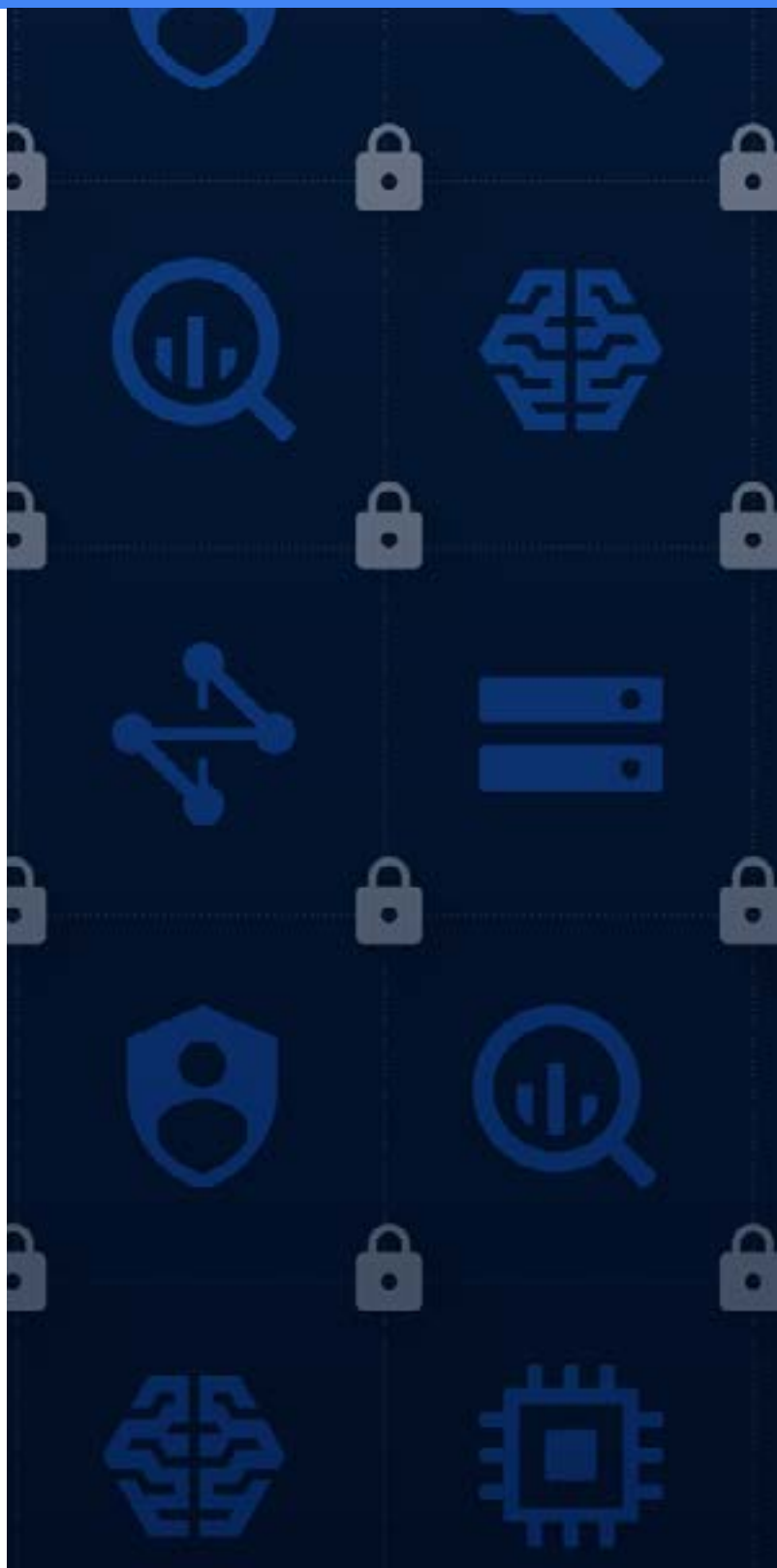
Google Cloud

Google Cloud en de algemene verordening gegevensbescherming (GDPR)



INTRO

Algemene verordening gegevensbescherming (General Data Protection Regulation, GDPR)

Op 25 mei 2018 treedt de belangrijkste Europese wetgeving inzake gegevensbescherming sinds 20 jaar in werking. De EU General Data Protection Regulation (GDPR) vervangt de 1995 EU Data Protection Directive. De GDPR versterkt de rechten van particulieren met betrekking tot hun persoonlijke gegevens en streeft naar het bundelen van de Europese wetten ter bescherming van gegevens, ongeacht waar de gegevens worden verwerkt.

U kunt erop vertrouwen dat Google alles in het werk stelt om voor alle Google Cloud-services te voldoen aan de vereisten van de GDPR. We helpen onze klanten ook bij de naleving van de nieuwe regelgeving met behulp van de uitgebreide privacy- en beveiligingsbescherming die we in de loop der jaren hebben ingebouwd in onze services en contracten.

WAT U KUNT DOEN

Wat zijn uw verantwoordelijkheden als klant?

Klanten van G Suite[1] en Google Cloud Platform treden doorgaans op als beheerder van de persoonlijke gegevens die ze aan Google verstrekken voor het gebruik van de services van Google. De gegevensbeheerder bepaalt de doeleinden en middelen voor de verwerking persoonlijke gegevens, terwijl de gegevensverwerker de gegevens namens deze beheerder verwerkt. Google is een gegevensverwerker en verwerkt persoonlijke gegevens namens de gegevensbeheerder wanneer de beheerder G Suite of Google Cloud Platform gebruikt.

Gegevensbeheerders zijn verantwoordelijk voor het nemen van de technische en organisatorische maatregelen die nodig zijn om de gegevensverwerking aantoonbaar uit te voeren in overeenstemming met de GDPR. De verplichtingen van beheerders hebben betrekking op principes zoals rechtmatigheid, redelijkheid en transparantie, doelbinding, gegevensminimalisering en nauwkeurigheid, evenals het nakomen van de rechten van betrokkenen, ook wel 'datasubjecten' genoemd.

Als u gegevensbeheerder bent, kunt op de hoogte blijven van uw verantwoordelijkheden onder de GDPR door regelmatig de website van uw nationale of, indien van toepassing, primaire instantie voor gegevensbescherming onder de GDPR te bezoeken[2], en door publicaties van organisaties zoals de **Internationale organisatie van privacyprofessionals (IAPP) te raadplegen.**

Vraag ook onafhankelijk advies over uw status en verplichtingen onder de GDPR aan een jurist. Alleen een jurist kan specifiek advies over uw situatie geven. De informatie op deze website mag niet worden opgevat als juridisch advies of als vervanging van juridisch advies.

Waar moet u beginnen?

Als huidige of toekomstige klant van Google Cloud is dit het juiste moment om u voor te bereiden op de GDPR. Hier volgen een aantal tips:

- Maak uzelf vertrouwd met de bepalingen van de **GDPR**, in het bijzonder de verschillen met uw huidige verplichtingen op het gebied van gegevensbescherming.
- Maak een actueel overzicht van de persoonlijke gegevens die u beheert. Onze tools kunnen u helpen bij het identificeren en classificeren van gegevens.
- Controleer of uw huidige beheeropties, beleid en processen voldoen aan de vereisten van de GDPR. Maak een plan om eventuele hiaten te dichten.
- Kijk hoe u de bestaande gegevensbeschermingsfuncties van Google Cloud kunt inpassen in uw eigen kader voor de naleving van wetten en regels. Evalueer de G Suite- en Google Cloud Platform-materialen voor audits en certificeringen om te zien hoe deze u kunnen helpen.
- Controleer regelmatig of de regelgevingsadviezen zijn geüpdatet en vraag een advocaat om specifiek juridisch advies voor uw bedrijf.

1 G Suite omvat G Suite for Business en G Suite for Education.

2 We raden u aan onafhankelijk juridisch advies in te winnen om te bepalen wat voor u de nationale of primaire instantie voor gegevensbescherming is.

WAT WE DOEN

Verplichtingen van G Suite en Google Cloud Platform volgens de GDPR

Gegevensbeheerders zijn onder meer verplicht uitsluitend gegevensverwerkers te gebruiken die voldoende waarborgen bieden dat er adequate technische en organisatorische maatregelen worden genomen om de verwerking te laten voldoen aan de vereisten van de GDPR. Hieronder volgen enkele aspecten die u in overweging kunt nemen bij het evalueren van de G Suite- en Google Cloud Platform-services.

VAKKENNIS, BETROUWBAARHEID EN MIDDELEN

Expertise op het gebied van gegevensbeveiliging

Google heeft beveiligings- en privacyprofessionals in dienst, waaronder een aantal wereldwijd toonaangevende deskundigen op het gebied van informatie-, app- en netwerkbeveiliging. Dit team heeft als taak de verdedigingssystemen van het bedrijf te onderhouden, processen voor beveiligingscontrole te ontwikkelen, de beveiligingsinfrastructuur op te bouwen en het beveiligingsbeleid van Google te implementeren.
Google heeft ook een groot aantal advocaten, experts op het gebied van naleving van regelgeving en specialisten op het gebied van overheidsbeleid in dienst, die zorgen dat Google de privacy- en beveiligingswetten naleeft.
Deze teams geven samen met klanten, stakeholders uit de sector en toezichthoudende autoriteiten vorm aan onze ***G Suite- en Google Cloud Platform-services****, zodat klanten aan hun wettelijke verplichtingen kunnen voldoen.*

VERPLICHTINGEN OP HET GEBIED VAN GEGEVENSBESCHERMING

Overeenkomsten voor gegevensverwerking

In onze overeenkomsten voor gegevensverwerking voor G Suite en Google Cloud Platform staan onze privacyverplichtingen aan klanten duidelijk vermeld. We hebben deze voorwaarden in de loop der jaren aangepast op basis van feedback van onze klanten en toezichthouders. We hebben deze voorwaarden recentelijk specifiek geüpdatet op basis van de GDPR. We hebben deze geüpdatete voorwaarden beschikbaar gemaakt ruim voordat de GDPR in werking treedt, zodat klanten die gebruikmaken van Google Cloud-services beter kunnen beoordelen of ze aan de GDPR voldoen en zich beter kunnen voorbereiden. Onze klanten kunnen deze geüpdatete voorwaarden voor gegevensverwerking nu aangaan via het aanmeldproces dat is beschreven hier voor het Amendement gegevensverwerking voor G Suite en hier voor de Voorwaarden voor gegevensverwerking en -beveiliging voor GCP. De geüpdatete voorwaarden gaan op 25 mei 2018 in, de dag waarop de GDPR in werking treedt.

Verwerking volgens instructies

De gegevens die klanten of hun gebruikers in onze systemen plaatsen, worden alleen verwerkt in overeenstemming met de instructies van de klant, zoals beschreven in onze huidige en onze voor de GDPR geüpdatete overeenkomsten voor gegevensverwerking.

Vertrouwelijkheidsverplichtingen van medewerkers

Alle medewerkers van Google zijn verplicht een vertrouwelijkheidsovereenkomst te ondertekenen. Ook volgen ze verplichte trainingen op het gebied van vertrouwelijkheid en privacy, evenals onze ***Gedragscode****-training. De Gedragscode van Google gaat specifiek in op verantwoordelijkheden en verwacht gedrag met betrekking tot de bescherming van informatie.*

GEBRUIK VAN SUBVERWERKERS

Ondernemingen binnen de Google Group verwerken de meeste gegevens die nodig zijn om de G Suite- en Google Cloud Platform-services te leveren. Daarnaast werken we met externe leveranciers die deze services ondersteunen. Alle leveranciers ondergaan een strenge selectieprocedure, zodat we zeker weten dat ze de vereiste technische expertise hebben en het juiste niveau van beveiliging en privacy kunnen bieden. We verstrekken informatie over subverwerkers van de Google Group die G Suite en Google Cloud Platform-services ondersteunen, evenals over externe subverwerkers die bij deze services betrokken zijn. Verplichtingen met betrekking tot subverwerkers zijn opgenomen in onze huidige en geüpdatete overeenkomsten voor gegevensverwerking.

BEVEILIGING VAN DE SERVICES

Volgens de GDPR moeten de beheerder en de verwerker voldoende technische en organisatorische maatregelen nemen om een veiligheidsniveau te waarborgen dat is toegespitst op het risico.

Google gebruikt een wereldwijde infrastructuur die is ontworpen om de allermodernste beveiliging te leveren voor de volledige cyclus van de informatieverwerking. Deze infrastructuur staat borg voor de veiligheid bij de implementatie van services, de opslag van gegevens met privacymaatregelen voor eindgebruikers, de communicatie tussen services, de privécommunicatie met klanten via internet en de exploitatie door beheerders. G Suite en Google Cloud Platform maken gebruik van deze infrastructuur.

We hebben de beveiliging van onze infrastructuur in lagen opgebouwd, van de fysieke beveiliging van de datacenters tot de beveiligingsmaatregelen voor onze hardware en software en de processen die we gebruiken om de operationele beveiliging te ondersteunen. Deze gelaagde bescherming zorgt voor een sterke beveiligingsbasis voor alles wat we doen. Gedetailleerde informatie over onze infrastructuurbeveiliging vindt u in onze whitepaper over het beveiligingsdesign van de Google-infrastructuur.

Beschikbaarheid, integriteit en veerkracht

Bij het ontwerp van het platform zorgt Google ervoor dat de onderdelen bijzonder redundant zijn. Zo zijn de datacenters van Google geografisch gespreid. Bij natuurrampen of plaatselijke stroomuitval worden zo de gevolgen beperkt van regionale onderbrekingen in de levering van wereldwijde producten. Bij een hardware-, software- of netwerkfout worden de services automatisch omgeschakeld naar een ander datacenter, zodat ze niet worden onderbroken. Dankzij deze zeer redundante infrastructuur zijn klanten beter beschermd tegen gegevensverlies.

Testen

Google voert jaarlijks rampersteltesten uit en beschikt over een platform voor infrastructuur- en app-teams. Zo kunnen communicatieplannen, storingsscenario's, operationele transities en andere noodmaatregelen worden getest. Alle teams die deelnemen aan deze rampersteloefeningen, ontwikkelen testplannen en evaluatierapporten waarin de resultaten en de geleerde lessen van de testen worden bijgehouden.

Versleuteling

Google maakt gebruik van versleuteling om gegevens te beschermen die in transit zijn of op een server staan. Gegevens die in transit zijn naar G Suite, worden beschermd met HTTPS. Dit is standaard geactiveerd voor alle gebruikers. De G Suite- en Google Cloud Platform-services versleutelen de content van klanten automatisch met een of meer mechanismen. Een uitgebreide beschrijving van deze gegevensversleuteling vindt u in onze **whitepaper over versleuteling.**

Toegangsbeheer

De toegangsrechten en -niveaus van Google-medewerkers zijn gebaseerd op hun functie en rol. Hierbij gaan we uit van minimale rechten en beperkte informatieverstrekking. Zo zorgen we ervoor dat de toegangsrechten overeenkomen met de gedefinieerde verantwoordelijkheden. Voor aanvullende toegang moet een formele procedure worden gevolgd en moet toestemming worden gevraagd aan en gegeven door een gegevens- of systeemeigenaar, manager of andere leidinggevende, zoals voorgeschreven door het beveiligingsbeleid van Google.

Kwetsbaarheidsbeheer

We scannen onze software op kwetsbaarheden. Hiervoor gebruiken we commercieel verkrijgbare tools, tools die we zelf voor dit doel hebben ontwikkeld, intensieve geautomatiseerde en handmatige inbraaktesten, kwaliteitsgarantieprocessen, softwarebeveiligingscontroles en externe audits. We vertrouwen ook op de community van mensen die onderzoek doen naar beveiliging en maken dankbaar gebruik van hun hulp bij het identificeren van kwetsbaarheden in G Suite, Google Cloud Platform en andere Google-producten. Ons Vulnerability Reward Program moedigt onderzoekers aan om ontwerp- en implementatieproblemen te melden die een risico voor klantgegevens kunnen vormen.

Productbeveiliging: G Suite

G Suite-klanten kunnen productfuncties en -configuraties gebruiken om persoonlijke gegevens nog beter te beschermen tegen ongeoorloofde of onwettige verwerking:

- *Authenticatie in twee stappen verlaagt het risico op ongeoorloofde toegang aanzienlijk door gebruikers tijdens het inloggen te vragen om een tweede bewijs van identiteit. Afgedwongen beveiligingssleutels vormen een extra beveiligingslaag voor gebruikersaccounts door een fysieke sleutel te vereisen.*
- *Controle op verdachte inlogpogingen helpt bij het opsporen van verdachte inlogpogingen op basis van geavanceerde machine learning.*
- *Verbeterde e-mailbeveiliging vereist dat e-mailberichten worden ondertekend en versleuteld met Secure/Multipurpose Internet Mail Extensions (S/MIME).*
- *Gegevensverlies voorkomen beschermt gevoelige informatie in Gmail en Drive tegen ongeoorloofd delen. Meer informatie vindt u in onze Whitepaper over DLP.*
- *Informatierechtenbeheerin Drive geeft u de mogelijkheid om via het geavanceerde deelmenu het downloaden, afdrukken en kopiëren van bestanden uit te schakelen en vervaldatums in te stellen voor bestandstoegang.*
- *Beheer van mobiele apparaten biedt continue systeemcontrole en geeft een waarschuwing bij verdachte apparaatactiviteit.*

Ga voor meer informatie naar diese webseite

Productbeveiliging: GCP

GCP-klanten kunnen productfuncties en -configuraties gebruiken om hun persoonlijke gegevens nog beter te beschermen tegen ongeoorloofde of onwettige verwerking:

- *Authenticatie in twee stappen verlaagt het risico van ongeoorloofde toegang aanzienlijk door gebruikers tijdens het aanmelden om een tweede bewijs van identiteit te vragen. Afgedwongen beveiligingssleutels bieden een extra beveiligingslaag voor gebruikersaccounts door een fysieke sleutel te vereisen.*
- *Identiteits- en toegangsbeheer in Google Cloud (Cloud Identity and Access Management, Cloud IAM) geeft u de mogelijkheid gedetailleerde toegangs- en wijzigingsrechten in te stellen en te beheren voor Google Cloud Platform-resources.*
- *De Data Loss Prevention API helpt u bij de identificatie en controle van de verwerking van speciale categorieën persoonlijke gegevens. Zo kun u adequate controlemechanismen implementeren.*
- *Stackdriver Logging en Stackdriver Monitoring zorgen ervoor dat systemen voor logboekregistratie, controle, waarschuwingen en detectie van afwijkingen worden geïntegreerd in Google Cloud Platform.*
- *Cloud Identity-Aware Proxy (Cloud IAP) beheert de toegang tot cloud-apps die op Google Cloud Platform worden uitgevoerd.*
- *Cloud Security Scanner spoort veelvoorkomende kwetsbaarheden op in Google App Engine-apps.*

Ga voor meer informatie naar diese webseite

GEGEVENS RETOURNEREN EN VERWIJDEREN

*Beheerders kunnen de gehele looptijd van de overeenkomst op elk gewenst moment klantgegevens exporteren met de functionaliteit van de G Suite- of Google Cloud Platform-services. Deze garantie is al enkele jaren opgenomen in onze voorwaarden voor gegevensverwerking en we blijven deze ook bieden nadat de GDPR in werking is getreden. Verder werken we continu aan verbetering van de gegevensexportfuncties van de G Suite services en de Google Cloud Platform-services (zie de **Google Cloud Platform-documentatie** voor meer informatie).*

Met de functionaliteit van de G Suite- of Google Cloud Platform-services kunt u ook op elk gewenst moment klantgegevens verwijderen. Als Google een volledige verwijderingsinstructie van u ontvangt (bijvoorbeeld wanneer u een verwijderde e-mail niet meer kunt terughalen uit de 'prullenbak'), verwijdert Google de betreffende klantgegevens binnen maximaal 180 dagen uit alle systemen, tenzij er bewaarverplichtingen van toepassing zijn.

HULP VOOR DE BEHEERDER

Rechten van betrokkenen

Gegevensbeheerders maken het met de beheerconsoles en de servicefunctionaliteit van G Suite en Google Cloud Platform mogelijk dat de gegevens die zij en hun gebruikers in onze systemen hebben gezet, worden gebruikt, gerectificeerd en verwijderd, en dat hun verwerking wordt beperkt. Met deze functionaliteit kunnen ze voldoen aan de verplichting om te reageren op verzoeken van betrokkenen die hun rechten onder de GDPR willen uitoefenen.

Team voor gegevensbescherming

Klanten van G Suite en Google Cloud Platform kunnen met hun vragen over gegevensbescherming terecht bij een gespecialiseerd team.

Incidentmeldingen

Voor G Suite en Google Cloud Platform gelden al jaren contractuele verplichtingen wat betreft incidentmeldingen. Wij blijven u zo snel mogelijk informeren over incidenten met uw klantgegevens, op grond van de voorwaarden inzake gegevensincidenten in onze huidige overeenkomsten en de geüpdatete voorwaarden die gelden vanaf 25 mei 2018, de dag waarop de GDPR in werking treedt.

INTERNATIONALE GEGEVENSOVERDRACHT

De GDPR biedt verschillende mechanismen om de overdracht van persoonlijke gegevens buiten de EU te vergemakkelijken. Deze mechanismen zijn bedoeld als waarborg voor een adequaat beschermingsniveau en voor de implementatie van voldoende beveiligingsmaatregelen bij de overdracht van gegevens naar een ander land. Modelcontractclausules kunnen voorzien in passende veiligheidsmaatregelen. Een adequaat beschermingsniveau kan worden bevestigd door middel van adequaatheidsbeslissingen. Denk hierbij aan beslissingen die de Europees-Amerikaans Privacy Shields ondersteunen.

Onder onze huidige voorwaarden voor gegevensverwerking verplichten we ons contractueel tot de handhaving van een mechanisme dat de overdracht van persoonlijke gegevens buiten de EU vergemakkelijkt, zoals vereist in de Gegevensbeschermingsrichtlijn. We gaan verder een overeenkomstige verplichting aan vanaf 25 mei 2018, de dag waarop de GDPR in werking treedt.

De certificering van Google onder het Europees-Amerikaans en Zwitsers-Amerikaans Privacy Shield-principe ***geldt ook voor G Suite en Google Cloud Platform****. Verder hebben de Europese instanties voor gegevensbescherming bevestigd dat onze modelcontractclausules en onze huidige contractuele verplichtingen voor G Suite en Google Cloud Platform volledig voldoen aan de vereisten van de Gegevensbeschermingsrichtlijn om de overdracht van persoonlijke gegevens van de EU naar de rest van de wereld juridisch vorm te geven.*

STANDAARDEN EN CERTIFICERINGEN

Onze klanten en toezichthouders verwachten een onafhankelijke controle van de maatregelen op het gebied van beveiliging, privacy en naleving. G Suite en Google Cloud Platform worden regelmatig door verschillende onafhankelijke externe partijen gecontroleerd om dit te waarborgen.

ISO 27001 (Information Security Management) ISO 27001 is een van de meest erkende, internationaal geaccepteerde onafhankelijke veiligheidsnormen. Google heeft een ISO 27001-certificering behaald voor de systemen, apps, medewerkers, technologie, processen en datacenters waaruit onze gedeelde gemeenschappelijke infrastructuur bestaat, maar ook voor de G Suite- en Google Cloud Platform-producten.

ISO 27017 (Cloud Security) ISO 27017 is een internationale praktijknorm voor informatiebeveiligingsfuncties van cloudservices, gebaseerd op ISO/IEC 27002. Google is gecertificeerd conform ISO 27017 voor G Suite en Google Cloud Platform.

ISO 27018 (Cloud Privacy) ISO 27018 is een internationale praktijknorm voor de bescherming van persoonlijk identificeerbare informatie (PII) in openbare cloudservices. Google is conform ISO 27018 gecertificeerd voor G Suite en Google Cloud Platform.

SSAE16 / ISAE 3402 (SOC 2/3) Het auditframework van het American Institute of Certified Public Accountants (AICPA) voor SOC 2- en SOC 3 (Service Organization Controls) definieert vertrouwensprincipes en criteria voor beveiliging, beschikbaarheid, verwerkingsintegriteit en vertrouwelijkheid. Google heeft zowel SOC 2- als SOC 3-rapporten voor Google Cloud Platform en G Suite.

VEELGESTELDE VRAGEN

" WAT IS DE GDPR? "

De Algemene verordening gegevensbescherming is een nieuwe privacywet van de EU die de Richtlijn 95/46/EG betreffende gegevensbescherming van 24 oktober 1995 zal vervangen.

" WANNEER TREEDT DE GDPR IN WERKING? "

De GDPR is vanaf 25 mei 2018 rechtstreeks van toepassing in alle lidstaten van de Europese Unie.

" VEREIST DE GDPR DAT PERSOONLIJKE GEGEVENS WORDEN OPGESLAGEN IN DE EU? "

Nee. Net als de Richtlijn 95/46/EG betreffende gegevensbescherming bevat de GDPR bepaalde voorwaarden voor de overdracht van persoonlijke gegevens buiten de EU. Aan dergelijke voorwaarden kan worden voldaan via mechanismen zoals modelcontractclausules.

" GEEFT DE GDPR KLANTEN HET RECHT OM GOOGLE CLOUD TE CONTROLEREN? "

Volgens de GDPR moeten gegevensbeheerders auditrechten krijgen op grond van hun contracten met gegevensverwerkers. In de geüpdatete overeenkomsten voor gegevensverwerking (aangeboden vanaf 15 mei 2018, de ingangsdatum van de GDPR) worden daarom auditrechten toegekend aan onze klanten.

" WELKE ROL HEBBEN EXTERNE RAPPORTEN ZOALS ISO 27001, ISO 27017, ISO 27018 EN SOC 2/3 IN RELATIE TOT DE GDPR? "

Onze externe ISO-certificeringen en SOC 2/3-auditrapporten kunnen door klanten worden gebruikt om risicoanalyses uit te voeren en vast te stellen of de juiste technische en organisatorische maatregelen zijn genomen.

" WELKE ANDERE INFORMATIE HEEFT GOOGLE OVER DE GDPR VERSTREKT? "

Raadpleeg **Google-website 'Bedrijven en gegevens'.**