# TECHNISCHE EN ORGANISATORISCHE MAATREGELEN VOOR GOTOASSIST CORPORATE

**CONTROLEMECHANISMEN VOOR BEVEILIGING EN PRIVACY**

**Publicatiedatum: Februari 2022**

# 1 Producten en services

Dit document bevat de Technische en Organisatorische Maatregelen (TOM's) voor GoToAssist Corporate, een gehoste service waarmee supportteams live technische ondersteuning op afstand kunnen bieden aan zakelijke gebruikers van zowel Windows als Mac. GoToAssist Corporate is aanpasbaar aan de unieke omgeving van een bedrijf en beschikt over geavanceerde administratieve en samenwerkingsfunctionaliteit, waaronder functies voor klantwachtrijen, teamsamenwerking, sessieoverdracht, klantenenquêtes en sessie-opname.

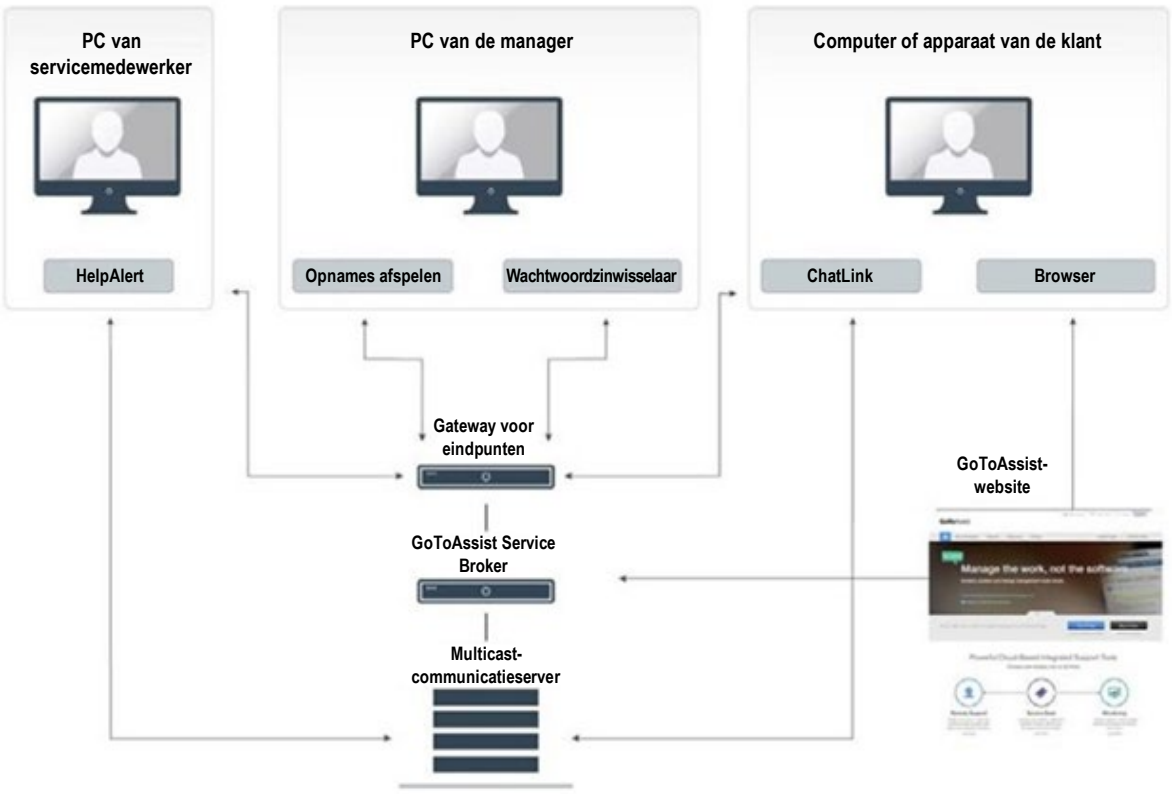
# 2 Productarchitectuur

GoToAssist Corporate maakt gebruik van een ASP-model (Application Service Provider) dat ontworpen is om veilige services te bieden die geïntegreerd kunnen worden in de bestaande netwerk- en beveiligingsinfrastructuur van een bedrijf. De architectuur is ontworpen met het oog op prestaties, betrouwbaarheid en schaalbaarheid. Er zijn redundante switches en routers ingebouwd in de architectuur, waarmee deze vrijwel volledig storingsvrij is. Het systeem is voorzien van geclusterde servers en back-upsystemen met hoge capaciteit, om applicatieprocessen te kunnen blijven uitvoeren in het geval van een zware belasting of systeemstoring. Servicebrokers verdelen daarnaast de belasting van de client/server-sessies over geografisch verspreide communicatieservers om optimale prestaties te kunnen garanderen.

De web-, toepassings-, communicatie- en databaseservers zijn ondergebracht in beveiligde co-locatiedatacenters met redundante stroomvoorziening en omgevingsbesturing. De fysieke toegang tot de servers is nauw afgebakend en wordt continu gecontroleerd. Toegangscontroles op basis van firewalls, routers en VPN's worden gebruikt om onze privéservicenetwerken en backendservers te beveiligen. De beveiliging van de infrastructuur wordt continu gemonitord en er worden op gezette tijden kwetsbaarheidstests uitgevoerd door zowel intern personeel als externe auditors.

# 3 Technische beveiligingsmaatregelen van GoToAssist Corporate

GoTo maakt gebruik van technische besturingselementen voor beveiliging die voldoen aan de industriestandaard, en die geschikt zijn voor de aard en het bereik van de services (zoals deze term wordt gedefinieerd in de Servicevoorwaarden). Ze zijn ontworpen om de infrastructuur van de service en de gegevens die zich daarin bevinden optimaal te beschermen. U vindt de Servicevoorwaarden op https://www.goto.com/company/legal/terms-and-conditions.




**GoToAssist-website** – Online toepassing die toegang biedt tot de website van GoToAssist en webgebaseerde interne en externe beheerportalen. De websites worden gehost in Tier-1-colocatiedatacenters.

**GoToAssist Service Broker** – Online toepassing voor het account- en servicebeheer van GoToAssist Corporate, die tevens permanente opslag en rapportagefuncties biedt. Brokers worden gehost in Tier 1-colocatiedatacenters.

**Gateway voor eindpunten (Endpoint Gateway (EGW))** – Een speciale gateway die door verschillende eindpunttoepassingen en voor verschillende doeleinden wordt gebruikt om veilig toegang te krijgen tot de GoToAssist Service Broker, met behulp van procedure-aanroepen op afstand. EGW wordt gehost op Amazon Web Services.

**Multicast-communicatieservers (MCS)** – Een vloot van wereldwijd gedistribueerde servers die worden gebruikt om een verscheidenheid aan unicast- en multicast-communicatieservices met hoge beschikbaarheid te kunnen realiseren. Multicast-communicatieservers worden gehost in Tier 1-colocatiedatacenters.

## 3.1. Logische toegangscontrole

Er zijn logische besturingselementen voor toegang geïmplementeerd, ingericht om ongeautoriseerde toegang tot toepassingen en gegevensverlies in bedrijfs- en productieomgevingen te voorkomen of te beperken. Medewerkers krijgen minimale toegang (met slechts zoveel rechten als nodig zijn) tot specifieke GoTo-systemen, toepassingen, netwerken en apparaten. Verder worden gebruikersrechten gescheiden op basis van functionele rol en omgeving.

Gebruikers aan wie toegang wordt verleend tot onderdelen van GoToAssist Corporate zijn onder meer medewerkers van GoTo (zoals van de teams Technische Operaties en Technische Ontwikkeling), beheerders van klanten, of eindgebruikers van het product. De productieservers op locatie zijn alleen beschikbaar vanaf jumphosts of via Ops VPN en beide worden beschermd door meervoudige verificatie (MFA). Cloudgebaseerde productiecomponenten zijn beschikbaar via verificatie met SSU (Self Service Unix).

## 3.2. Perimeterbescherming en inbraakdetectie

GoTo heeft tools, technieken en services voor perimeterbescherming geïmplementeerd, ingericht om te voorkomen dat onbevoegd netwerkverkeer de productinfrastructuur binnendringt. Het GoTo-netwerk is voorzien van externe firewalls en interne netwerksegmentatie. Cloudbronnen maken ook gebruik van hostgebaseerde firewalls. Daarnaast wordt een cloudgebaseerde DDoS-preventieservice (Distributed Denial of Service) van derden gebruikt ter bescherming tegen volumetrische DDoS-aanvallen; deze service wordt minstens één keer per jaar getest. Kritieke systeembestanden zijn beschermd tegen kwaadwillige aanvallen en onbedoelde blootstelling of vernietiging.

## 3.3. Scheiding van gegevens

GoTo maakt gebruik van een architectuur met meerdere tenants, logisch gescheiden op databaseniveau, en gebaseerd op de GoTo-account van de organisatie. Alleen geverifieerde partijen krijgen toegang tot accounts.

## 3.4. Fysieke beveiliging

GoTo werkt samen met datacenters om de fysieke beveiliging te waarborgen van serverruimtes waar productieservers staan. Deze beveiligingsmaatregelen omvatten:

- Videobewaking en -opname
- Meervoudige verificatie voor zeer gevoelige ruimtes
- Temperatuurregeling met verwarming, ventilatie en airconditioning
- Brandbestrijding en rookmelders
- Ononderbreekbare stroomvoorziening (UPS)
- Verhoogde vloeren of uitgebreid kabelbeheer
- Continue monitoring en waarschuwingen
- Bescherming tegen veel voorkomende natuurrampen en door de mens veroorzaakte rampen, zoals vereist afhankelijk van de locatie van het betreffende datacenter
- Gepland onderhoud en validatie van alle kritieke besturingselementen voor fysieke beveiliging.

GoTo beperkt fysieke toegang tot productiedatacenters tot bevoegde personen. Voor toegang tot een fysieke serverruimte of hostingfaciliteit van een derde partij moet een verzoek worden ingediend via een ticketingsysteem. Vervolgens moet de aanvraag worden goedgekeurd door de betreffende manager, en worden beoordeeld en goedgekeurd door het team Technische Operaties. Het GoTo-management controleert minstens elk kwartaal de logbestanden ten aanzien van de fysieke toegang tot datacenters en serverruimtes. Daarnaast verliest eerder geautoriseerd personeel bij ontslag direct het recht op fysieke toegang tot de datacenters.

## 3.5. Back-up van gegevens, noodherstel en beschikbaarheid

De architectuur van GoTo is ontworpen om replicatie bijna in realtime uit te voeren naar geografisch verschillende locaties. Back-ups van databases worden gemaakt met behulp van incrementele back-ups. In het geval van een ramp of een totale uitval van een site op een van de actieve locaties, zijn de resterende locaties ingericht om de belasting van de applicatie in evenwicht te houden. De noodherstelprocedure met betrekking tot het systeem wordt periodiek getest.

## 3.6. Bescherming tegen malware

Op alle GoToAssist Corporate-servers wordt malwarebeschermingssoftware met auditlogbestanden geïnstalleerd. Meldingen die duiden op mogelijke kwaadwillige activiteiten worden doorgestuurd naar het passende responsteam.

## 3.7. Versleuteling

GoTo houdt zich aan een cryptografische standaard die overeenkomt met aanbevelingen van brancheverenigingen, overheidspublicaties en andere erkende normgroepen. De cryptografische standaard wordt periodiek herzien en gebruikte technologieën en vercijferingen kunnen worden bijgewerkt in overeenstemming met het ingeschatte risico en de marktacceptatie van nieuwe standaarden.

De versleuteling die wordt gebruikt in GoToAssist Corporate is gebaseerd op:

- Op openbare sleutels gebaseerde verificatie van het SRP-protocol (Secure Remote Password) voor verificatie en sleutelvorming tussen eindpunten
- 128-bits AES-codering om de sessiegegevens te beveiligen
- Door eindpunten gegenereerde sessiesleutels die nooit bekend zijn bij de GoTo-medewerkers, noch in de systemen van GoTo zijn opgeslagen
- Communicatieservers die alleen versleutelde pakketten routeren en niet beschikken over de encryptiesleutel van de sessie

### 3.7.1. Versleuteling tijdens de overdracht

Om de Klantcontent tijdens de overdracht nog beter te beschermen, gebruikt GoTo de laatste Transport Layer Security (TLS)-protocollen en bijbehorende vercijferingen om meerdere internetprotocollen te kunnen beveiligen. Daarnaast gebruikt GoTo de nieuwste versie van Secure Shell (SSH) voor bepaalde beheerfuncties. De verbinding met interne netwerken wordt beschermd met geschikte VPN-technologieën (Virtual Private Network), die bedoeld zijn om de vertrouwelijkheid en integriteit van het interne verkeer van GoTo te garanderen.

#### Beveiligingsfuncties voor communicatie

Communicatie tussen deelnemers in een sessie van GoToAssist Corporate verloopt via een multicast-overlay-netwerkstack die logisch is gepositioneerd boven de conventionele TCP/IP-stack in de computers van alle gebruikers. Dit netwerk wordt geleverd door een verzameling van multicast-communicatieservers (MCS).

## Vertrouwelijkheid en integriteit van communicatie

GoToAssist Corporate treft maatregelen voor gegevensbeveiliging ter bescherming tegen passieve en actieve aanvallen op vertrouwelijkheid, integriteit en beschikbaarheid. Gegevens voor schermdeling, gegevens over toetsenbord- en muisbediening en chatinformatie zijn te allen tijde versleuteld terwijl deze zich tijdelijk op communicatieservers bevinden of via openbare of particuliere netwerken worden verzonden.

Als opname is uitgeschakeld, wordt de sessiesleutel van GoToAssist Corporate in geen enkele vorm naar de servers gestuurd. Zo zou bijvoorbeeld een inbraak op een server niet de sleutel onthullen voor een versleutelde stream die een kwaadwillende onderschept. Als opname is ingeschakeld, worden chat-, schermdelings- en schermweergavegegevens in versleutelde vorm opgeslagen. De sessiesleutel wordt ook opgeslagen, maar deze wordt beschermd met 1024-bits RSA-versleuteling met persoonlijk-openbaar sleutelpaar. Een portaalspecifieke openbare sleutel en een aanpasbare wachtwoordzin worden gebruikt om de sessiesleutel te versleutelen voordat deze wordt opgeslagen. Als maatregel om sessiegegevens te beveiligen, is voor sessieherhalingen het volgende vereist: toegang tot de sessieopname, de versleutelde sessiesleutel, en de persoonlijke sleutel van de portal plus de wachtwoordzin. In zowel de TCP-laag als de beveiligingslaag voor multicastpakketten (Multicast Packet Security Layer, MPSL) zijn besturingselementen voor communicatiebeveiliging geïmplementeerd, op basis van sterke cryptografie.

## Beveiliging TCP-laag

De conform de IETF-standaard (Internet Engineering Task Force) ingerichte TLS-protocollen worden gebruikt om de communicatie tussen eindpunten te beschermen.

Voor de bescherming van klanten zelf adviseert GoTo dat zij hun browser zo te configureren dat er standaard waar mogelijk gebruik wordt gemaakt van sterke cryptografie, en dat zij altijd het meest recente besturingssysteem en de laatste beveiligingspatches voor hun browser installeren.

Wanneer TLS-verbindingen tot stand worden gebracht met de website en tussen onderdelen van GoToAssist Corporate, verifiëren de GoTo-servers zich bij clients met behulp van openbare-sleutelcertificaten. Voor extra beveiliging tegen aanvallen op de infrastructuur, wordt wederzijdse verificatie op basis van certificaten gebruikt voor alle verbindingen tussen servers onderling (bijvoorbeeld MCS-naar-MCS of MCS-naar-broker).

## Beveiligingslaag voor multicastpakketten

Extra functies voegen nog een encryptielaag toe voor gegevens van toetsenbord- en muisbesturing en tekstberichten, naast de TLS-beveiliging. Alle sessiegegevens zijn hierdoor beveiligd met versleuteling en integriteitsbeveiligingen. Dit voorkomt dat mensen met toegang tot onze communicatieservers (al dan niet geoorloofd) kunnen meeluisteren met een sessie of ongemerkt gegevens kunnen aanpassen.

De sleutels worden gegenereerd op basis van een willekeurige 128-bits beginwaarde die wordt gekozen door GoToAssist Corporate-servicebroker. Deze waarde wordt per TLS verdeeld over alle eindpunten en gebruikt als input voor een sleutelafleider met NIST-goedkeuring. Wanneer de sessie wordt beëindigd, wordt de basiswaarde uit het geheugen van de GoToAssist Corporate-servicebroker gewist.

Sessiegegevens worden daarnaast beschermd tegen afluisteren met een 128-bits AES-versleuteling in countermodus. Gegevens in leesbare tekst worden standaard gecomprimeerd voorafgaand aan de versleuteling. Hiervoor wordt eigen, krachtige technologie ingezet om bandbreedte te optimaliseren. Voor de bescherming van de gegevensintegriteit wordt momenteel een controlewaarde gegenereerd met het HMAC-SHA-1-algoritme. Omdat er consequent sterke encryptietechnologieën worden toegepast, kunnen klanten erop vertrouwen dat hun sessiegegevens beschermd zijn tegen ongeoorloofde openbaarmaking of onopgemerkte aanpassingen.

Bovendien brengen deze essentiële functies voor communicatiebeveiliging geen extra kosten, verminderde prestaties of problemen op het gebied van de bruikbaarheid met zich mee. Hoogwaardige gegevensbescherming op basis van erkende standaarden is een ingebouwde functie in elke sessie.

### 3.8. Beheersing van kwetsbaarheden

Maandelijks worden systemen en netwerken gescand op interne en externe kwetsbaarheden. Er worden daarnaast ook periodiek dynamische en statische tests uitgevoerd op de kwetsbaarheid van applicaties, evenals penetratietests voor getroffen omgevingen. Deze scan- en testresultaten worden gerapporteerd in netwerkbewakingstools en waar nodig en afhankelijk van de ernst van de geïdentificeerde kwetsbaarheden worden herstelmaatregelen getroffen.

Kwetsbaarheden worden ook gecommuniceerd en beheerst met maand- en kwartaalrapporten voor zowel de ontwikkelingsteams als het management.

### 3.9. Rapporteren en waarschuwen

GoTo verzamelt geïdentificeerd afwijkend of verdacht verkeer in de relevante beveiligingslogbestanden van de betreffende productiesystemen.

## 4 Organisatorische besturingselementen

GoTo biedt een uitgebreide reeks organisatorische en administratieve controlemechanismen om de beveiliging en privacy van GoToAssist Corporate te beschermen.

### 4.1. Beveiligingsbeleid en -procedures

GoTo heeft een uitgebreid beveiligingsbeleid, met beleidsregels en procedures die zijn afgestemd op bedrijfsdoelen, nalevingsprogramma's en algemeen verantwoord zakelijk bestuur. Deze beleidsregels en procedures worden periodiek herzien en waar nodig bijgewerkt om de voortdurende naleving ervan te garanderen.

### 4.2. Naleving van normen

GoTo voldoet aan de van toepassing zijnde wettelijke, financiële, gegevensprivacy- en regelgevende vereisten, en houdt zich aan de volgende certificeringen en externe auditrapporten:

- TRUSTe-certificaat inzake privacy en best practices voor gegevensbeheer voor ondernemingen, voor de operationele besturingselementen voor privacy- en gegevensbescherming die zijn afgestemd op de belangrijkste privacywetten en erkende privacyraamwerken. Raadpleeg voor meer informatie onze blogpost hierover.

- Attestatierapport Service Organization Control (SOC) 2 Type 2 van het American Institute of Certified Public Accountants (AICPA).
- Compliance met de Payment Card Industry Data Security Standard (PCI DSS) voor de e-commerce- en betalingsomgevingen van GoTo
- Beoordeling van interne besturingselementen zoals vereist in het kader van de controle van de jaarrekeningen door de Public Company Accounting Oversight Board (PCAOB)

## 4.3. Het Security Operations Center en incidentbeheer

Het Security Operations Center (SOC) van GoTo wordt beheerd door het Team Beveiligingsoperaties, dat verantwoordelijk is voor het detecteren van en reageren op beveiligingsgebeurtenissen. Het SOC maakt gebruik van beveiligingssensoren en analysesystemen om potentiele problemen te identificeren, en heeft een gedocumenteerd Incidentenbestrijdingsplan om adequaat op incidenten te reageren.

Het Incidentenbestrijdingsplan is afgestemd op de kritieke communicatieprocessen van GoTo, het Beleidsreglement voor Incidentbeheer van Informatiebeveiliging, en de bijbehorende standaardwerkprocedures. Het is ontworpen om verdachte of geïdentificeerde beveiligingsgebeurtenissen in interne systemen en services als de GoToAssist Services te beheren, te identificeren en op te lossen. In het Incidentenbestrijdingsplan is vastgelegd dat er technisch personeel aanwezig moet zijn om mogelijke gebeurtenissen en kwetsbaarheden met betrekking tot informatiebeveiliging te identificeren, en vermoedelijke of bevestigde gebeurtenissen indien nodig naar het management te escaleren. Medewerkers kunnen beveiligingsincidenten melden via e-mail, telefoon en/of tickets, volgens het proces dat is gedocumenteerd op de GoTo-intranetsite. Alle geïdentificeerde of verdachte gebeurtenissen worden gedocumenteerd en geëscaleerd via gestandaardiseerde gebeurtenistickets, waarbij prioriteit wordt gegeven aan de meest alarmerende gebeurtenissen.

## 4.4. Beveiliging van toepassingen

Het applicatiebeveiligingsprogramma van GoTo is gebaseerd op de SDL (Security Development Lifecycle) van Microsoft om productcode te beveiligen. De kernelementen van dit programma zijn handmatige codebeoordelingen, bedreigingsmodellen, statische codeanalyse, dynamische analyse en systeemverharding.

## 4.5. Screening van personeel

Er worden vóór de datum van indiensttreding algemene achtergrondcontroles uitgevoerd ten aanzien van nieuwe werknemers, voor zover toegestaan door de toepasselijke wetgeving en passend bij de functie. De resultaten worden bijgehouden in het functiedossier van de medewerker. De criteria voor achtergrondcontroles variëren afhankelijk van de wetgeving, de functieverantwoordelijkheid en het leiderschapsniveau van de potentiële werknemer, en zijn onderhevig aan de gangbare en aanvaardbare best practices van het betreffende land.

## 4.6. Bewustzijns- en trainingsprogramma's over beveiliging

Nieuwe medewerkers worden tijdens de oriëntatie geïnformeerd over het beveiligingsbeleid en de Gedragscode en Bedrijfsethiek van GoTo. Deze verplichte jaarlijkse beveiligings- en privacytraining wordt gegeven aan relevant personeel en beheerd door het Team Talentontwikkeling met ondersteuning van het Beveiligingsteam.

Vaste en tijdelijke medewerkers van GoTo worden regelmatig geïnformeerd over richtlijnen, procedures, beleidsregels en normen op het gebied van beveiliging en privacy via verschillende mediakanalen. Dit zijn bijvoorbeeld onboardingkits voor nieuwe medewerkers, bewustmakingscampagnes, webinars met de CISO, een programma voor 'beveiligingskampioenen', en posters en ander materiaal dat minstens twee keer per jaar wordt uitgewisseld en waarop de methoden voor het beveiligen van gegevens, apparaten en faciliteiten worden geïllustreerd.

# 5 Privacy

GoTo neemt de privacy van zijn klanten, de abonnees van de GoTo-services en eindgebruikers zeer serieus, en zet zich in om relevante best practices voor gegevensverwerking en -beheer op een open en transparante manier bekend te maken.

## 5.1. AVG

De General Data Protection Regulation (GDPR), in het Nederlands de Algemene Verordening Gegevensbescherming (AVG), is de Europese wet om de privacy en gegevens van alle EU-ingezetenen te beschermen. De GDPR is voornamelijk bedoeld om burgers en ingezetenen controle te geven over hun persoonlijke gegevens en om het regelgevingskader EU-breed te vereenvoudigen. GoToAssist Corporate voldoet aan de toepasselijke bepalingen van de GDPR. Ga voor meer informatie naar https://www.goto.com/company/trust/privacy.

## 5.2. CCPA

GoTo verklaart en garandeert hierbij dat het voldoet aan de California Consumer Privacy Act (CCPA). Ga voor meer informatie naar https://www.goto.com/company/trust/privacy.

## 5.3. Gegevensbescherming en Privacybeleid

GoTo heeft een uitgebreid en wereldwijd geldend Addendum gegevensverwerking ('DPA'; Data Processing Addendum) opgesteld, beschikbaar in het Engels en het Duits, waarin de verwerking van persoonsgegevens door GoTo is geregeld, en die voldoet aan de eisen van de AVG en CCPA, en deze zelfs overstijgt.

Concreet zijn in de DPA verschillende AVG-gerichte beveiligingsmechanismen voor de gegevensprivacy verwerkt, waaronder: (a) details over gegevensverwerking, openbaarmaking aan een andere gegevensverwerkende partij, enzovoorts, zoals vereist onder Artikel 28; (b) Europese modelbepalingen (standaardbepalingen voor overeenkomsten); en (c) de technische en organisatorische maatregelen voor gegevensbeveiliging van GoTo. Om in te spelen op het van kracht worden van de CCPA hebben we onze wereldwijde DPA bijgewerkt om de volgende aspecten hierin op te nemen: (a) aangepaste definities die aansluiten bij de CCPA; (b) recht op toegang en verwijdering; en (c) garanties dat GoTo de persoonlijke gegevens van onze gebruikers niet zal verkopen.

Voor bezoekers van onze webpagina's maakt GoTo in zijn Privacybeleid op de openbare website bekend welke soorten informatie worden verzameld en gebruikt om de Services te leveren, te onderhouden, te verbeteren en te beveiligen. Het bedrijf kan van tijd tot tijd het Privacybeleid bijwerken om wijzigingen in de verwerking van informatie en/of wijzigingen in de toepasselijke wetgeving weer te geven, maar zal op haar website melding maken van eventuele materiële wijzigingen voordat een dergelijke wijziging van kracht wordt.

## 5.4. Overdrachtskaders

GoTo heeft een krachtig wereldwijd gegevensbeschermingsprogramma ingericht, dat rekening houdt met de toepasselijke wetgeving, en rechtmatige internationale overdrachten binnen de volgende kaders ondersteunt:

### 5.4.1. Standaardcontractbepalingen

De Standaardbepalingen ('SCC's'; Standard Contractual Clauses) zijn gestandaardiseerde contractbepalingen die zijn erkend en aangenomen door de Europese Commissie. Het hoofddoel van deze bepalingen is om ervoor te zorgen dat alle persoonsgegevens die de Europese Economische Ruimte ('EER') verlaten, worden overgedragen in overeenstemming met de Europese wetgeving voor gegevensbescherming. GoTo heeft geïnvesteerd in een privacyprogramma van wereldklasse om te voldoen aan de strenge vereisten van de SCC's voor de overdracht van persoonsgegevens. GoTo biedt zijn klanten SCC's, soms ook bekend als de Modelbepalingen van de EU, die specifieke garanties bevatten aangaande de overdracht van persoonsgegevens voor de relevante GoTo-services. Ze zijn onderdeel van de wereldwijde DPA. Naleving van de SCC's garandeert dat klanten van GoTo veilig vrijuit gegevens kunnen overdragen vanuit de EER naar de rest van de wereld.

#### Aanvullende maatregelen

Naast de maatregelen die in deze TOM's zijn gespecificeerd, heeft GoTo de navolgende Veelgestelde vragen en de antwoorden daarop verzameld, om GoTo's aanvullende maatregelen te schetsen die zijn getroffen om rechtmatige overdrachten, zoals bedoeld in hoofdstuk 5 van de AVG, te ondersteunen. Hiermee bieden we ook de mogelijkheid om case-by-case-analyses, die door het Europese Hof van Justitie worden aanbevolen in verband met de SCC's, te bespreken en te begeleiden.

### 5.4.2. Certificeringen voor de CBPR en PRP van de APEC

GoTo heeft ook de certificeringen van de Asia-Pacific Economic Cooperation ('APEC') voor de Cross-Border Privacy Rules ('CBPR') en de Privacy Recognition for Processors ('PRP'). De CBPR en de PRP van APEC zijn de eerste standaarden voor gegevensbeveiliging die zijn goedgekeurd voor de overdracht van persoonsgegevens tussen lidstaten van de APEC. De certificeringen zijn behaald en onafhankelijk gevalideerd door TrustArc, een externe leider op het gebied van naleving van gegevensbeveiliging die is goedgekeurd door de APEC.

## 5.5. Klantcontent retourneren en verwijderen

Klanten van GoToAssist Corporate kunnen te allen tijde om teruggave of verwijdering van hun Klantcontent vragen via gestandaardiseerde interfaces. Als deze interfaces niet beschikbaar zijn of als GoTo anderszins niet in staat is om een dergelijk verzoek in te willigen, zal GoTo een commercieel redelijke poging doen om de Klant, afhankelijk van de technische haalbaarheid, te helpen bij het ophalen of verwijderen van zijn Content. De Klantcontent zal binnen dertig (30) dagen na het verzoek van de Klant worden verwijderd. De Klantcontent in GoToAssist Corporate wordt automatisch binnen negentig (90) dagen na afloop of beëindiging van de laatste abonnementstermijn verwijderd. Op schriftelijk verzoek zal GoTo de verwijdering van dergelijke Content bevestigen.

## 5.6. Gevoelige gegevens

Hoewel GoTo ernaar streeft om alle Klantcontent te beschermen, zijn we door wettelijke en contractuele beperkingen genoodzaakt om het gebruik van GoToAssist Corporate voor bepaalde soorten informatie te beperken. Tenzij de Klant schriftelijke toestemming van GoTo heeft, mogen de volgende gegevens niet worden geüpload naar of gegenereerd in GoToAssist Corporate:

- Door de overheid uitgegeven identificatienummers en afbeeldingen van identificatiedocumenten.
- Informatie met betrekking tot de gezondheid van een persoon, inclusief maar niet beperkt tot Beschermde Gezondheidsinformatie (PHI; Protected Health Information), zoals geïdentificeerd in de Amerikaanse Health Insurance Portability and Accountability Act (HIPAA) en daaraan gerelateerde wet- en regelgeving.
- Informatie met betrekking tot financiële rekeningen en betaalinstrumenten, inclusief maar niet beperkt tot creditcardgegevens. De enige algemene uitzondering op deze bepaling betreft expliciet geïdentificeerde betalingsformulieren en -pagina's die door GoTo worden gebruikt om betalingen voor GoToAssist Corporate te innen.
- Alle informatie die speciaal beschermd wordt door toepasselijke wet- en regelgeving, in het bijzonder informatie over ras, etniciteit, religieuze of politieke overtuigingen, lidmaatschappen van organisaties, etc. van een individu.

## 5.7. Volgen en analyseren

GoTo verbetert zijn websites en producten voortdurend met behulp van webanalysetools van derden, waarmee GoTo inzichtelijk maakt hoe bezoekers zijn websites, desktopapplicaties en mobiele toepassingen gebruiken, en wat de voorkeuren en problemen van gebruikers zijn. Voor meer informatie verwijzen wij u naar het Privacybeleid.

# 6 Derde partijen

## 6.1. Gebruik van derde partijen

Als onderdeel van de interne beoordeling en processen met betrekking tot leveranciers en derde partijen, kunnen de evaluaties van leveranciers door meerdere teams worden uitgevoerd, afhankelijk van de relevantie en toepasbaarheid. Het Beveiligingsteam evalueert alle leveranciers die op informatiebeveiliging gebaseerde services leveren, en beoordeelt eveneens de hostingfaciliteiten van derde partijen. Juridische zaken en Inkoop kunnen contracten, werkomschrijvingen en serviceovereenkomsten evalueren, indien vereist volgens interne processen. Er worden indien nodig passende nalevingsdocumentatie of -rapporten verkregen die ten minste jaarlijks worden geëvalueerd, om ervoor te zorgen dat de controleomgeving adequaat functioneert en alle noodzakelijke controles op gebruikersoverwegingen worden uitgevoerd. Daarnaast moeten derde partijen die gevoelige of vertrouwelijke gegevens hosten of die toegangsmachtigingen krijgen van GoTo, een schriftelijk contract ondertekenen waarin de relevante vereisten voor toegang tot of opslag of behandeling van de informatie (zoals van toepassing) zijn opgenomen.

## 6.2. Best practices bij contractering

Om de bedrijfscontinuïteit te waarborgen en ervoor te zorgen dat er passende maatregelen worden getroffen om de vertrouwelijkheid en integriteit van bedrijfsprocessen en gegevensverwerking van derden te beschermen, beoordeelt GoTo allereerst de voorwaarden van relevante derde partijen. Vervolgens wordt beslist om ofwel GoTo's goedgekeurde inkoopsjablonen te gebruiken, ofwel om te onderhandelen over dergelijke voorwaarden van derden, indien dat nodig blijkt.

# 7 Contact opnemen met GoTo

Klanten kunnen contact opnemen met GoTo op https://support.goto.com voor algemene vragen of privacy@goto.com voor privacy-gerelateerde vragen.