geval: (a) de EU AVG; en/of (b) de VK AVG.

"Google": de Google Entiteit die partij is bij de Overeenkomst.

"Google Aangeslotenen Subverwerkers": heeft de betekenis die hieraan gegeven wordt in artikel 11.1 (Toestemming voor het inschakelen van subverwerkers).

"Google Entiteit": Google LLC (voorheen bekend als Google Inc.), Google Ireland Limited of een andere Aangeslotene van Google LLC.

"ISO 27001-certificering": ISO/IEC 27001:2013-certificering of een vergelijkbare certificering voor de Verwerkingsdiensten.

"Niet-Europese Wetgeving inzake gegevensbescherming": wetgeving inzake gegevensbescherming of privacy die van kracht is buiten de EER, Zwitserland en het VK.

"E-mailadres voor kennisgevingen": het e-mailadres (indien van toepassing) dat door de Klant doorgegeven is via de gebruikersinterface van de Verwerkingsdiensten of een ander door Google aangeboden middel voor het ontvangen van bepaalde kennisgevingen van Google met betrekking tot deze Voorwaarden voor Gegevensverwerking.

"Privacy Shield": het juridisch kader van het EU-U.S. Privacy Shield, het Swiss-U.S. Privacy Shield, en elk gelijkwaardig wettelijk kader dat van toepassing kan zijn tussen het Verenigd Koninkrijk en de Verenigde Staten.

"Verwerkingsdiensten": de toepasselijke diensten die vermeld zijn op privacy.google.com/businesses/adsservices.

"Beveiligingsdocumentatie": het certificaat dat afgegeven is voor de ISO 27001-certificering en andere beveiligingscertificeringen of documentatie die

Google kan verstrekken ten aanzien van de Verwerkingsdiensten.

“Beveiligingsmaatregelen”: heeft de betekenis die hieraan gegeven wordt in artikel 7.1.1 (Beveiligingsmaatregelen van Google).

“Subverwerkers”: derden die uit hoofde van deze Voorwaarden voor Gegevensverwerking bevoegd zijn tot logische toegang tot en het verwerken van Persoonsgegevens van Klant om delen van de Verwerkingsdiensten en hiermee samenhangende technische ondersteuning te leveren.

“Toezichthoudende Autoriteit”: naargelang het toepasselijke geval: (a) een “toezichthoudende autoriteit” zoals gedefinieerd in de EU AVG; en/of (b) de “Commissioner” zoals gedefinieerd in de UK AVG.

“Looptijd”: de periode vanaf de Ingangsdatum Voorwaarden tot het einde van levering door Google van de Verwerkingsdiensten uit hoofde van deze Overeenkomst.

“Ingangsdatum Voorwaarden”: zoals van toepassing:

- (a) 25 mei 2018, indien Klant heeft geklikt om akkoord te gaan, of partijen anderszins ingestemd hebben met deze Voorwaarden voor Gegevensverwerking vóór of op die datum; of
- (b) de datum waarop Klant heeft geklikt om akkoord te gaan, of partijen anderszins ingestemd hebben met deze Voorwaarden voor Gegevensverwerking, indien deze datum na 25 mei 2018 is.

“Derde Subverwerkers”: heeft de betekenis die hieraan wordt gegeven in artikel 11.1 (Toestemming voor het inschakelen van subverwerkers).

“VK AVG”: de EU AVG zoals gewijzigd en opgenomen in wetgeving van het Verenigd Koninkrijk krachtens de UK European Union (Withdrawal) Act 2018, indien van kracht.

- 2.2 De termen **“verwerkingsverantwoordelijke”**, **“betrokkene”**, **“persoonsgegevens”**, **“verwerking”** en **“verwerker”** hebben, zoals in deze Voorwaarden voor Gegevensverwerking gebruikt, de betekenis die hieraan in de AVG wordt gegeven.
- 2.3 De woorden **“met inbegrip van”** en **“waaronder”** betekenen **“inclusief maar niet beperkt tot”**. Alle voorbeelden in deze Voorwaarden voor Gegevensverwerking zijn illustratief en zijn niet de enige voorbeelden van een bepaald concept.

- 2.4 Elke verwijzing naar een juridisch kader, wet of andere wettelijke maatregel is een verwijzing hiernaar zoals van tijd tot tijd gewijzigd of opnieuw uitgevaardigd.
- 2.5 Indien deze Voorwaarden voor Gegevensverwerking zijn vertaald in een andere taal, en er een discrepantie bestaat tussen de Engelse tekst en de vertaalde tekst, dan is de Engelse tekst leidend.

3. Duur van deze Voorwaarden voor Gegevensverwerking

Deze Voorwaarden voor Gegevensverwerking gaan in op de Ingangsdatum Voorwaarden en blijven, ondanks het verstrijken van de Looptijd van kracht tot, en vervallen automatisch bij, verwijdering van alle Persoonsgegevens van Klant door Google zoals beschreven in deze Voorwaarden voor Gegevensverwerking.

4. Toepassing van deze Voorwaarden voor Gegevensverwerking

- 4.1 **Toepassing van Europese Wetgeving inzake gegevensbescherming.** De Artikelen 5 (Gegevensverwerking) tot 12 (Contact opnemen met Google; Register van verwerkingsactiviteiten) (inclusief) gelden alleen voor zover de Europese Wetgeving inzake gegevensbescherming van toepassing is op de verwerking van Persoonsgegevens van Klant, waaronder indien:
- (a) de verwerking plaatsvindt in het kader van de activiteiten van een vestiging van Klant binnen de EER of het Verenigd Koninkrijk; en/of
 - (b) Persoonsgegevens van Klant persoonsgegevens zijn die betrekking hebben op betrokkenen die zich bevinden in de EER of het Verenigd Koninkrijk en de verwerking betrekking heeft op het aan hen aanbieden van goederen of diensten of het monitoren op hun gedrag binnen de EER of het Verenigd Koninkrijk.
- 4.2 **Toepasselijkheid op Verwerkingsdiensten.** Deze Voorwaarden voor

Gegevensverwerking zijn alleen van toepassing op de Verwerkingsdiensten waarvoor partijen ingestemd hebben met deze Voorwaarden voor Gegevensverwerking (bijvoorbeeld: (a) de Verwerkingsdiensten waarvoor de Klant geklikt heeft om akkoord te gaan met deze Voorwaarden voor Gegevensverwerking; of (b) als in de Overeenkomst deze Voorwaarden voor Gegevensverwerking door verwijzing zijn opgenomen, de Verwerkingsdiensten die het onderwerp zijn van de Overeenkomst).

- 4.3 **Opneming van Aanvullende Voorwaarden voor Niet-Europese Wetgeving inzake gegevensbescherming.** De Aanvullende Voorwaarden voor niet-Europese Wetgeving inzake gegevensbescherming vormen een aanvulling op deze Voorwaarden voor gegevensverwerking.

5. Gegevensverwerking

5.1 Rollen en naleving van regelgeving; Authorisatie

5.1.1 **Verantwoordelijkheden van Verwerker en Verwerkingsverantwoordelijke.** Partijen erkennen en stemmen ermee in dat:

- (a) Bijlage 1 het onderwerp en de details beschrijft van de verwerking van Persoonsgegevens van Klant.
- (b) Google op grond van de Europese Wetgeving inzake gegevensbescherming een verwerker van Persoonsgegevens van Klant is;
- (c) Klant op grond van de Europese Wetgeving inzake gegevensbescherming, een verwerkingsverantwoordelijke of een verwerker is, zoals van toepassing, van Persoonsgegevens van Klant; en
- (d) elke partij voldoet aan de verplichtingen die voor haar gelden uit hoofde van de Europese Wetgeving inzake gegevensbescherming met betrekking tot de verwerking van Persoonsgegevens van Klant.

5.1.2 **Authorisatie van Derde Verwerkingsverantwoordelijke.** Als Klant een verwerker is, verzekert Klant aan Google dat voor de instructies en het handelen van Klant ten aanzien van Persoonsgegevens van Klant, met inbegrip van het door hem aanwijzen van Google als een andere

verwerker, autorisatie verleend is door de desbetreffende Verwerkingsverantwoordelijke.

- 5.2 **Instructies van Klant.** Door in te stemmen met deze Voorwaarden voor Gegevensverwerking, geeft Klant Google opdracht om Persoonsgegevens van Klant uitsluitend in overeenstemming met toepasselijk recht te verwerken: (a) om Verwerkingsdiensten en samenhangende technische ondersteuning te verlenen; (b) zoals nader bepaald door middel van het gebruik door Klant van de Verwerkingsdiensten (met inbegrip van de instellingen en andere functionaliteiten van de Verwerkingsdiensten); (c) zoals vastgelegd in de vorm van de Overeenkomst, met inbegrip van deze Voorwaarden voor Gegevensverwerking; en (d) zoals nader vastgelegd in andere door de Klant verstrekte schriftelijke instructies en die door Google zijn erkend als zijnde instructies voor de doeleinden van deze Voorwaarden voor Gegevensverwerking.
- 5.3 **Voldoen aan Instructies door Google.** Google voldoet aan de instructies die beschreven zijn in artikel 5.2 (Instructies van Klant) (waaronder met betrekking tot gegevensdoorgifte), tenzij Europese of nationale wetgeving die op Google van toepassing is andere verwerking vereist van Persoonsgegevens van Klant door Google, in welk geval Google Klant hierover zal informeren (tenzij dergelijke wetgeving Google dit verbiedt op grond van belangrijke redenen van openbaar belang).
- 5.4 **Extra producten.** Als Klant gebruikt maakt van een Extra product, kunnen de Verwerkingsdiensten toestaan dat dit Extra product toegang heeft tot de Persoonsgegevens van Klant zoals vereist voor de interoperabiliteit van het Extra product met de Verwerkingsdiensten. Voor de duidelijkheid: deze Voorwaarden voor Gegevensverwerking zijn niet van toepassing op de verwerking van persoonsgegevens in verband met de levering van een door de Klant gebruikt Extra product, met inbegrip van persoonsgegevens die verzonden worden naar of uit dat Extra product.

6. Verwijdering van gegevens

- 6.1 **Verwijdering tijdens de Looptijd.**
- 6.1.1 **Verwerkingsdiensten met een verwijderingsfunctionaliteit.** Tijdens de Looptijd, als:
- (a) de functionaliteit van de Verwerkingsdiensten voor de Klant

de optie bevat om Persoonsgegevens te verwijderen;

- (b) Klant de Verwerkingsdiensten gebruikt om bepaalde Persoonsgegevens van Klant te verwijderen; en
- (c) de verwijderde Persoonsgegevens van Klant door Klant niet teruggehaald kunnen worden (bijvoorbeeld uit de “Prullenbak”),

dan zal Google deze Persoonsgegevens van Klant uit zijn systemen verwijderen zo snel als dit redelijkerwijs mogelijk is en binnen een periode van maximaal 180 dagen, tenzij op grond van Europese of nationale wetgeving opslag verplicht is.

6.1.2 **Verwerkingsdiensten zonder een verwijderingsfunctionaliteit.** Als de functionaliteit van de Verwerkingsdiensten tijdens de Looptijd voor Klant niet de optie bevat om Persoonsgegevens van Klant te verwijderen, zal Google voldoen aan:

- (a) elk redelijk verzoek van Klant om het verwijderen van deze gegevens te faciliteren, voor zover dit mogelijk is rekening houdend met de aard en functionaliteit van de Verwerkingsdiensten, en tenzij op grond van Europese of nationale wetgeving opslag verplicht is;
- (b) de praktijken voor gegevensbewaring zoals beschreven op policies.google.com/technologies/ads.

Voor het verwijderen van gegevens op grond van artikel 6.1.2(a) mag Google een vergoeding in rekening brengen (op basis van door Google redelijk gemaakte kosten). Google verstrekt Klant vóór het verwijderen van dergelijke gegevens nadere informatie over een eventuele van toepassing zijnde vergoeding, alsmede de basis voor de berekening hiervan.

6.2 **Verwijdering bij het verstrijken van de Looptijd.** Bij het verstrijken van de Looptijd instrueert Klant Google om alle Persoonsgegevens van Klant (met inbegrip van bestaande kopieën) overeenkomstig toepasselijk recht uit de systemen van Google te verwijderen. Google voldoet aan deze instructie zo snel als redelijkerwijs mogelijk is en binnen een periode van maximaal 180 dagen, tenzij op grond van Europese of nationale wetgeving opslag verplicht is.

7. Gegevensbeveiliging

7.1 Beveiligingsmaatregelen en hulp van Google.

- 7.1.1 **Beveiligingsmaatregelen van Google.** Google implementeert en behoudt technische en organisatorische maatregelen ter bescherming van Persoonsgegevens van Klant tegen de/het onvoorziene of onrechtmatige vernietiging, verlies, wijziging, ongeoorloofde openbaarmaking of toegang, zoals beschreven in Bijlage 2 (de "**Beveiligingsmaatregelen**"). Zoals beschreven in Bijlage 2, omvatten de Beveiligingsmaatregelen maatregelen: (a) voor het encrypten van persoonsgegevens; (b) om de voortdurende vertrouwelijkheid, integriteit, beschikbaarheid en weerbaarheid te helpen bewerkstelligen van de systemen en diensten van Google (c) voor het helpen herstellen van tijdige toegang tot persoonsgegevens na een incident; en (d) voor het regelmatig testen van effectiviteit. Google kan de Beveiligingsmaatregelen van tijd tot tijd bijwerken of wijzigen, op voorwaarde dat deze bijwerkingen en wijzigingen niet leiden tot de aantasting van de algemene veiligheid van de Verwerkingsdiensten.
- 7.1.2 **Naleving van beveiligingsmaatregelen door personeel van Google.** Google neemt passende maatregelen om te zorgen voor naleving van de Beveiligingsmaatregelen door zijn werknemers, contractanten en Subverwerkers voor zover dit van toepassing is op de omvang van hun taken, waaronder ervoor zorgen dat alle personen die gemachtigd zijn tot toegang tot Persoonsgegevens van Klant zich verplicht hebben tot het vertrouwelijk behandelen hiervan, of een passende wettelijke geheimhoudingsverplichting hebben.
- 7.1.3 **Veiligheidshulp van Google.** Klant stemt ermee in dat Google (rekening houdend met de aard van de verwerking van Persoonsgegevens van Klant en de informatie waarover Google beschikt) Klant helpt om te zorgen dat voldaan wordt aan verplichtingen van Klant met betrekking tot de beveiliging van persoonsgegevens en inbreuk op de beveiliging van persoonsgegevens, met inbegrip van (indien van toepassing) de verplichtingen van Klant uit hoofde van artikel 32 tot en met 34 van de AVG, door:

- (a) de Beveiligingsmaatregelen te implementeren en te behouden overeenkomstig art 7.1.1 (Beveiligingsmaatregelen van Google);
- (b) te voldoen aan de bepalingen van artikel 7.2 (Data-incidenten); en
- (c) Klant de Beveiligingsdocumentatie overeenkomstig artikel 7.5.1 (Beoordelingen van Beveiligingsdocumentatie) en de informatie die opgenomen is in deze Voorwaarden voor Gegevensverwerking te verstrekken.

7.2 **Data-incidenten.**

- 7.2.1 **Kennisgeving van een incident.** Als Google kennis neemt van een Data-incident, gaat Google over tot: (a) Klant onverwijld en zonder vertraging in kennis stellen van het Data-incident (b) onverwijld redelijke maatregelen nemen om de schade zoveel mogelijk te beperken en de Persoonsgegevens van Klant veilig te stellen.
- 7.2.2 **Details van een Data-incident.** Kennisgevingen die gedaan worden uit hoofde van artikel 7.2.1 (Kennisgeving van een incident) beschrijven, voor zover mogelijk, de details van het Data-incident, met inbegrip van maatregelen die genomen zijn om de potentiële risico's te beperken en maatregelen die Google Klant aanraadt te nemen om het Data-incident aan te pakken.
- 7.2.3 **Bezorging van de kennisgeving.** Google bezorgt de kennisgeving van een Data-incident op het E-mailadres voor kennisgevingen of, naar eigen goeddunken van Google (waaronder indien Klant geen E-mailadres voor kennisgevingen heeft verstrekt), door middel van andere directe communicatie (bijvoorbeeld een telefoongesprek of een persoonlijke ontmoeting). Klant is zelf verantwoordelijk voor het verstrekken van het E-mailadres voor kennisgevingen en om ervoor te zorgen dat het E-mailadres voor kennisgevingen actueel en geldig is.
- 7.2.4 **Kennisgevingen van derden.** Klant is zelf verantwoordelijk voor de naleving van wetgeving inzake melding van Data-incidenten die op Klant van toepassing is en het voldoen aan eventuele verplichtingen inzake kennisgeving aan derden in verband met een Data-incident.
- 7.2.5 **Geen erkenning van schuld door Google.** Kennisgeving van of

reactie op een Data-incident door Google uit hoofde van dit artikel 7.2 (Data-incidenten) wordt niet opgevat als een erkenning door Google van schuld of aansprakelijkheid met betrekking tot het Data-incident.

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

7.3.1 **Beveiligingsverantwoordelijkheden van Klant.** Klant gaat ermee akkoord dat, onverminderd de verplichtingen van Google uit hoofde van artikel 7.1 (Beveiligingsmaatregelen en hulp van Google) en 7.2 (Data-incidenten):

- (a) uitsluitend Klant verantwoordelijk is voor zijn gebruik van de Verwerkingsdiensten, met inbegrip van:
 - (i) op correcte wijze gebruik maken van de Verwerkingsdiensten om een beveiligingsniveau te garanderen dat passend is voor het risico met betrekking tot de Persoonsgegevens; en
 - (ii) de verificatiegegevens van accounts, systemen en apparaten te beveiligen die Klant gebruikt voor toegang tot de Verwerkingsdiensten; en
- (b) Google geen verplichting heeft om Persoonsgegevens van Klant te beschermen die Klant verkiest op te slaan of door te geven buiten de systemen van Google en zijn Subverwerkers.

7.3.2 **Beoordeling van de beveiliging door Klant.** Klant erkent en stemt ermee in dat (rekening houdend met de stand van de techniek, de kosten van implementatie en de aard, omvang, context en doeleinden van de verwerking van Persoonsgegevens van Klant, evenals met de risico's voor personen) de beveiligingsmaatregelen die door Google genomen en behouden worden, zoals omschreven in art. 7.1.1 (Beveiligingsmaatregelen van Google) een beschermingsniveau bieden dat passend is voor het risico met betrekking tot de Persoonsgegevens van Klant.

7.4 **Beveiligingscertificaat.** Om de Beveiligingsmaatregelen te evalueren en te zorgen voor een blijvende doeltreffendheid hiervan, zal Google de ISO 27001-certificering behouden.

7.5 **Beoordelingen en audits met betrekking tot naleving.**

7.5.1 **Beoordelingen van Beveiligingsdocumentatie.** Ten behoeve van het door Google aantonen van het voldoen aan zijn verplichtingen uit hoofde van deze Voorwaarden voor Gegevensverwerking, stelt Google de Beveiligingsdocumentatie ter beoordeling aan de Klant beschikbaar.

7.5.2 **Auditrechten van Klant.**

- (a) Google staat Klant of een door Klant aangewezen derde auditor toe om audits uit te voeren (met inbegrip van inspecties) om te controleren of Google voldoet aan zijn verplichtingen op grond van deze Voorwaarden voor Gegevensverwerking overeenkomstig artikel 7.5.3 (Aanvullende zakelijke voorwaarden voor audits). Google werkt mee aan dergelijke audits zoals beschreven in art. 7.4 (Beveiligingscertificaat) en dit artikel 7.5 (Beoordelingen en audits van naleving).
- (b) Klant kan ook een audits uitvoeren ter verificatie van de naleving door Google van zijn verplichtingen uit hoofde van deze Voorwaarden voor Gegevensverwerking door de beoordeling van het certificaat dat afgegeven is in het kader van de ISO 27001-certificering (waarin het resultaat van een door een derde partij auditor uitgevoerde audit wordt weergegeven).

7.5.3 **Aanvullende zakelijke voorwaarden voor audits.**

- (a) Klant verstuurt een verzoek voor een audit uit hoofde van art. 7.5.2(a) aan Google zoals beschreven in artikel 12.1 (Contact opnemen met Google).
- (b) Na ontvangst door Google van een verzoek uit hoofde van art. 7.5.3(a) overleggen en bepalen Google en Klant vooraf een redelijke begindatum, omvang en duur van, en beveiliging- en vertrouwelijkheidswaarborgen die van toepassing zijn op, een audit op grond van artikel 7.5.2(a).
- (c) Google kan een vergoeding in rekening brengen voor een audit op grond van artikel 7.5.2(a) (op basis van door Google redelijk gemaakte kosten). Google verstrekt Klant vóór een dergelijke audit nadere informatie over een eventuele van toepassing zijnde vergoeding, alsmede de basis voor de

berekening hiervan. Eventuele kosten die in rekening gebracht worden door een derde partij auditor die door Klant wordt aangewezen om een dergelijke audit uit te voeren komen voor rekening van Klant.

- (d) Google kan bezwaar maken tegen een derde partij auditor die door Klant wordt aangewezen om een audit uit hoofde van artikel 7.5.2(a) uit te voeren indien de auditor, naar de redelijke mening van Google, niet naar behoren gekwalificeerd of onafhankelijk is, een concurrent van Google is of anderszins kennelijk ongeschikt is. In geval van een dergelijk bezwaar van Google moet Klant een andere auditor aanwijzen of zelf de audit uitvoeren.
- (e) Geen enkele bepaling in deze Voorwaarden voor Gegevensverwerking verplicht Google tot bekendmaking aan Klant of zijn derde partij auditor, of tot toestaan van toegang door Klant of zijn derde auditor van:
 - (i) gegevens van een andere klant van een Google Entiteit;
 - (ii) boekhoudkundige of financiële gegevens van een Google Entiteit;
 - (iii) bedrijfsgeheimen van een Google Entiteit;
 - (iv) informatie die, naar de redelijke mening van Google; (A) de beveiliging van een systeem of bedrijfslocatie van een Google Entiteit in gevaar zou kunnen brengen; of (B) ertoe zou kunnen leiden dat een Google Entiteit zijn verplichtingen schendt op grond van de Europese Wetgeving inzake gegevensbescherming of zijn verplichtingen met betrekking tot beveiliging en/of privacy jegens Klant of een derde; of
 - (v) informatie waartoe Klant of zijn derde auditor toegang wil verkrijgen om een andere reden dan het te goeder trouw voldoen aan de verplichtingen van Klant uit hoofde van de Europese Wetgeving inzake gegevensbescherming.

8. Effectbeoordelingen en raadplegingen

Klant stemt ermee in dat Google (rekening houdend met de aard van de verwerking en de informatie waarover Google beschikt) Klant helpt om te zorgen dat voldaan wordt aan verplichtingen van Klant met betrekking tot gegevensbeschermingseffectbeoordelingen in verband en voorafgaande raadpleging, met inbegrip van (indien van toepassing) de verplichtingen van Klant uit hoofde van artikel 35 en 36 van de AVG, door:

- (a) het verstrekken van de Beveiligingsdocumentatie in overeenstemming met artikel 7.5.1 (Beoordelingen van Beveiligingsdocumentatie);
- (b) het verstrekken van de informatie die opgenomen is in deze Voorwaarden voor Gegevensverwerking; en
- (c) het verstrekken of anders beschikbaar stellen, in overeenstemming met de standaardprocedures van Google, van ander materiaal betreffende de aard van de Verwerkingsdiensten en de verwerking van Persoonsgegevens van Klant (bijvoorbeeld, materiaal van helpcenters).

9. Rechten van betrokkenen

9.1 **Reacties op verzoeken van betrokkenen.** Wanneer Google een verzoek ontvangt van een betrokkene in verband met Persoonsgegevens van Klant, zal Google:

- (a) als het verzoek gedaan wordt via een Betrokkene-instrument, direct reageren op het verzoek van de betrokkene, in overeenstemming met de standaardfunctionaliteit van het Betrokkene-instrument; of
- (b) als het verzoek niet gedaan wordt via een Betrokkene-instrument, de betrokkene adviseren om zijn/haar verzoek in te dienen bij Klant, en is Klant verantwoordelijk voor het reageren op dit verzoek.

9.2 **Hulp van Google bij verzoeken van Betrokkenen.** Klant stemt ermee in dat Google (rekening houdend met de aard van de verwerking van de Persoonsgegevens van Klant en, indien van toepassing, artikel 11 van de AVG) Klant helpt bij het nakomen van eventuele verplichtingen van Klant om te

reageren op verzoeken van betrokkenen, met inbegrip van (indien van toepassing) de verplichting van Klant om te reageren op verzoeken voor de uitoefening van rechten van betrokkenen zoals vastgelegd in Hoofdstuk III van de AVG, door

- (a) het verstrekken van de functionaliteit van de Verwerkingsdiensten;
- (b) te voldoen aan de verplichtingen die beschreven zijn in artikel 9.1 (Reacties op verzoeken van betrokkenen); en
- (c) indien van toepassing op de Verwerkingsdiensten, Betrokkene-instrumenten beschikbaar te maken.

10. Gegevensdoorgifte

- 10.1 **Gegevensopslag en Verwerkingsfaciliteiten.** Klant stemt ermee in dat Google, behoudens artikel 10.2 (Doorgifte van gegevens), Persoonsgegevens van Klant kan opslaan en verwerken in de Verenigde Staten van Amerika en elk ander land waar Google of een van zijn Subverwerkers een bedrijfslocatie heeft.
- 10.2 **Doorgifte van gegevens.** Google zorgt ervoor dat;
 - (a) de moedermaatschappij van de Google-groep, Google LLC, op grond van Privacy Shield zelfcertificering behoudt; en
 - (b) de omvang van de certificering in het kader van Privacy Shield van Google LLC Persoonsgegevens van Klant omvat.
- 10.3 **Informatie over datacenters.** Informatie over de locaties van de datacenters van Google is beschikbaar op www.google.com/about/datacenters/inside/locations/index.html.

11. Subverwerkers

- 11.1 **Toestemming voor het inschakelen van Subverwerkers.** Klant verleent specifiek autorisatie voor het inschakelen van Google Aangeslotenen als Subverwerkers ("**Google Aangeslotenen Subverwerkers**"). Daarnaast verleent Klant algemene autorisatie voor het inschakelen van andere derden als Subverwerkers ("**Derden Subverwerkers**").
- 11.2 **Informatie over Subverwerkers.** Informatie over Subverwerkers is

beschikbaar op privacy.google.com/businesses/subprocessors.

11.3 **Vereisten voor het inschakelen van Subverwerkers.** Bij het inschakelen van een Subverwerker zal Google:

- (a) door middel van een schriftelijk contract waarborgen dat:
 - (i) de Subverwerker alleen toegang verschaft tot de Persoonsgegevens van Klant en deze alleen gebruikt voor zover nodig om de aan hem uitbestede verplichtingen uit te voeren, en dit doet in overeenstemming met de Overeenkomst (met inbegrip van deze Voorwaarden voor Gegevensbescherming) en Privacy Shield; en
 - (ii) indien de AVG van toepassing is op de verwerking van Persoonsgegevens van Klant, de verplichtingen inzake gegevensbescherming die omschreven zijn in artikel 28(3) van de AVG worden opgelegd aan de Subverwerker; en
- (b) volledig aansprakelijk blijven voor alle verplichtingen die uitbesteed worden aan, en alle handelingen en nalatigheden van, de Subverwerker.

11.4 **Mogelijkheid om bezwaar te maken tegen Verandering van Subverwerker.**

- (a) Indien tijdens de Looptijd een nieuwe Derde Subverwerker ingeschakeld wordt, stelt Google Klant, minstens 30 dagen voordat de nieuwe Subverwerker Persoonsgegevens van Klant verwerkt, op de hoogte van deze inschakeling (met inbegrip van de naam en locatie van de betreffende Subverwerker en de activiteiten die deze uit zal voeren) door het sturen van een e-mail aan het E-mailadres voor kennisgevingen.
- (b) Klant kan bezwaar maken tegen een nieuwe Derde Subverwerker door het onmiddellijk na schriftelijke kennisgeving aan Google beëindigen van de Overeenkomst, op voorwaarde dat Klant deze kennisgeving doet binnen 90 dagen nadat hij geïnformeerd is over de inschakeling van de nieuwe Derde Subverwerker zoals beschreven in artikel 11.4(a). Dit recht op beëindiging is het enige en uitputtende rechtsmiddel in het geval Klant bezwaar maakt tegen een nieuwe Derde Subverwerker.

12. Contact opnemen met Google; Register van verwerkingsactiviteiten

- 12.1 **Contact opnemen met Google.** Klant kan contact opnemen met Google met betrekking tot de uitoefening van zijn rechten uit hoofde van deze Voorwaarden voor Gegevensverwerking op privacy.google.com/businesses/processorsupport of via andere middelen die door Google van tijd tot tijd beschikbaar worden gesteld.
- 12.2 **Registers van verwerkingsactiviteiten van Google.** Klant erkent dat Google op grond van de AVG verplicht is om: (a) bepaalde informatie te verzamelen en hiervan registers bij te houden, waaronder de naam en contactgegevens van de verwerker en/of verwerkingsverantwoordelijke namens wie Google handelt, en (indien van toepassing) van de lokale vertegenwoordiger en de functionaris voor gegevensbescherming; en (b) deze informatie beschikbaar stellen aan enige Toezichthoudende Autoriteit. Dienovereenkomstig zal Klant, indien vereist en zoals van toepassing op Klant, deze informatie aan Google verstrekken via de gebruikersinterface van de Verwerkingsdiensten of via een ander middel dat door Google ter beschikking kan worden gesteld, en zal deze gebruikersinterface of dit andere middel gebruiken om ervoor te zorgen dat alle verstrekte informatie correct en actueel is.

13. Aansprakelijkheid

Indien de Overeenkomst beheerst wordt door het recht van:

- (a) een staat van de Verenigde Staten van Amerika, dan is de totale aansprakelijkheid van een van elk van beide partijen jegens de andere partij op grond van of in verband met deze Voorwaarden voor Gegevensverwerking, niettegenstaande een andere bepaling in de Overeenkomst, beperkt tot het maximale bedrag in geld of een op een betaling gebaseerd bedrag tot welk de aansprakelijkheid van de partij op grond van de Overeenkomst is gelimiteerd (voor de duidelijkheid: uitsluitingen van vrijwaringsclaims op de beperking van de aansprakelijkheid op grond van deze Overeenkomst zijn niet van toepassing op vrijwaringsclaims op grond van deze Overeenkomst die verband houden met Europese Wetgeving inzake gegevensbescherming of de

niet-Europese Wetgeving inzake gegevensbescherming); of

- (b) een rechtsgebied dat geen staat van de Verenigde Staten van Amerika is, dan is de aansprakelijkheid van de partijen op grond van of in verband met deze Voorwaarden voor Gegevensverwerking onderworpen aan de uitsluitingen en beperkingen van aansprakelijkheid in de Overeenkomst.

14. Effect van deze Voorwaarden voor Gegevensverwerking

In geval van tegenstrijdigheid of inconsistentie tussen de bepalingen van de Aanvullende Voorwaarden voor niet-Europese Wetgeving inzake gegevensbescherming, de rest van deze Voorwaarden voor Gegevensverwerking en/of de rest van de Overeenkomst, dan geldt de volgende rangorde (a) de Aanvullende Voorwaarden voor niet-Europese Wetgeving inzake gegevensbescherming; (b) de rest van deze Voorwaarden voor Gegevensverwerking; en (c) de rest van de Overeenkomst. Behoudens de in deze Voorwaarden voor Gegevensverwerking aangebrachte wijzigingen, blijft de Overeenkomst volledig van kracht en in werking.

15. Wijzigingen in deze Voorwaarden voor Gegevensverwerking

15.1 **Wijzigingen in URL's.** Google kan van tijd tot tijd een URL en de inhoud van deze URL waarnaar in deze Voorwaarden voor Gegevensverwerking wordt verwezen wijzigen. Google kan de lijst van potentiële Verwerkingsdiensten op privacy.google.com/businesses/adsservices alleen wijzigen om:

- (a) uiting te geven aan een wijziging in de naam van een dienst;
- (b) een nieuwe dienst toe te voegen; of
- (c) een dienst te verwijderen indien: (i) alle contracten voor het verlenen van die dienst beëindigd zijn; of (ii) Google toestemming van Klant heeft.

15.2 **Wijzigingen in de Voorwaarden voor Gegevensverwerking.** Google kan deze Voorwaarden voor Gegevensverwerking wijzigen indien de wijziging:

- (a) door deze Voorwaarden voor Gegevensverwerking uitdrukkelijk is toegestaan, met inbegrip van zoals beschreven in artikel 15.1 (Wijzigingen in URL's);
- (b) uiting geeft aan een wijziging in de naam of de vorm van een rechtspersoon;
- (c) vereist is om te voldoen aan door een regelgevende overheidsinstantie of -agentschap uitgevaardigde toepasselijke wetgeving, toepasselijke regelgeving, een gerechtelijk bevel of een richtsnoer; of
- (d) niet (i) leidt tot een verslechtering van de algehele beveiliging van de Verwerkingsdiensten; (ii) het toepassingsgebied uitbreidt van, of beperkingen verwijderd op, (x) in het geval van de Aanvullende Voorwaarden voor Niet-Europese Wetgeving inzake gegevensbescherming, het recht van Google om de gegevens te gebruiken of anderszins te verwerken binnen het toepassingsbereik van de Aanvullende Voorwaarden voor Niet-Europese Wetgeving inzake gegevensbescherming of (y) in het geval van de rest van de Voorwaarden voor Gegevensverwerking, de verwerking door Google van Persoonsgegevens van Klant, zoals beschreven in artikel 5.3 (Voldoen aan Instructies door Google); en (iii) anderszins een aanzienlijke negatieve invloed heeft op de rechten van Klant uit hoofde van deze Voorwaarden voor Gegevensverwerking, zoals door Google redelijkerwijs bepaald.

15.3 **Kennisgeving van wijzigingen.** Wanneer Google deze Voorwaarden voor Gegevensverwerking wil wijzigen op grond van artikel 15.2(c) of (d), stelt Google Klant hiervan in kennis minstens 30 dagen (of een kortere periode zoals vereist kan zijn om te voldoen aan toepasselijke wetgeving, toepasselijke regelgeving, een gerechtelijk bevel of richtsnoeren uitgevaardigd door regelgevende overheidsinstanties of -agentschappen) vóór de wijziging van kracht wordt, door middel van: (a) het versturen van een e-mail naar het E-mailadres voor kennisgevingen; of (b) het attenderen van Klant via de gebruikersinterface voor de Verwerkingsdiensten. Indien Klant bezwaar maakt tegen een dergelijke wijziging, kan Klant de Overeenkomst beëindigen door middel van een schriftelijke kennisgeving aan Google binnen 90 dagen nadat hij door Google over de wijziging is geïnformeerd.

Bijlage 1: Onderwerp en details van Gegevensverwerking Onderwerp

Levering door Google van de Verwerkingsdiensten en daarmee samenhangende technische ondersteuning aan Klant.

Duur van de Verwerking

De Looptijd plus de periode vanaf het verstrijken van de Looptijd tot het wissen van alle Persoonsgegevens van Klant door Google in overeenstemming met deze Voorwaarden voor Gegevensverwerking.

Aard en doel van de Verwerking

Google verwerkt (met inbegrip van, zoals van toepassing op de Verwerkingsdiensten en de instructies die beschreven zijn in artikel 5.2 (Instructies van Klant), door het verzamelen, vastleggen, ordenen, structureren, opslaan, wijzigen, opvragen, gebruiken, openbaar maken, samenvoegen, wissen en vernietigen van Persoonsgegevens van Klant ten behoeve van het verstrekken van de Verwerkingsdiensten en daarmee samenhangende technische ondersteuning aan Klant in overeenstemming met deze Voorwaarden voor Gegevensverwerking.

Soorten Persoonsgegevens

Persoonsgegevens van Klant kunnen de soorten persoonsgegevens omvatten die beschreven worden op privacy.google.com/businesses/adsservices.

Categorieën betrokkenen

Persoonsgegevens van Klant hebben betrekking op de volgende categorieën betrokkenen:

- betrokkenen over wie Google persoonsgegevens verzamelt bij het leveren van de Verwerkingsdiensten; en/of
- Betrokkenen over wie persoonsgegevens aan Google worden doorgegeven in verband met de Verwerkingsdiensten door, op aanwijzing van, of namens Klant;

Afhankelijk van de aard van de Verwerkingsdiensten, kunnen deze betrokkenen personen omvatten: (a) tot wie online advertenties zijn or worden gericht; (b) die specifieke websites of applicaties bezocht hebben met betrekking waartoe Google de Verwerkingsdiensten levert; en/of (c) die klanten of gebruikers zijn van de producten of diensten van Klant.

Bijlage 2: Beveiligingsmaatregelen

Vanaf de Ingangsdatum van de Voorwaarden, implementeert en behoudt Google de Beveiligingsmaatregelen die beschreven zijn in deze Bijlage 2. Google kan deze Beveiligingsmaatregelen van tijd tot tijd bijwerken of wijzigen, op voorwaarde dat deze bijwerkingen en wijzigingen niet leiden tot de aantasting van de algemene veiligheid van de Verwerkingsdiensten.

1. Datacenter en netwerkbeveiliging

(a) **Datacenters.**

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

Redundantie. De infrastructuursystemen zijn ontworpen om zwakke punten ("single points of failure") te verwijderen en de impact van verwachte milieurisico's te minimaliseren. Om deze redundantie te realiseren wordt gebruik gemaakt van dubbele circuits, schakelaars, netwerken en andere noodzakelijke instrumenten. De Verwerkingsdiensten zijn ontwikkeld om

Google in staat te stellen om bepaalde vormen van preventief en correctief onderhoud zonder onderbreking te kunnen uitvoeren. Alle milieubescherpende apparaten en faciliteiten hebben gedocumenteerde procedures voor preventief onderhoud waarin de procedure voor en frequentie van uitvoering worden beschreven in overeenstemming met de specificaties van de fabrikant of de interne specificaties. Preventief en correctief onderhoud van de datacenter-apparatuur wordt gepland door middel van een standaardprocedure in overeenstemming met gedocumenteerde procedures.

Stroom. De elektriciteitsvoorzieningen van de datacenters zijn ontworpen om redundant te zijn en onderhouden te kunnen worden zonder gevolgen voor continue processen, 24 uur per dag en 7 dagen per week. In de meeste gevallen hebben onderdelen van kritieke infrastructuur in een datacenter een primaire en een alternatieve stroombron, elk met hetzelfde vermogen. Noodstroom wordt verschaft door verschillende mechanismen, zoals noodstroomvoorziening (UPS)-accu's, die een altijd betrouwbare stroombeveiliging verschaffen tijdens spanningsdalingen van nutsvoorzieningen, overspanning, onderspanning en omstandigheden waarbij frequenties de tolerantiegrenzen overschrijden. In het geval de netstroom uitvalt, zorgt een reserve energievoorziening voor tijdelijke stroomvoorziening aan het datacenter, op volledige capaciteit, gedurende maximaal 10 minuten totdat de dieselgeneratoren de stroomvoorziening overnemen. Deze dieselgeneratoren kunnen binnen een aantal seconden opstarten om genoeg noodstroom te leveren om het datacenter op volledige capaciteit te laten werken, meestal voor een periode van een aantal dagen.

Serverbesturingssystemen. Servers van Google maken gebruik van geharde besturingssystemen die zijn aangepast aan de unieke serverbehoeften van het bedrijf. Gegevens worden met behulp van bedrijfseigen algoritmen opgeslagen om de beveiliging en redundantie van gegevens te vergroten. Google maakt gebruik van een procedure voor code review om de veiligheid te verhogen van de code die gebruikt wordt om de Verwerkingsdiensten te leveren en de beveiligingsproducten in productie-omgevingen te verbeteren.

Bedrijfscontinuïteit Google repliceert gegevens in meerdere systemen ten behoeve van beveiliging tegen onvoorziene vernietiging of onvoorzien verlies. Google heeft bedrijfscontinuïteitsplanning/programma's voor herstel na een noodgeval ontwikkeld en plant en test deze regelmatig.

(b) **Netwerken en overdracht.**

Gegevensoverdracht. Datacenters zijn meestal verbonden via particuliere snelle verbindingen om te zorgen voor een veilige en snelle gegevensoverdracht tussen datacenters. Dit is ontwikkeld om te voorkomen dat gegevens tijdens elektronische uitwisseling of doorgifte of tijdens registratie op dataopslagmedia zonder toestemming kunnen worden gelezen, gekopieerd, gewijzigd of verwijderd. Google verzendt gegevens via standaardprotocollen voor Internet.

Risico op aanvallen van buitenaf. Google maakt gebruik van meerder lagen van netwerkapparaten en inbraakdetectie ter bescherming van zijn risico op externe aanvallen. Google houdt rekening met potentiële aanvalsvectoren en integreert passende speciaal ontwikkelde technologieën in naar buiten gerichte systemen.

Inbraakdetectie. Inbraakdetectie is bedoeld om inzicht te verschaffen in actuele aanvalsactiviteiten en voldoende informatie te verschaffen om te reageren op incidenten. De inbraakdetectie van Google omvat:

1. Strenge controle van de omvang en samenstelling van het aanvalsrisico van Google door middel van preventieve maatregelen;
2. Gebruik van intelligente detectiecontroles op de ingangspunten van gegevens; en
3. Gebruik van technologieën die automatisch bepaalde gevaarlijke situaties verhelpen.

Incident response. Google controleert een scala aan communicatiekanalen op beveiligingsincidenten, en de beveiligingsmedewerkers van Google reageren snel op incidenten.

Encryptietechnologieën. Google stelt HTTPS-codering (ook wel SSL- of TLS-verbinding) beschikbaar. Google-servers ondersteunen efemere elliptische curve Diffie-Hellman-uitwisseling voor cryptografische sleutels ondertekend met RSA en ECDSA. Deze perfect forward secrecy (PFS) methoden helpen verkeer te beschermen en minimaliseren de gevolgen van een ontcijferde sleutel of een cryptografische doorbraak.

2. Toegang en controle van bedrijfslocaties

(a) **Controles van bedrijfslocaties.**

Beveiliging ter plaatse van datacenters. De datacenters van Google beschikken over beveiliging ter plaatse die 24 uur per dag, 7 dagen per week verantwoordelijk is voor alle fysieke beveiligingswerkzaamheden voor het datacenter. Het beveiligingspersoneel van het datacenter controleren Closed Circuit TV (“CCTV”)-camera's en alarmsystemen. Het beveiligingspersoneel van het datacenter voert regelmatig interne en externe patrouilles uit in en rond het datacenter.

Procedures voor toegang tot datacenters. Google beschikt over formele toegangsprocedures voor het toestaan van fysieke toegang tot de datacenters. De datacenters zijn gevestigd in gebouwen waartoe middels een elektronische sleutelpas toegang moet worden verkregen, met een alarm dat gekoppeld is aan de ter plaatse aanwezige beveiliging. Alle personen die het datacenter binnengaan moeten zich identificeren en een identiteitsbewijs tonen aan het beveiligingspersoneel. Alleen geverifieerde medewerkers, contractanten en bezoekers mogen de datacenters binnengaan. Alleen geverifieerde medewerkers en contractanten mogen verzoeken om toegang tot deze gebouwen middels een elektronische sleutelpas. Verzoeken om toegang tot een datacenter middels een elektronisch sleutelpas moeten vooraf schriftelijk gedaan worden, en voor het verstrekken van een sleutelpas moet toestemming worden gegeven door de manager van de verzoeker en de dagelijkse leiding van het datacenter. Alle andere bezoekers die tijdelijke toegang tot het datacenter willen moeten: (i) vooraf toestemming ontvangen van de managers van het datacenter voor het specifieke datacenter en de ruimten hierbinnen die ze willen bezoeken; (ii) zich aanmelden bij de beveiliging; (iii) een goedgekeurd document voor toegang tot het datacenter laten zien waarin aan de persoon toegang verleend wordt.

Beveiligingsinstallaties ter plaatse van datacenters. De datacenters van Google beschikken over een systeem van elektronische sleutelpassen en biometrische toegangscontrole dat gekoppeld is aan een alarmsysteem. Het systeem voor toegangscontrole controleert en registreert de elektronische sleutelpas van elke persoon wanneer deze binnenkomt door de hoofdingang, bij de expeditieafdeling of andere kritieke plaatsen. Ongeoorloofde activiteiten en mislukte toegangspogingen worden door het systeem voor toegangscontrole geregistreerd en zo nodig onderzocht. Ongeoorloofde toegang tot de zakelijke activiteiten en datacenters is beperkt, en gebaseerd op zones en de functietaken van de persoon. De branddeuren van de datacenters zijn uitgerust met een alarm. CCTV-camera's zijn zowel binnen

als buiten de datacenters ingeschakeld. De plaatsing van de camera's is ontworpen om strategische gebieden te dekken, waaronder de hoofdingang, deuren tot het gebouw van het datacenter en expeditie. Beveiligingspersoneel beheert de controle en registratie van CCTV-beelden en de CCTV-regelapparatuur. De CCTV-apparatuur is door het hele datacenter heen met beveiligde kabels verbonden. Camera's registreren de locatie 24 uur per dag, 7 dagen per week door middel van digitale videorecorders. De bewakingsgegevens worden, op basis van activiteiten, bewaard gedurende ten minste 7 dagen.

(b) **Toegangscontrole.**

Beveiligingspersoneel infrastructuur. Google heeft en onderhoudt een veiligheidsbeleid voor zijn medewerkers, en veiligheidstraining maakt onderdeel uit van het opleidingspakket voor het personeel. Het beveiligingspersoneel infrastructuur van Google is verantwoordelijk voor de voortdurende bewaking van de beveiligingsinfrastructuur van Google, de beoordeling van de Verwerkingsdiensten en het reageren op beveiligingsincidenten.

Toegangscontrole en privilegebeheer. Om gebruik te kunnen maken van de Verwerkingsdiensten, moeten beheerders en gebruikers van Klant zich verifiëren door middel van een centraal verificatiesysteem of via een eenmalige aanmelding op het systeem.

Interne procedures en beleid voor toegang tot gegevens – Toegangsbeleid.

De interne procedures van Google voor toegang tot gegevens zijn ontwikkeld om te voorkomen dat onbevoegde personen en/of systemen toegang verkrijgen tot systemen die gebruikt worden om persoonsgegevens te verwerken. Google streeft ernaar systemen te ontwerpen die: (i) alleen bevoegde personen toegang verlenen tot gegevens waarvoor hen toegang verleend is; en (ii) ervoor zorgen dat persoonsgegevens tijdens verwerking, gebruik en na registratie niet zonder toestemming gelezen, gekopieerd, gewijzigd of verwijderd kunnen worden. De systemen zijn ontworpen om alle ongeoorloofde toegang te detecteren. Google maakt gebruik van een gecentraliseerd systeem voor toegangscontrole om toegang van personeel tot productieservers te controleren, en verleent alleen toegang aan een beperkt aantal geautoriseerde medewerkers. LDAP, Kerberos en een eigen systeem dat gebruik maakt van SSH-certificaten zijn bedoeld om Google veilige en flexibele toegangsmechanismen te verschaffen. Deze mechanismen zijn ontworpen om alleen goedgekeurde toegangsrechten te verlenen aan website hosts, logs, gegevens en configuratiegegevens. Google

vereist het gebruik van unieke ID's, sterke wachtwoorden, tweeledige verificatiemethoden en zorgvuldig gecontroleerde toegangslijsten om de kans op ongeoorloofd gebruik van accounts te minimaliseren. De toekenning of wijziging van toegangsrechten is gebaseerd op: de functieverantwoordelijkheden van de geautoriseerde persoon; de functietaken die nodig zijn om de geautoriseerde taken uit te voeren; en op basis van "need-to-know". De toekenning of wijziging van toegangsrechten moet tevens in overeenstemming zijn met het beleid van Google inzake interne gegevenstoegang en training. Goedkeuringen worden beheerd met hulpprogramma's voor workflows die controlerapporten van alle wijzigingen bijhouden. Toegang tot systemen wordt geregistreerd zodat in het geval van een verantwoordingsplicht een audittrail beschikbaar is. Indien wachtwoorden gebruikt worden voor verificatie (bv. inloggen op werkstations), is wachtwoordbeleid ingevoerd dat ten minste voldoet aan de standaardprocedures van de sector. Deze standaardprocedures omvatten beperkingen op hergebruik van wachtwoorden en voldoende sterke wachtwoorden.

3. Gegevens

(a) **Opslag, isolatie en verificatie van gegevens.**

Google slaat gegevens op in multi-cliënt omgevingen op servers die het eigendom zijn van Google. Gegevens, de database en de architectuur van het bestandssysteem worden tussen meerdere geografisch verspreide datacenters gerepliceerd. Google zorgt voor logische isolatie van de gegevens van elke klant. In alle Verwerkingsdiensten wordt gebruik gemaakt van een centraal verificatiesysteem om de uniformiteit van de gegevensbeveiliging te verbeteren.

(b) **Afgedankte schijven en richtsnoeren voor schijfvernietiging..**

Op bepaalde schijven die gegevens bevatten kunnen zich prestatieproblemen, fouten of hardwarefouten voordoen waardoor ze afgedankt worden ("**Afgedankte schijf**"). Elke Afgedankte schijf wordt onderworpen aan een reeks van processen voor gegevensvernietiging (de "**Richtsnoeren voor gegevensvernietiging**") voordat de schijf de bedrijfslocatie van Google verlaat voor hergebruik of vernietiging. Afgedankte schijven worden gewist door middel van een uit meerdere stappen bestaand proces dat door minstens twee onafhankelijke validatoren als voltooid gevalideerd wordt. De wisresultaten worden ten behoeve van tracerings

geregistreerd met het serienummer van de schijf. Tenslotte wordt de gewiste Afgedankte schijven vrijgegeven aan voorraadbeheer voor hergebruik en herplaatsing. Indien de Afgedankte schijf door een hardwarefout niet gewist kan worden, wordt de schijf veilig opgeslagen totdat hij kan worden vernietigd. Elke faciliteit wordt regelmatig gecontroleerd op naleving van de Richtsnoeren voor gegevensvernietiging.

4. Beveiliging met betrekking tot het personeel

Personeel van Google dient zich te gedragen op een wijze die strookt met de richtsnoeren van het bedrijf met betrekking tot vertrouwelijkheid, bedrijfsethiek, passend gebruik en professionele normen. Google voert naar redelijkheid passende antecedentenonderzoeken uit, voor zover wettelijk toegestaan en overeenkomstig het toepasselijke lokale arbeidsrecht en wettelijke regelingen.

Personeel is verplicht een geheimhoudingsovereenkomst te ondertekenen, en moet ontvangst en naleving van Google's beleid inzake vertrouwelijkheid en privacy bevestigen. Personeel ontvangt veiligheidstrainingen. Personeel dat Persoonsgegevens van Klanten behandelt moet voldoen aan aanvullende, bij hun functie passende vereisten. Het personeel van Google verwerkt niet zonder toestemming Persoonsgegevens van Klanten.

5. Beveiliging met betrekking tot Subverwerkers

Voordat Subverwerkers te contracteren, voert Google een controle uit van het beleid inzake beveiliging en privacy van Subverwerkers, om ervoor te zorgen dat Subverwerkers een niveau van beveiliging en privacy bieden dat past bij hun toegang tot gegevens en de reikwijdte van de door hen uit te voeren diensten. Zodra Google het door de Subverwerker gevormde risico beoordeeld heeft, moet de Subverwerker, altijd behoudens de vereisten die beschreven zijn in artikel 11.3 (Vereisten voor het inschakelen van Subverwerkers), akkoord gaan met passende contractuele voorwaarden voor beveiliging, vertrouwelijkheid en privacy.

Bijlage 3: Aanvullende Voorwaarden voor Niet-Europese Wetgeving inzake gegevensbescherming

De volgende Aanvullende Voorwaarden voor Niet-Europese Wetgeving inzake gegevensbescherming vormen een aanvulling op deze Voorwaarden voor Verwerkingsverantwoordelijken:

- CCPA Service Provider Addendum via privacy.google.com/businesses/processorterms/ccpa (datum 1 januari 2020)

Google Ads Voorwaarden voor Gegevensverwerking, Versie 1.4

1 januari 2020

Eerdere versies

- [31 oktober 2019](#)
- [12 oktober 2017](#)