TECHNISCHE EN ORGANISATORISCHE MAATREGELEN VOOR GOTO DIGITAL ENGAGEMENT

CONTROLEMECHANISMEN VOOR BEVEILIGING EN PRIVACY

Versie 2.0 | december 2023

Samenvatting

In dit document met Technische en Organisatorische Maatregelen ('TOM's') worden GoTo's privacy-, beveiligings- en verantwoordingsverplichtingen voor GoTo Contact uiteengezet. Specifiek heeft GoTo robuuste wereldwijde privacy- en beveiligingsprogramma's en organisatorische, administratieve en technische beveiligingen die ontworpen zijn om: (i) de vertrouwelijkheid, integriteit en beschikbaarheid van de Klantcontent te waarborgen; (ii) bescherming te bieden tegen bedreigingen en gevaren voor de veiligheid van de Klantcontent; (iii) bescherming te bieden tegen verlies, misbruik, ongeautoriseerde toegang, openbaarmaking, wijziging en vernietiging van Klantcontent; en (iv) naleving van de toepasselijke wet- en regelgeving te handhaven, waaronder wetgeving inzake gegevensbescherming en privacy. Dergelijke maatregelen omvatten:

- **Versleuteling:**
  - *Tijdens de overdracht:* Transport Layer Security (TLS) v1.2.
  - *Tijdens de opslag:* Advanced Encryption Standard (AES) 256-bits voor Klantcontent.
- **Datacenters:** Gevestigd in de Verenigde Staten, Brazilië, Duitsland, Australië, Singapore en het Verenigd Koninkrijk ter ondersteuning van redundantie en stabiliteit.
- **Fysieke beveiliging:** Er zijn besturingselementen voor fysieke beveiliging en omgevingen beschikbaar, die zijn ontworpen om fysieke toegang te beschermen, te controleren en te beperken voor systemen en servers die Klantcontent onderhouden, om te kunnen voldoen aan uptime-, prestatie- en schaalbaarheidsverplichtingen.
- **Nalevingsaudits:** GoTo Contact beschikt over SOC 2 Type II, SOC 3 Type 2, BSI C5, PCI DSS, PCAOB, TRUSTe-certificaat inzake privacy van ondernemingen en APEC-CBPR- en PRP-certificeringen.
- **Naleving van wet- en regelgeving:** GoTo heeft een uitgebreid gegevensbeschermingsprogramma met processen en beleidsregels die ervoor zorgen dat de Klantcontent wordt behandeld in overeenstemming met de toepasselijke privacywetgeving, waaronder de AVG, CCPA/CPRA en LGPD.
- **Beveiligingsbeoordelingen**: Naast interne tests sluit GoTo contracten af met externe bedrijven om regelmatig beveiligingsbeoordelingen en/of penetratietests uit te voeren.
- **Logische besturingselementen voor toegang:** Er zijn logische besturingselementen voor toegang geïmplementeerd, ingericht om ongeautoriseerde toegang tot toepassingen en gegevensverlies in bedrijfs- en productieomgevingen te voorkomen of te beperken.
- **Scheiding van gegevens**: GoTo maakt gebruik van een architectuur met meerdere tenants en scheidt klantaccounts logisch op databaseniveau.
- **Perimeterbescherming en inbraakdetectie**: Er zijn tools, technieken en diensten voor perimeterbescherming beschikbaar, ingericht om te voorkomen dat onbevoegd netwerkverkeer de productinfrastructuur binnendringt. Het GoTo-netwerk is voorzien van externe firewalls en interne netwerksegmentatie.
- **Bewaring van gegevens:**
  - GoTo Contact-klanten kunnen te allen tijde verzoeken om retournering of verwijdering van Klantcontent, waaraan binnen dertig (30) dagen na het verzoek van de klant zal worden voldaan.
  - Klantcontent wordt dertig (30) dagen na het verstrijken van de op dat moment laatst betaalde abonnementstermijn van een Klant automatisch verwijderd. Gedurende de abonnementstermijn worden gespreksopnamen en gespreksverslagen dertien (13) maanden bewaard vanaf de datum waarop ze zijn gemaakt.

1 Producten en services

GoTo Contact is een CCaaS-oplossing (Contact Center as a Service) die geïntegreerd is in het GoTo Connect-platform, waarmee organisaties de resultaten van hun communicatie met (potentiële) klanten via meerdere communicatiekanalen, zoals telefonisch keuzemenu's, tekstberichten, webchat en sociale media, kunnen verbeteren. Deze oplossing is geschikt voor organisaties van alle groottes, maar is in het bijzonder ingericht voor kleine tot middelgrote bedrijven.

In dit document worden de Technische en Organisatorische Maatregelen (TOM's) van GoTo Contact beschreven, evenals sommige van het in GoTo Contact geïntegreerde GoTo Connect-platform.

Hieronder volgen de bij de GoTo Contact-service inbegrepen functies en aanbiedingen (de 'Service'):

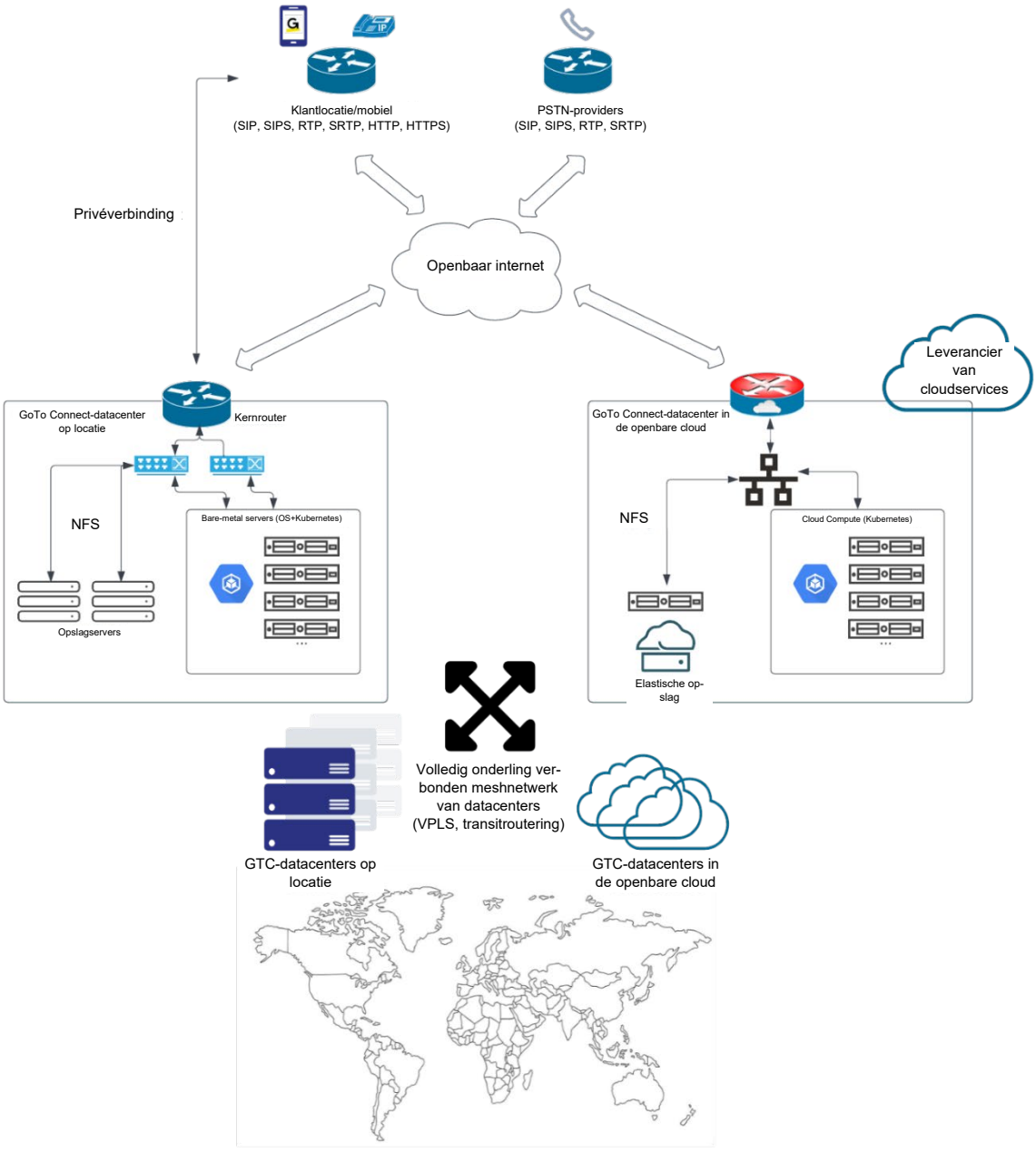
- Met GoTo Contact kunnen gebruikers wachtrijen en inkomende gesprekken van klanten beheren via interactieve voice responses, automatische gespreksdistributie en integraties met klantenrelatiebeheer.

- Chatwachtrijen zijn ingericht zodat mensen een bericht naar een wachtrij kunnen sturen, dat vervolgens wordt afgeleverd bij een vertegenwoordiger van het bedrijf, alsof het externe nummer het rechtstreekse nummer van de vertegenwoordiger is. Chatwachtrijberichten kunnen via verschillende communicatiekanalen worden verzonden: tekstbericht, webchat, Facebook-post en andere socialemediakanalen.

- Andere kanalen ter ondersteuning van communicatie met klanten zijn spraak-naar-video en chat-naar-video.

- De analyses van GoTo Contact hebben een realtime en historische rapportagefunctie waarmee supervisors en managers klantinteracties kunnen verbeteren, de klantervaring kunnen optimaliseren, de benodigde tijd van vertegenwoordigers om klanten te bedienen kunnen optimaliseren, en vertegenwoordigers kunnen coachen op hun communicatievaardigheden.

2 Productarchitectuur



Afbeelding 1: Infrastructuur van GoTo Contact

3 Technische controlemechanismen van GoTo Contact

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.

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.

De via een API geïntegreerde GoTo Contact-service maakt gebruik van GoTo's eigen identiteitsbeheerplatform voor de inrichting van klanten, en biedt single sign-on (SSO) aan met behulp van Security Assertion Markup Language (SAML). Zo kunnen krachtige besturingselementen worden aangeboden, waaronder de mogelijkheid voor beheerders van klantaccounts om beleidsregels voor wachtwoorden te configureren, het resetten van wachtwoorden af te dwingen, en het gebruik van SAML voor aanmelding verplicht te stellen.

PBX-beheerders (superbeheerders) van GoTo Contact kunnen de machtigingen van andere gebruikers instellen, zoals het aanstellen van Beheerders. Deze machtigingen omvatten de mogelijkheid om de PBX te configureren, E911-adressen en -locaties te bewerken, rapporten weer te geven, facturen te bekijken en te betalen, en instellingen en accounts bij te werken en te verwijderen voor:

- Gebruikers;
- Gebruikersgroepen;
- Extensies;
- Apparaten;
- Hardware;
- Locaties; en
- Telefoonnummers (verwijderen en aanmaken, beheerd via nummerbestelling).

Machtigingen op gebruikersniveau worden niet rechtstreeks geconfigureerd, omdat ze worden afgeleid van de gebruiker-, apparaat- en lijnrelaties.

Raadpleeg de PBX-handleiding van GoTo Connect voor beheerders voor meer informatie over groepsmachtigingen.

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. Kritieke systeembestanden zijn beschermd tegen kwaadwillige aanvallen en onbedoelde blootstelling of vernietiging.

3.3 Scheiding van gegevens

De service maakt gebruik van een multi-PBX-architectuur met meerdere tenants, logisch gescheiden op databaseniveau, gebaseerd op de serviceaccount van een gebruiker of organisatie. Alleen geverifieerde partijen krijgen toegang tot relevante accounts.

3.4 Fysieke beveiliging

Fysieke beveiliging van datacenters
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 het betreffende ticketingsysteem. Vervolgens moet de aanvraag worden goedgekeurd door de betreffende manager, en worden beoordeeld en goedgekeurd door het technische operationele team. 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

Om redundantie, oproepdoorschakeling, schaalbaarheid en hoge beschikbaarheid te bieden, gebruikt de Service een meshnetwerk met microservices en containers, dat een snelle implementatie en schaalbaarheid van services mogelijk maakt om aan de behoeften van de klanten van GoTo te voldoen. De onderlinge verbondenheid van dit ontwerp zorgt ervoor dat microservices zichzelf kunnen ontdekken en herstellen bij een storing in een bepaald datacenter, of in het geval van een probleem dat geografisch gelokaliseerd is op het openbare internet. Services zijn ontworpen om wanneer nodig automatisch te kunnen schakelen tussen datacenters.

De infrastructuur is onderling verbonden tussen datacenters in de vorm van 'clusters', met interconnectiviteit van een VPLS-meshnetwerk (Virtual Private LAN Service). VPLS-verbindingen kunnen wanneer nodig automatisch doorschakelen naar een Dynamic Multipoint Virtual Private Network (DMVPN) in het geval dat primaire links offline gaan. Elke site heeft meerdere peering-verbindingen met het openbare internet. Alle productiedatacenters zijn zodanig met elkaar verbonden dat interne toepassingen vanaf elke locatie services kunnen bereiken. Elk datacenter wordt gehost op eigen hardware (op rack- en bladeservers).

Vanuit elk datacenter is er verbinding met het openbare telefoonnetwerk (PSTN) via Session Initiation Protocol (SIP)-trunks over het openbare internet naar meerdere PSTN-partners/ providers.

Om een hoge beschikbaarheid te kunnen aanbieden, beheert GoTo een netwerk van datacenters in een volledig onderling verbonden meshnetwerk. Deze datacenters werken met een capaciteit van 'N+1 datacenters', wat betekent dat de service ontworpen is om het uitvallen van het equivalent van één datacenter aan capaciteit aan te kunnen, en toch uptime te behouden door automatisch verkeer door te sturen naar andere datacentersites.

3.6 Bescherming tegen malware

De Service monitort en meldt proactief afwijkende activiteiten. Waarschuwingen die duiden op mogelijk kwaadwillige activiteiten worden naar de relevante teams gestuurd om opgelost of beperkt te worden.

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.

Versleuteling tijdens de overdracht

De Service biedt end-to-end gegevensbeveiligingsmaatregelen. De Service is zo ontworpen dat communicatiegegevens niet in onversleutelde vorm worden blootgesteld aan communicatieservers of tijdens de overdracht via openbare of privénetwerken.

De standaard TLS-protocollen (Transport Layer Security) van de Internet Engineering Task Force (IETF) worden gebruikt om de communicatie tussen eindpunten te beschermen. Al het netwerkverkeer dat GoTo-datacenters in en uit gaat, inclusief alle Klantcontent, wordt tijdens de overdracht versleuteld. Zie de Servicevoorwaarden voor meer informatie.

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, verifiëren GoTo-servers zich bij clients met behulp van openbare-sleutelcertificaten. TLS wordt kan ook worden gebruikt voor signalering tussen fysieke telefoons en de Service-infrastructuur om het verkeer en de communicatie te beveiligen, indien ondersteund door de apparatuur van de Klant. Media wordt verzonden via het Secure Real-time Transport Protocol (SRTP), met gedeelde sleutels die via Session Initiation Protocol Secure (SIPS) worden overgedragen om het audioverkeer te beveiligen. Informatie benodigd voor de inrichting, waaronder de fysieke telefoongegevens, wordt ook beveiligd met TLS tijdens de overdracht van de infrastructuur van de Service naar de telefoons.

Versleuteling tijdens de opslag

Voicemailopnamen, voicemailbegroetingen en gespreksopnamen worden versleuteld met 256-bits AES-codering wanneer ze zijn opgeslagen met de cloudopslag van GoTo.

3.8 Beheersing van kwetsbaarheden

Alle interne en externe systemen en netwerken worden minstens eens per maand gescand op 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 de ontwikkelingsteams.

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 de service 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 II incl. BSI Cloud Computing-catalogus (C5) van het American Institute of Certified Public Accountants (AICPA)
- Attestatierapport Service Organization Control (SOC) 3 Type II 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 beveiligingsgebeur-

tenissen. 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, 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. GoTo Contact voldoet aan de toepasselijke bepalingen van 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 dat beschikbaar is in het Engels en het Duits en die voldoet aan de eisen van de AVG en CCPA, en deze zelfs overstijgt, en waarin de verwerking van persoonsgegevens door GoTo is geregeld.

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. Daarnaast hebben we, om rekening te houden met de CCPA, 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 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. Bij verloop of beëindiging van het account van de Klant wordt de Klantcontent automatisch verwijderd na dertig (30) dagen vanaf de datum dat het account verloopt of is beëindigd. Op schriftelijk verzoek zal GoTo de verwijdering van dergelijke Content bevestigen.

5.6 Gevoelige gegevens

Hoewel GoTo ernaar streeft om alle Klantcontent te beschermen en te beveiligen, zijn we door wettelijke en contractuele beperkingen genoodzaakt om het gebruik van GoTo Contact 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 GoTo Contact:

- 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), evenals andere relevante toepasselijke 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 de service 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 GoTo's interne beoordeling en processen met betrekking tot het beheer van 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.