Technische en organisatorische maatregelen (TOM's)
GoTo Resolve

Samenvatting

Dit document met Technische en Organisatorische Maatregelen ('TOM's') beschrijft GoTo's privacy-, beveiligings- en verantwoordingsverplichtingen voor GoTo Resolve. 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:**[1] Verenigde Staten, Duitsland, Ierland, Zweden, Singapore, India en Nederlandse datacenterlocaties 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 Resolve heeft ISO/IEC 27001:2013, SOC 2 Type II, BSI C5, PCI DSS, PCAOB, TRUSTe Enterprise Privacy 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 Resolve-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 automatisch verwijderd: (a) negentig (90) dagen na het verstrijken van de op dat moment laatst betaalde abonnementstermijn van een Klant; of (b) voor gratis accounts, na twee (2) jaar van inactiviteit (bijv. geen aanmeldingen). Opnames worden na negentig (90) dagen op doorlopende basis verwijderd.

[1] Hostinglocaties kunnen variëren (d.w.z. afhankelijk van de gekozen verblijfplaats van de gegevens). Raadpleeg de toepasselijke openbaarmaking van subverwerkers van GoTo Resolve, die u kunt vinden in het gedeelte Productbronnen van het GoTo Trust & Privacy Center (https://www.goto.com/company/trust/resource-center).

Inhoud

Klik op de paginanummers hieronder om naar het relevante TOM-gedeelte te gaan

1 Productintroductie

GoTo Resolve stelt IT- en ondersteuningsprofessionals in staat om ondersteuning op afstand te bieden op computers, servers en mobiele apparaten, met de functionaliteit voor externe weergave, besturing op afstand, en het delen van camera's, vanaf een online of desktopconsole van een medewerker. GoTo Resolve maakt gebruik van gegevensbeveiligingsmaatregelen die ontworpen zijn ter verdediging tegen zowel passieve als actieve aanvallen.

Termen in dit document die met een hoofdletter beginnen maar niet in de tekst worden gedefinieerd, worden ofwel gedefinieerd in de Servicevoorwaarden of uitgelegd in Sectie 23.

2 Technische maatregelen

De producten van GoTo zijn ontworpen om oplossingen te bieden die veilig, betrouwbaar en privé zijn. De hieronder gedefinieerde technische maatregelen beschrijven hoe GoTo dat ontwerp implementeert en in de praktijk toepast voor GoTo Resolve.

2.1 Beveiligingsmechanismen

GoTo implementeert beveiligingsmechanismen, functionaliteit en best practices op basis van de volgende vuistregels:

I. Ontwikkeling van producten waarbij beveiliging en privacy de basis vormen van het ontwerp, en waarbij extra beveiligingslagen worden opgenomen om Klantcontent te beschermen;

II. Inrichting van organisatorische besturingselementen voor de vorming van intern beleid en afstemming van interne procedures op naleving van standaarden, incidentbeheer, applicatiebeveiliging, personeelsbeveiliging en regelmatige trainingsprogramma's; en

III. Ervoor zorgen dat er privacyprocedures zijn geïmplementeerd voor gegevensverwerking en -beheer, in overeenstemming met de toepasselijke wetgeving, waaronder de AVG, CCPA/CPRA, LGPD en ons eigen Addendum gegevensverwerking ('DPA'; Data Processing Addendum) en de toepasselijke beleidsregels en verplichtingen van GoTo.

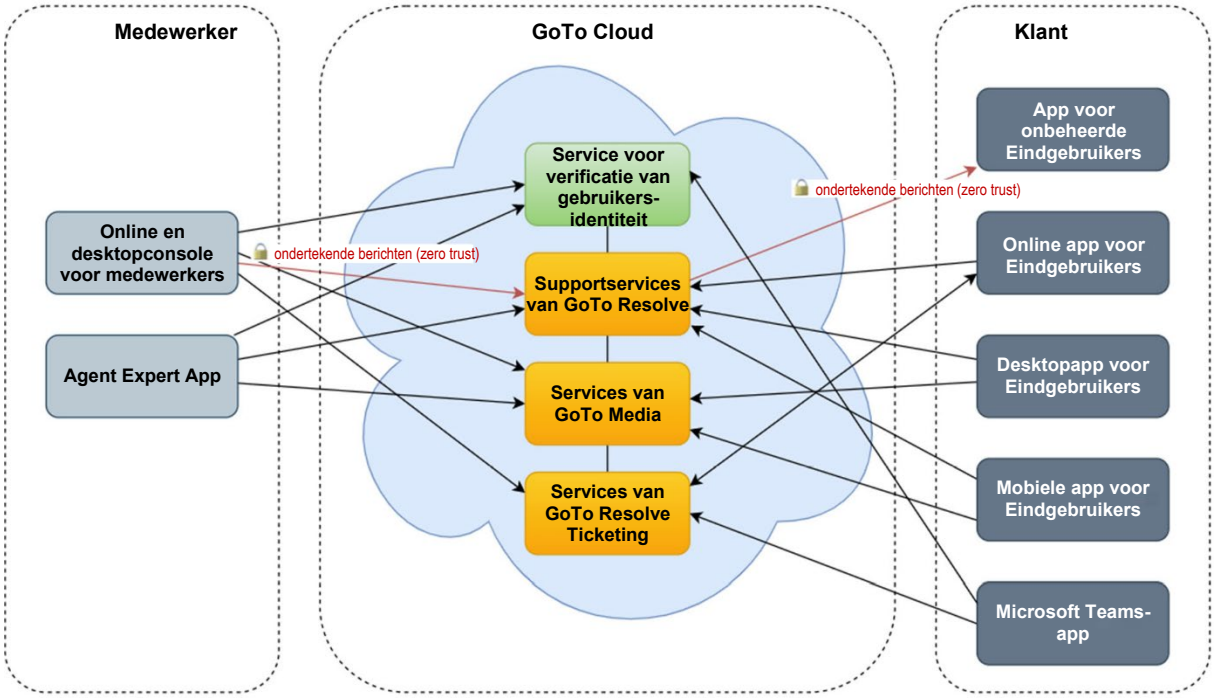
We ontwikkelen producten met beveiligingsmechanismen aan de basis, om Klantcontent van GoTo optimaal tegen bedreigingen te beschermen en ervoor te zorgen dat de voor beveiliging ingerichte besturingselementen ook echt geschikt zijn voor de aard en reikwijdte van de services. Met de configureerbare beveiligingsfuncties van GoTo kunnen beheerders bedreigingen en risico's voor systemen en netwerken, veroorzaakt door gebruikers van GoTo-services, minimaliseren.

3 Productarchitectuur

GoTo Resolve gebruikt een ASP-model (Application Service Provider) dat ontworpen is om een beveiligde werkomgeving te bieden, terwijl het geïntegreerd wordt met de bestaande netwerk- en beveiligingsinfrastructuur van een bedrijf. De architectuur is ontworpen met het oog op optimale prestaties, betrouwbaarheid en schaalbaarheid. GoTo Resolve maakt gebruik van Amazon Web Services en Microsoft Azure cloudresources om een schaalbare, en zeer beschikbare oplossing te bieden, die storingsvrij is. GoTo Resolve heeft back-upsystemen die in meerdere regio's worden gehost om de continue werking van applicatieprocessen te ondersteunen in het geval van te zware belasting of algehele systeemstoring.

3.1 Communicatiearchitectuur

De communicatiearchitectuur van GoTo Resolve wordt in de onderstaande afbeelding samengevat:



Afbeelding 1: Communicatiearchitectuur van GoTo Resolve

Voor de verificatie van medewerkers wordt GoTo's eigen service voor verificatie van gebruikersidentiteit ingezet. Communicatie tussen deelnemers in een GoTo Resolve-sessie vindt plaats via een overlay-netwerkstack die logisch is gepositioneerd boven het conventionele User Datagram Protocol (UDP) en Transmission Control Protocol/Internet Protocol (TCP/IP). Dit netwerk wordt geleverd door GoTo Resolve en GoTo Media Services, en is gehost op Amazon Web Services en Microsoft Azure.

Deelnemers aan GoTo Resolve-sessies (met de online console voor medewerkers, desktopconsole voor medewerkers, Agent Expert App, en eindpunten van eindgebruikers (in afbeelding 1 weergegeven als eindpunten van de 'Klant')) communiceren met de services van GoTo Resolve en de GoTo Media via uitgaande TCP-verbindingen op poort 443 of UDP-poort 15000, afhankelijk van beschikbaarheid. Omdat GoTo Resolve een webgebaseerde service is, hebben deelnemers er bijna overal toegang toe als ze verbonden zijn met het internet – op een extern kantoor, thuis, in een winkelcentrum of verbonden met het netwerk van een ander bedrijf.

3.2 Desktopconsole voor medewerkers

Medewerkers kunnen de online console of de installeerbare desktopconsole gebruiken om verbinding te maken met GoTo Resolve. De desktopconsole gebruikt de voor alle platforms geschikte Qt-toolkit, om zowel op MacOS als op Windows te kunnen draaien, en de open-sourcewebbrowser Chromium, om onderdelen van de online console te ondersteunen.

3.3 Model op basis van 'zero trust'

3.3.1 Architectuur

GoTo Resolve maakt gebruik van een zero-trust-architectuur. Medewerkers die GoTo Resolve gebruiken moeten een persoonlijke sleutel aanmaken die een vereiste, extra vorm van verificatie is, en gebruikt wordt bij het uitvoeren van gevoelige taken.

Bij het implementeren van de GoTo Resolve-applicatie op een extern apparaat creëert de sleutel een koppeling tussen de medewerker en het apparaat, om de medewerker op unieke wijze te identificeren. Deze sleutel wordt gebruikt bij versleuteling van elke opdracht die naar een apparaat op afstand wordt verzonden, en laat zien wie elke opdracht verzendt. Autorisatie van opdrachten is gebaseerd op asymmetrische sleutelparen van zowel een openbare als een persoonlijke sleutel, waarbij de persoonlijke sleutel wordt gebruikt om opdrachten te ondertekenen, en alleen bekend is bij de medewerker (d.w.z. niet bekend bij GoTo Resolve-services of eindpunten van Klanten). De openbare sleutel wordt ingezet op elk eindpunt van de eindgebruiker, en dient om de handtekening van elke door de medewerker ontvangen opdracht te verifiëren. In dit model 'vertrouwen' de eindgebruikers niet GoTo Resolve-services, maar de opdrachten die van een medewerker met een geverifieerde sleutel komen.

3.3.2 Typen handtekeningsleutels

De kern van de handtekeningensleutel is een persoonlijk-openbaar sleutelpaar: de openbare sleutel wordt op de backend opgeslagen en met elk apparaat gedeeld, terwijl de persoonlijke sleutel de machine/browser nooit in ongecodeerde vorm verlaat. Het sleutelpaar wordt willekeurig gegenereerd op de elliptische P-384-curve, in de browser van de medewerker, en met behulp van native methoden.

De cryptografische sleutelparen worden versleuteld met een wachtwoord en vervolgens opgeslagen in het backend, zodat de medewerker er vanuit elke browser toegang toe heeft. De coderingssleutel wordt afgeleid van het wachtwoord en is voor elk bedrijf en elke medewerker anders.

3.3.3 Blokvercijfering

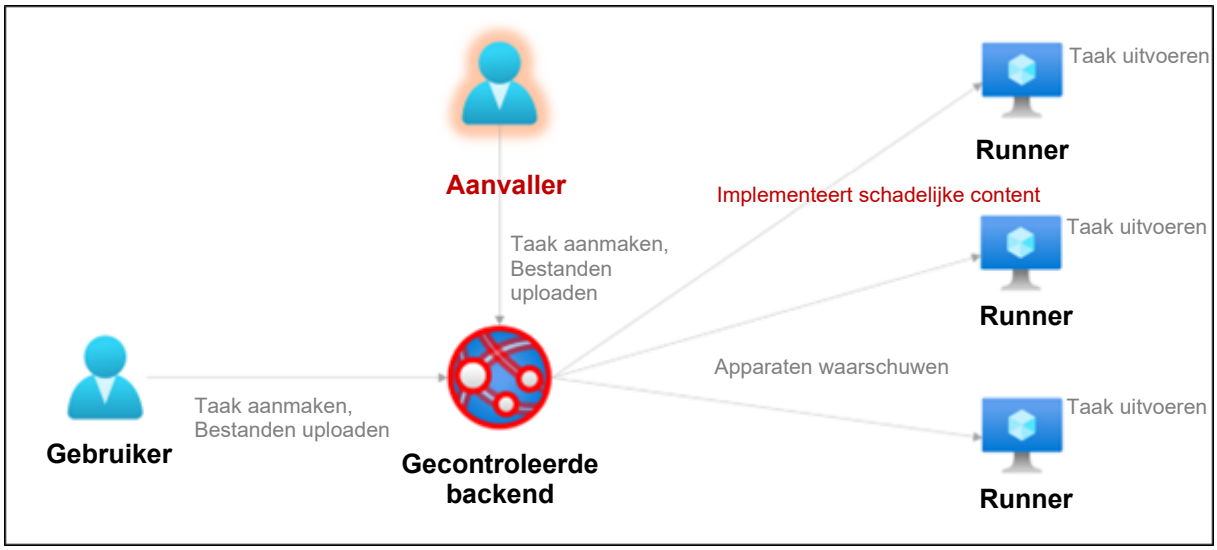
De cryptografische bewerkingen van de zero-trust-architectuur komen tot stand met de volgende algoritmen:

- ECDSA op elliptische P-384-curve (gebruikt voor het genereren van persoonlijk-openbare sleutels)
- Hashing-algoritme SHA-256/512
- HMAC-SHA-256 (gebruikt voor verificatie van berichten)
- AES256 met GCM-blokvercijfering (gebruikt voor sleutelcodering)
- PBKDF2-sleutelafleidingsfunctie

Deze cryptosystemen en blokvercijferingen worden verwerkt door het besturingssysteem of de OpenSSL-bibliotheek.

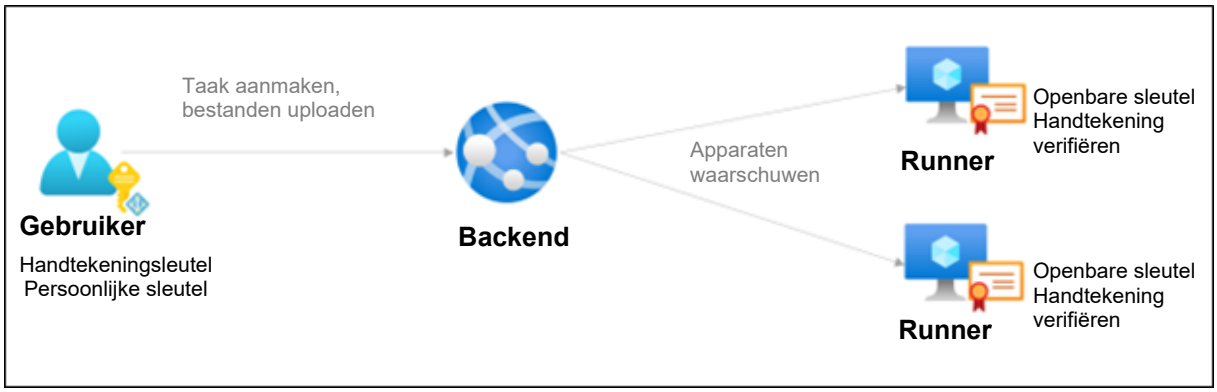
3.4 Probleemvaststelling

De volgende diagrammen (Afbeeldingen 2, 3 en 4 hieronder) maken inzichtelijk hoe de zero-trust-architectuur van GoTo Resolve is ontworpen om personen te beschermen. Afbeelding 2 toont een hypothetisch scenario dat zou ontstaan als een backend wordt gecompromitteerd in een architectuur zonder zero trust, waarbij een aanvaller kwaadaardige content kan implementeren op de runners door jobs aan te maken.



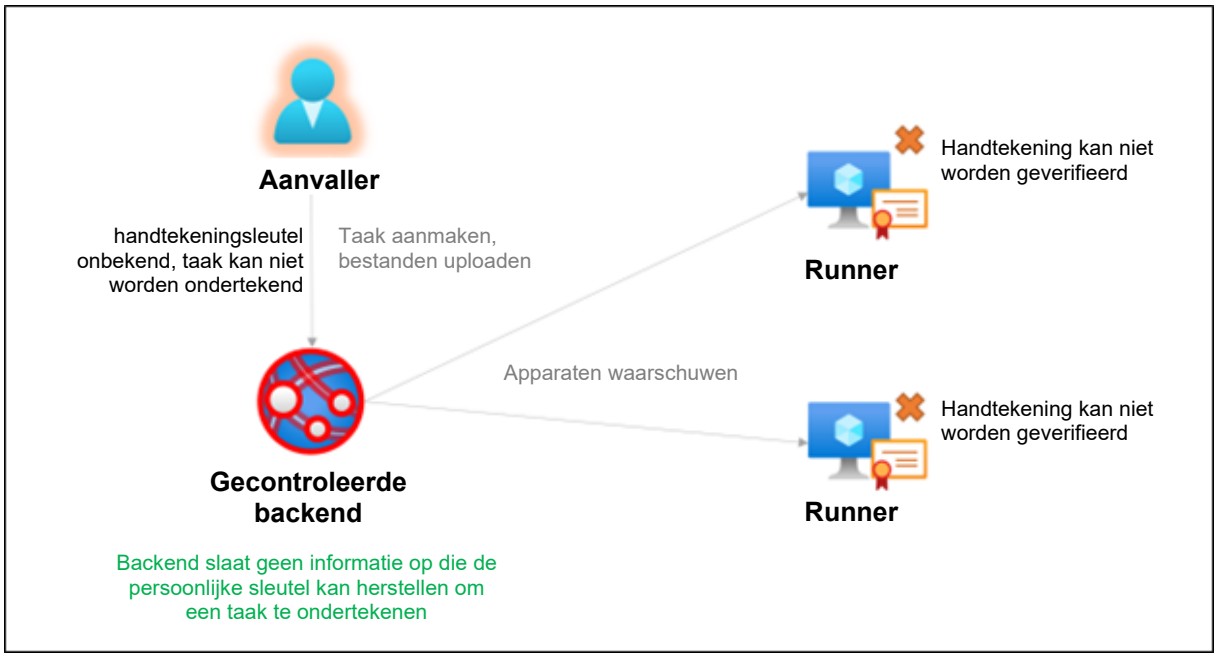
Afbeelding 2. Gecompromitteerd backendsysteem zonder zero trust

Afbeeldingen 3 en 4 laten de voordelen zien van het zero-trust-model, waarbij elke taak wordt ondertekend met de (persoonlijke) sleutel van de gebruiker voordat deze naar de backend wordt gestuurd. Ondertekende taken worden doorgestuurd naar de runners, die ze vervolgens kunnen verifiëren met behulp van de openbare sleutel. De taken worden pas uitgevoerd nadat de openbare sleutel is geverifieerd. Afbeelding 3 laat zien hoe zero trust enkele van deze potentiële risico's uitsluit.



Afbeelding 3. Taak ondertekenen en handtekeningverificatie in zero-trust-omgeving

Afbeelding 4 geeft een hypothetisch scenario weer dat zou ontstaan als een backend wordt gecompromitteerd in een zero-trust-omgeving. In dit scenario heeft de aanvaller geen toegang tot de handtekeningsleutel en kan hij dus geen kwaadaardige content implementeren of communiceren met de runners. In dit scenario zou de verificatie van de persoonlijke en openbare sleutel mislukken en zou de runner de taak of opdracht afwijzen. De handtekeningsleutel kan niet hersteld worden vanuit de openbare sleutel.



Afbeelding 4. Gecompromitteerde backend binnen een zero-trust-omgeving

3.5 Infrastructuur voor mediaservices

De media-infrastructuur bestaat uit de volgende servers/protocollen:

- Signaleringsserver
- De servers Session Traversal Utilities for NAT (STUN) en Traversal Using Relays around NAT Secure (TURN(S))

De signaleringsserver gebruikt veilige WebSockets (kanalen voor full-duplexcommunicatie) om tegelijkertijd met de eindgebruiker en de medewerker te communiceren en metadata en verificatiegegevens te delen die nodig zijn voor het opzetten van de peer-to-peer-verbinding. Na het upgraden van de HTTPS-verbinding communiceren de client en de server via dezelfde TCP-verbinding en gebruiken ze TLS 1.2 om de verbinding te beveiligen.

WebRTC wordt gebruikt om realtimecommunicatie (RTC) te bieden aan webbrowsers en toepassingen voor ondersteuning op afstand. Alle WebRTC-sessies maken gebruik van SRTP-versleuteling (Secure Real-Time Transport Protocol). WebRTC versleutelt informatie (met name gegevenskanalen) met behulp van Datagram Transport Layer Security (DTLS) 1.2 in het geval van UDP, en TLS 1.2 in het geval van TCP-verbindingen. Alle gegevens die via RTCDataChannel worden verzonden zijn beveiligd met DTLS.

DTLS-SRTP wordt gebruikt als een veilig protocol voor sleuteluitwisseling en vereist dat de sleutels met betrekking toto media van peer naar peer worden verzonden. De TURNS-server gebruikt TLS 1.2 over TCP om gegevens tussen de peers door te geven.

4 Technische beveiligingsmaatregelen

GoTo maakt gebruik van technische besturingselementen voor beveiliging die zijn ontworpen om de infrastructuur van de service en de gegevens daarin te beschermen.

4.1 Versleuteling

GoTo herziet regelmatig zijn standaarden op het gebied van versleuteling, en kan de gebruikte blokvercijferingen en/of technologieën bijwerken in overeenstemming met het ingeschatte risico en de marktacceptatie van nieuwe standaarden.

4.1.1 Versleuteling tijdens de overdracht

GoTo gebruikt TLS-protocollen en bijbehorende blokvercijfering om de Klantcontent tijdens de overdracht te beschermen.

De communicatie tussen eindpunt en backend van de eindgebruiker wordt versleuteld via de OpenSSL-bibliotheek. Er zijn via TLS-oplossingen besturingselementen voor beveiliging van communicatie geïmplementeerd op de TCP-laag.

Schermgegevens, toetsenbord-/muisbesturingsgegevens, overgedragen bestanden, diagnostische gegevens op afstand en tekstchatinformatie worden tijdens de overdracht versleuteld met TLS 1.2 (ECDHE, DHE en RSA voor sleuteluitwisseling, RSA voor verificatie, AES256 voor gegevensversleuteling met een 384- of 256-bits SHA-2 HMAC-algoritme). Sessiesleutels worden vanaf de server gegenereerd en blijven daar om de verbinding met de Eindgebruiker mogelijk te maken.

GoTo-servers verifiëren zichzelf voor klanten met behulp van openbare-sleutelcertificaten die worden ondertekend door DigiCert of GlobalSign Global Root CA wanneer verbindingen tot stand worden gebracht met de GoTo Resolve-website, en tussen GoTo Resolve-onderdelen. Server-to-server-API's zijn alleen toegankelijk binnen het door een firewall beschermde privénetwerk van GoTo.

4.1.2 Versleuteling tijdens de opslag

Aan de serverkant wordt de opgeslagen Klantcontent versleuteld met AES256, met behulp van Galois Counter Mode (GCM) of vergelijkbare moderne blokvercijfering. Aan de clientkant heeft GoTo de clienttoepassing geconfigureerd om aanmeldingsgegevens op te slaan en te beveiligen die verbinding met de service mogelijk maken via de cryptografische API's van het besturingssysteem. Klantcontent wordt niet op de client opgeslagen.

4.2 Beveiliging TCP-laag

TLS-protocollen worden gebruikt om communicatie tussen openbare eindpunten te beschermen.

4.3 Bescherming van eindpunten voor eindgebruikers

Desktopapps voor Eindgebruikers en apps voor onbeheerde Eindgebruikers worden gedownload en geïnstalleerd via een digitaal ondertekend installatieprogramma.

Het installatieprogramma maakt gebruik van een uitvoerbare download waarvoor robuuste cryptografische maatregelen zijn getroffen om de eindgebruiker te beschermen tegen het per ongeluk installeren van een Trojaans paard of andere malware die zich voordoet als GoTo Resolve-software.

De eindpuntsoftware van GoTo Resolve bestaat uit verschillende digitaal ondertekende uitvoerbare bestanden en dynamisch gekoppelde bibliotheken. GoTo heeft procedures voor kwaliteitscontrole en configuratiebeheer geïmplementeerd, zowel voor tijdens de ontwikkeling als de implementatie van de software.

4.4 Verificatie van gebruikers

Medewerkers en accountbeheerders worden geïdentificeerd aan de hand van hun e-mailadres en geverifieerd met een wachtwoord. Tijdens geautoriseerde verificatie is het wachtwoord gedurende de hele overdracht versleuteld.

Op de verificatieprocedures zijn de volgende beleidsregels van toepassing:

Vereisten voor sterke wachtwoorden: Wachtwoorden moeten minimaal 8 tekens lang zijn en zowel letters als cijfers bevatten. Wachtwoorden moeten aan deze minimumvereisten voldoen wanneer ze worden aangemaakt of gewijzigd.

Tweeledige verificatie: Tweeledige verificatie is optioneel en kan worden ingeschakeld op accountniveau. Indien ingeschakeld, vereist tweeledige verificatie dat elke gebruiker of eindgebruiker binnen het account toegang verifieert via twee afzonderlijke methoden.

Vergrendeling van accounts: Een account van een Gebruiker of Eindgebruiker wordt verplicht 'zacht vergrendeld' na vijf opeenvolgende mislukte inlogpogingen. Deze zachte vergrendeling voorkomt toegang tot het account gedurende vijf minuten. Na afloop van de vergrendeling kan de Gebruiker of Eindgebruiker zich opnieuw proberen aan te melden bij zijn account.

4.5 Beveiliging tijdens de sessie

Een Gebruiker kan een onbeheerde sessie op elk moment beëindigen, en de privileges voor onbeheerde ondersteuning van de medewerker permanent intrekken.

5 Bijwerken van beveiliging

GoTo controleert en actualiseert zijn beveiligingsprogramma regelmatig, en schakelt onafhankelijke derden in om relevante besturingselementen voor beveiliging minstens eenmaal per jaar te beoordelen. Zo zorgt GoTo ervoor dat de beveiliging opgewassen blijft tegen actuele bedreigingen en voldoet aan relevante kaders, industrienormen, toezeggingen van klanten en, indien van toepassing, wijzigingen in wet- en regelgeving met betrekking tot de beveiliging van GoTo-gegevens.

6 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 deze systemen wordt periodiek getest.

7 Datacenters

De GoTo-infrastructuur is ontworpen om de betrouwbaarheid van de service te verhogen en het risico op uitval door storingen te verminderen, door gebruik te maken van:

a) redundante, actief-passieve datacenters; of
b) datacenters van cloudhostingproviders.

Bij het aanmaken van een account kunnen klanten van GoTo Resolve ervoor kiezen om de Europese of wereldwijde gegevensinfrastructuur van GoTo te gebruiken om hun Klantcontent in op te slaan. De hostinglocaties zijn hieronder gespecificeerd[2]:

- **Europese Unie:** Duitsland, Ierland, Zweden en Nederland
- **Wereldwijd:** de Verenigde Staten, Duitsland, Singapore, India en Nederland.

Alle datacenters bewaken de omgevingscondities, en zijn 24 uur per dag voorzien van fysieke beveiligingsmaatregelen die hieronder worden beschreven.

7.1 Fysieke beveiliging datacenters

GoTo werkt samen met datacenters om de fysieke beveiliging te waarborgen voor systemen en servers die Klantcontent bevatten. Deze beveiligingsmiddelen zijn bijvoorbeeld:

- Videobewaking en -opname
- Temperatuurregeling met verwarming, ventilatie en airconditioning
- Brandbestrijding en rookmelders
- Ononderbreekbare stroomvoorziening
- 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 biedt uitsluitend fysieke toegang tot productiedatacenters aan daartoe 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 van GoTo. Alle fysieke toegang tot datacenters en serverruimtes wordt bijgehouden, en de logbestanden worden minstens elk kwartaal gecontroleerd door het GoTo-management. Daarnaast wordt de autorisatie voor fysieke toegang tot het datacenter onmiddellijk opgeheven bij het wijzigen van de rol (wanneer dergelijke toegang niet langer vereist is) of bij het ontslag van eerder geautoriseerd personeel. Toegang met meerdere factoren (zoals biometrische gegevens, een badge of een toetsenblok) is vereist voor zeer gevoelige gebieden, waaronder datacenters.

[2] Hostinglocaties kunnen variëren (d.w.z. afhankelijk van de gekozen verblijfplaats van de gegevens). Raadpleeg de toepasselijke openbaarmaking van subverwerkers van GoTo Resolve, die u kunt vinden in het gedeelte Productbronnen van het GoTo Trust & Privacy Center (https://www.goto.com/company/trust/resource-center).

8 Naleving van normen

GoTo beoordeelt regelmatig of het voldoet aan de toepasselijke wettelijke, beveiligings-, financiële, gegevensprivacy- en regelgevingsvereisten. De privacy- en beveiligingsprogramma's van GoTo voldoen aan strenge en internationaal erkende normen, zijn beoordeeld volgens uitgebreide externe auditnormen en hebben belangrijke certificeringen behaald, waaronder:

- **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.
- **TRUSTe APEC CBPR- en PRP-certificaten** voor de overdracht van Klantcontent tussen APEC-lidstaten, verkregen en onafhankelijk gevalideerd door TrustArc, een door APEC goedgekeurde derde partij die toonaangevend is op het gebied van naleving van gegevensbescherming. Klik hier voor meer informatie over onze APEC-certificaten.
- Internationale Organisatie voor Standaardisatie – **ISO/IEC 27001:2013** Certificaat Information Security Management System (ISMS), inzake beheersystemen voor informatiebeveiliging.
- **Attestatierapport Service Organization Control (SOC) 2 Type II** incl. **BSI Cloud Computing-catalogus (C5)** 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)**.

9 Beveiliging van toepassingen

Het applicatiebeveiligingsprogramma van GoTo volgt de SDL (Security Development Lifecycle) van Microsoft om productcode te beveiligen. Het Microsoft SDL-programma omvat handmatige codebeoordelingen, bedreigingsmodellen, statische codeanalyse, dynamische analyse en systeemverharding. GoTo-teams voeren ook periodiek dynamische en statische tests uit op de kwetsbaarheid van applicaties, evenals penetratietests voor getroffen omgevingen.

10 Rapporteren, monitoren en waarschuwen

GoTo heeft beleidsregels en procedures ingericht voor alle vormen van rapporteren, monitoren en waarschuwen. Hierin worden de principes en besturingselementen beschreven die worden geïmplementeerd om verdachte activiteiten beter te detecteren en hier tijdig op te reageren. GoTo verzamelt geïdentificeerd afwijkend of verdacht verkeer in relevante beveiligingslogbestanden in toepasselijke productiesystemen.

11 Detectie en respons van eindpunten

Software voor detectie en respons van eindpunten, inclusief auditrapportage, wordt op alle GoTo-servers gebruikt om onderbrekingen van of impact op de prestaties van de service tot een minimum te beperken. Voor zover van toepassing en noodzakelijk worden er beveiligingsonderzoeken uitgevoerd, in overeenstemming met onze procedures voor het reageren op incidenten, wanneer er verdachte activiteiten worden gedetecteerd. Zie hoofdstuk 17 voor meer informatie over GoTo's Beveiligingscentrum en de procedures voor het reageren op incidenten.

12 Beheren van bedreigingen

GoTo's Cyber Security Incident Respons Team ('CSIRT') bestaat uit meerdere teams en is verantwoordelijk voor de bescherming tegen cyberbedreigingen. Het Cyber Threat Intelligence-team binnen het CSIRT verzamelt, onderzoekt en verspreidt informatie over huidige en opkomende bedreigingen. GoTo blijft op de hoogte van informatie over bedreigingen en risicobeperking door zowel open als gesloten bronnen te bekijken, deel te nemen aan groepen waarin informatie over bedreigingen gedeeld wordt, en via lidmaatschap bij brancheverenigingen (IT-ISAC, FIRST.org, enz.).

13 Scannen op beveiliging en kwetsbaarheid en patchbeheer

GoTo heeft een formeel patchbeheerprogramma ingericht en voert minstens elk kwartaal patchbeheeractiviteiten uit op alle relevante systemen, apparaten, firmware, besturingssystemen, toepassingen en andere software waarmee Klantcontent wordt verwerkt. GoTo beoordeelt en scant op kwetsbaarheden op systeemniveau en in interne en externe hosts/netwerken ('Systemen'), ten minste maandelijks, en na elke wezenlijke verandering aan dergelijke Systemen, en verhelpt relevante ontdekte kwetsbaarheden in overeenstemming met gedocumenteerde Beleidsregels die prioriteit geven aan herstel op basis van risico.

14 Logische toegangscontrole

Er zijn procedures ingericht voor logische toegangscontrole om het risico van onbevoegde toegang tot toepassingen en gegevensverlies in bedrijfs- en productieomgevingen te beperken. Medewerkers krijgen toegang tot specifieke GoTo-systemen, toepassingen, netwerken en apparaten op basis van het principe van de minste rechten. Gebruikersprivileges worden gescheiden op basis van functionele rol (toegangscontrole op basis van rollen) en omgeving, door onderscheid te maken tussen besturingselementen, processen en/of procedures van functies.

Productieservers zijn alleen beschikbaar via een virtueel privénetwerk (VPN). Verificatie via Self Service Unix (SSU) is vereist om toegang te krijgen tot cloudgebaseerde productieonderdelen.

14.1 Toegangscontrole op basis van toestemming

14.1.1 Bijgewoonde sessie

Een essentieel onderdeel van de beveiliging van GoTo Resolve is het toegangscontrolemodel op basis van toestemming, dat ontworpen is om de toegang tot het systeem en de gegevens van de eindgebruiker te beschermen. Tijdens live ondersteuningssessies die door een Eindgebruiker worden bijgewoond, wordt de Eindgebruiker voorafgaand aan de schermdeling, besturing op afstand of bestandsoverdracht, om toestemming gevraagd voor het relevante proces.

Wanneer een Eindgebruiker tijdens een beheerde sessie toestemming geeft voor besturing op afstand en schermdeling, kan deze alles zien wat de medewerker doet. De Eindgebruiker kan op elk moment de controle terugnemen of de sessie beëindigen.

14.1.2 Onbeheerde sessie

Voor onbeheerde ondersteuning moet de app voor onbeheerde eindgebruikers geïnstalleerd zijn op het apparaat van de Eindgebruiker. De app kan op twee manieren worden ingesteld: installatie tijdens een beheerde sessie, of met een programma voor installatie buiten de sessie om. In beide gevallen is toestemming van de Eindgebruiker vereist.

Installatie tijdens de sessie: Zodra de eindgebruiker en de medewerker een sessie zijn begonnen, kan de medewerker toestemming vragen om de app voor onbeheerde Eindgebruikers te installeren. De Eindgebruiker krijgt een venster te zien waarin hij expliciet wordt gevraagd om zijn toestemming te verlenen.

Programma voor installatie buiten de sessie om: Nadat een medewerker veilig is aangemeld bij de GoTo Resolve-website of -desktopapplicatie, kan deze een installatieprogramma downloaden waarmee de app voor onbeheerde eindgebruikers kan worden geïnstalleerd op elke Windows-pc of Mac waarvoor de medewerker beheerderstoegang heeft.

14.1.3 Rolgebaseerde toegangscontrole

GoTo Resolve biedt toegang tot verschillende bronnen en diensten met behulp van een toegangscontrolesysteem op basis van rollen. De volgende rollen zijn gedefinieerd:

Beheerder: GoTo Resolve-gebruiker met volledige beheerdersbevoegdheden om administratieve functies met betrekking tot medewerkers uit te voeren. Beheerders van accounts kunnen accounts van medewerkers aanmaken, wijzigen en verwijderen, en de abonnementsgegevens ervan wijzigen.

Medewerker: GoTo Resolve-gebruiker die GoTo Resolve-sessies kan starten om technische ondersteuning te bieden aan Eindgebruikers, via externe weergave, besturing op afstand, en het delen van camera's.

Eindgebruiker: personen die GoTo services gebruiken (zoals niet-geverifieerde personen die ondersteuning van een medewerker vragen). De eindgebruiker kan sessies sluiten en moet de medewerker toegang verlenen tot zijn apparaat.

15 Scheiding van gegevens

GoTo heeft besturingselementen geïmplementeerd om te voorkomen dat Gebruikers de gegevens van andere Gebruikers zien. GoTo maakt bijvoorbeeld gebruik van een architectuur met meerdere tenants, logisch gescheiden op databaseniveau, gebaseerd op de GoTo-account van een gebruiker of organisatie. Partijen moeten worden geverifieerd om toegang te krijgen tot een account.

16 Perimeterbescherming en inbraakdetectie

GoTo gebruikt tools, technieken en diensten voor perimeterbescherming, ingericht om te voorkomen dat onbevoegd netwerkverkeer de productinfrastructuur binnendringt. Deze omvatten, maar zijn niet beperkt tot:

- Intrusiedetectiesystemen waarmee systemen, diensten, netwerken en toepassingen worden gecontroleerd op onbevoegde toegang
- Bewaking van kritieke systemen en configuratiebestanden
- Webtoepassingsfirewall (WAF) en DDoS-preventiediensten op de applicatieniveau die fungeren als proxy voor GoTo-verkeer
- AWS-beveiligingsgroepen op GoTo-webservers die inkomende en uitgaande verbindingen filteren, inclusief interne verbindingen tussen GoTo-systemen
- Interne netwerksegmentatie.

17 Het Security Operations Center en incidentbeheer

Het Security Operations Center (SOC) van GoTo is verantwoordelijk voor het detecteren van en reageren op beveiligingsgebeurtenissen. Het SOC maakt gebruik van beveiligingssensoren en analysesystemen om potentiële problemen te identificeren, en heeft procedures ontwikkeld om op incidenten te reageren, waaronder een gedocumenteerd Incidentenbestrijdingsplan.

Het Incidentenbestrijdingsplan van GoTo is afgestemd op de kritieke communicatieprocessen, beleidsregels en standaardwerkprocedures van GoTo. Het is ontworpen om relevante verdachte of geïdentificeerde beveiligingsgebeurtenissen in interne systemen en diensten, inclusief GoTo Resolve, te beheren, te identificeren en op te lossen. Het Incidentenbestrijdingsplan beschrijft mechanismen voor medewerkers om verdachte beveiligingsgebeurtenissen te melden, evenals escalatiepaden die indien nodig gevolgd moeten worden. Verdachte gebeurtenissen worden gedocumenteerd en indien nodig geëscaleerd via gestandaardiseerde gebeurtenistickets, waarbij prioriteit wordt gegeven aan de meest alarmerende gebeurtenissen.

18 Verwijderen en retourneren van Content

Verwijdering en/of teruggave: Klanten kunnen verzoeken om teruggave en/of verwijdering van hun Klantcontent door een verzoek in te dienen via GoTo's Portaal voor Beheer van Individuele Rechten ('IRM'; Individual Rights Management Portal), via support.goto.com of door een e-mail te sturen naar privacy@goto.com. Verzoeken worden binnen dertig (30) dagen na ontvangst door GoTo verwerkt, maar in het onwaarschijnlijke geval dat we meer tijd nodig hebben, zullen we u zo snel mogelijk op de hoogte stellen van de verwachte termijn.

Schema voor het bewaren van Klantcontent: Sessie-opnamen worden doorlopend verwijderd na een termijn van 90 dagen.[3] Daarnaast wordt de Klantcontent automatisch verwijderd, tenzij anders vereist door de toepasselijke wetgeving: 1) voor betaalde accounts; negentig (90)

[3] Klanten met andere retentievereisten kunnen ervoor kiezen om opnames lokaal op te slaan, op een opslaglocatie van hun keuze, buiten de GoTo-omgevingen. Voor meer informatie kunt u de sectie 'Sessieopnames afspelen' hier raadplegen.

dagen na de beëindiging, annulering of afloop ervan en, in elk geval wordt de inrichting van het op dat moment laatste abonnement van de Klant opgeheven; of 2) voor gratis accounts; na twee (2) jaar van inactiviteit (bijv. geen aanmeldingen).

Op schriftelijk verzoek kan GoTo een schriftelijke bevestiging/certificering van de verwijdering van de Content geven.

19 Organisatorische besturingselementen

19.1 Beveiligingsbeleid en -procedures

GoTo heeft een uitgebreide reeks beveiligingsbeleidsregels en -procedures die regelmatig worden herzien en bijgewerkt, ter ondersteuning van de beveiligingsdoelstellingen van GoTo, of wegens wijzigingen in de nalevingsvereisten van toepasselijke wetgeving of industriestandaarden.

19.2 Veranderingsbeheer

GoTo heeft een proces ingericht voor het beheren van veranderingen. Wijzingen in GoTo-systemen worden vóór de implementatie ervan beoordeeld, getest en goedgekeurd om het risico op onderbreking van GoTo-services te beperken.

19.3 Bewustzijns- en trainingsprogramma's over beveiliging

GoTo's heeft een programma ingericht ter vergroting van de bewustwording ten aanzien van privacy en beveiliging. Het programma biedt trainingen aan medewerkers over het belang van de ethische, verantwoordelijke en zorgvuldige behandeling van Persoonsgegevens en vertrouwelijke informatie, en de verwerking ervan conform de toepasselijke wetgeving. Nieuwe medewerkers, contractanten en stagiaires worden tijdens de inwerkperiode geïnformeerd over het beveiligingsbeleid en de Gedragscode en Bedrijfsethiek van GoTo. Medewerkers van GoTo volgen minstens eenmaal per jaar een bewustwordingstraining ten aanzien van privacy en beveiliging. Activiteiten ter vergroting van de bewustwording vinden het hele jaar door plaats. Denk bijvoorbeeld aan campagnes voor Dag van de Gegevensprivacy en Maand van de Cyberveiligheid, webinars van het Hoofd Informatiebeveiliging, en een beloningsprogramma voor 'beveiligingskampioenen'.

Waar nodig kunnen medewerkers ook verplicht worden om rolspecifieke trainingen te volgen. Daarnaast moeten alle medewerkers, contractanten en dochterondernemingen van GoTo het beleid van GoTo met betrekking tot beveiliging en gegevensbescherming doornemen en naleven.

20 Privacy

GoTo neemt de privacy van onze Klanten, Gebruikers 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.

20.1 Privacyprogramma.

GoTo heeft een uitgebreid privacyprogramma waarmee coördinatie van meerdere functies binnen het bedrijf gemoeid is, waaronder de afdelingen Privacy, Beveiliging, Governance, Risico- en nalevingsbeheer, Juridische Zaken, het Productteam, Engineering en Marketing. Dit privacyprogramma is gericht op naleving en omvat de implementatie en het onderhoud van interne en externe beleidsregels, normen en addenda om de best practices van het bedrijf te regelen.

20.2 Naleving van regelgeving

20.2.1 AVG

De Algemene verordening gegevensbescherming (AVG) is een wet van de Europese Unie (EU) met betrekking tot gegevensbescherming en privacy voor personen binnen de EU. GoTo heeft een uitgebreid AVG-nalevingsprogramma, en voor zover GoTo namens de Klant persoonsgegevens verwerkt die onder de AVG vallen, zullen we dit doen in overeenstemming met de toepasselijke vereisten van de AVG. Ga voor meer informatie naar https://www.goto.com/company/trust/privacy.

20.2.2 CCPA

De California Consumer Privacy Act, zoals gewijzigd door de California Privacy Rights Act (samen de 'CCPA' genoemd) geeft Californiërs extra rechten en bescherming met betrekking tot de manier waarop bedrijven hun persoonlijke gegevens mogen gebruiken. GoTo heeft een uitgebreid nalevingsprogramma en voor zover GoTo namens de klant persoonsgegevens verwerkt die onder de CCPA vallen, zullen we dit doen in overeenstemming met de van toepassing zijnde vereisten van de CCPA. Voor meer informatie over onze naleving van de CCPA, zie GoTo's Privacybeleid en Aanvullende Californische Privacywetgeving voor consumenten.

20.2.3 LGPD

De Braziliaanse Wet Bescherming Persoonsgegevens (LGPD) regelt de verwerking van Persoonsgegevens in Brazilië en/of van personen die zich ten tijde van de verzameling in Brazilië bevinden. GoTo heeft een uitgebreid nalevingsprogramma en voor zover GoTo namens de Klant persoonsgegevens verwerkt die onder de LGPD vallen, zullen wij dit doen in overeenstemming met de toepasselijke vereisten van de LGPD. Ga voor meer informatie naar https://www.goto.com/company/trust/privacy.

20.3 Gegevensverwerkingsaddendum ('DPA')

GoTo biedt een wereldwijd Addendum gegevensverwerking (DPA), dat beschikbaar is in het Engels en Duits. Deze DPA voldoet aan de vereisten voor AVG, CCPA, LGPD en andere van toepassing zijnde regelgeving, en regelt de verwerking van Klantcontent door GoTo.

Specifiek bevat onze DPA verschillende methoden voor AVG-gerichte bescherming van gegevensprivacy, waaronder:

(a) bekendmaking van de details van de gegevensverwerking en subverwerkers zoals vereist krachtens artikel 28;
(b) de (in 2021) herziene Standaardcontractbepalingen (ook bekend als de EU-modelclausules); en
(c) productspecifieke technische en organisatorische maatregelen van GoTo.

Om te voldoen aan de CCPA-vereisten, omvat onze wereldwijde DPA daarnaast:

(a) herziene definities in kaart gebracht aan de hand van de CCPA;
(b) toegangs- en verwijderingsrechten; en
(c) de garantie dat GoTo de persoonlijke informatie van onze klanten, gebruikers en eindgebruikers niet zal verkopen.

Onze wereldwijde DPA bevat ook bepalingen om:

(a) de naleving van de LGPD door GoTo te realiseren;
(b) rechtmatige overdrachten van Persoonsgegevens van en naar Brazilië ondersteunen; en

(c) ervoor zorgen dat onze Gebruikers dezelfde privacyvoordelen genieten als onze andere wereldwijde Gebruikers.

20.4 Overdrachtskaders

GoTo ondersteunt rechtmatige internationale gegevensoverdrachten onder de volgende kaders:

20.4.1 Standaardcontractbepalingen

De Standaardcontractbepalingen ('SCC's'; Standard Contractual Clauses), soms EU-modelclausules genoemd, zijn gestandaardiseerde contractvoorwaarden, die zijn erkend en aangenomen door de Europese Commissie, om ervoor te zorgen dat alle Persoonsgegevens die de Europese Economische Ruimte (EER) verlaten, worden overgedragen in overeenstemming met de EU-wetgeving inzake gegevensbescherming. De SCC's, herzien en uitgegeven in 2021, zijn opgenomen in de wereldwijde DPA van GoTo, om GoTo-klanten in staat te stellen gegevens buiten de EER over te dragen in overeenstemming met de AVG.

20.4.2 Aanvullende maatregelen

Naast de maatregelen die in deze TOM's zijn gespecificeerd, heeft GoTo Veelgestelde vragen en de antwoorden daarop verzameld, om de aanvullende maatregelen te schetsen die zijn geïmplementeerd 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 het gebruik van de SCC's, te bespreken en te begeleiden.

20.4.3 Certificeringen voor de CBPR en PRP van de APEC

GoTo heeft certificeringen behaald 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 aanbieder op het gebied van naleving van gegevensbeveiliging die is goedgekeurd door de APEC.

20.5 Verzoeken om gegevens

GoTo heeft uitgebreide processen ingericht om het ontvangen van verzoeken met betrekking tot gegevensbescherming en beveiliging te vergemakkelijken, waaronder het IRM-portaal, een speciaal privacy-e-mailadres (privacy@goto.com) en de klantenondersteuning op https://support.goto.com.

20.6 Openbaarmakingen van subverwerkers en datacentra

GoTo publiceert openbaarmakingen van subverwerkers in het Trust & Privacy Center (https://www.goto.com/company/trust/resource-center). Deze openbaarmakingen tonen de namen, locaties en verwerkingsdoeleinden van datahostingproviders en andere derden die Klantcontent verwerken als onderdeel van het leveren van de service aan GoTo-klanten.

20.7 Gevoelige gegevens Verwerkingsbeperkingen

Tenzij GoTo hier uitdrukkelijk om heeft verzocht of de klant hierover anderszins schriftelijke toestemming van GoTo heeft ontvangen, mogen de volgende soorten gevoelige gegevens niet naar GoTo Resolve worden geüpload of anderszins aan GoTo worden verstrekt:

- 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.

20.8 Naleving in gereguleerde omgevingen

Klanten zijn zelf verantwoordelijk voor het implementeren van de juiste beleidsregels, procedures en beveiligingsmechanismen wanneer zij GoTo Resolve gebruiken om apparaten in gereguleerde omgevingen te ondersteunen.

21 Mechanismen voor de controle van beveiliging en privacy van derden

Voordat GoTo externe leveranciers inschakelt die Klantcontent of vertrouwelijke, gevoelige of personeelsgegevens verwerken, controleert en analyseert GoTo de beveiligings- en privacyprocedures van de leverancier via geschikte inkoopkanalen. Indien nodig kan GoTo periodiek nalevingsdocumentatie of -rapporten van leveranciers opvragen en evalueren om ervoor te zorgen dat hun controleomgeving en -normen toereikend blijven.

GoTo sluit schriftelijke overeenkomsten met alle externe leveranciers en gebruikt ofwel door GoTo goedgekeurde inkoopsjablonen of onderhandelt over de standaardvoorwaarden van dergelijke derde partijen om aan de door GoTo geaccepteerde privacy- en beveiligingsnormen te voldoen, waar dat nodig wordt geacht. De teams Financiën, Juridische Zaken, Privacy en Beveiliging zijn betrokken bij het beoordelingsproces van verkopers en controleren waar nodig en/of van toepassing of verkopers voldoen aan bepaalde verplichte vereisten voor gegevensverwerking en contractuele vereisten. GoTo's risicobeleid voor derden regelt de privacy- en beveiligingseisen van leveranciers op basis van het type en de duur van de gegevensverwerking en het toegangsniveau. Waar van toepassing (bijv. waar Klantcontent wordt verwerkt of opgeslagen), bevatten overeenkomsten met verkopers vereisten voor "naleving van toepasselijke wetgeving", een DPA, of vergelijkbaar document waarin onderwerpen zoals AVG, CCPA, LGPD en gebruiks- en verkoopbeperkingen worden behandeld. De DPA voor leveranciers van GoTo regelt bijvoorbeeld beperkingen rond het 'verkopen' van gegevens zoals gedefinieerd onder de CCPA. Op dezelfde manier worden met relevante leveranciers beveiligingsaddenda met passende vereisten voor besturingselementen en systemen opgesteld.

22 Contact opnemen met GoTo

Klanten kunnen voor algemene vragen contact opnemen met GoTo op support.goto.com . Voor vragen of verzoeken met betrekking tot Persoonsgegevens of privacy kunt u terecht op ons IRM-portaal of een e-mail sturen naar privacy@goto.com.

23 Terminologie

Online console voor medewerkers: Een online toepassing die op een pc, Mac, Android- of iOS-tablet of Chromebook-apparaat van de medewerker draait in een van de ondersteunde browsers (Chrome, Firefox, Safari) en verbinding maakt met de GoTo Resolve-service. Hiermee kunnen medewerkers GoTo Resolve-sessies aanmaken en uitvoeren, evenals verschillende functies voor accountbeheer, servicebeheer en rapportage.

Desktopconsole voor medewerkers: Een desktoptoepassing die op MacOS en Windows computers draait en verbinding maakt met de GoTo Resolve-service. De Desktopconsole voor medewerkers maakt gebruik van native GoTo Resolve-technologie, Qt en de Chromium-webengine. De desktopconsole biedt dezelfde functionaliteit als de online console voor medewerkers, maar heeft een native look en feel.

Beheerde sessie: Een ondersteuningssessie waarbij de Eindgebruiker aanwezig is tijdens de sessie en eraan kan deelnemen.

Desktopapplicatie voor eindgebruiker: Een desktopapplicatie die op de computer van de eindgebruiker (Windows of Mac) draait en via de GoTo Resolve-service verbinding maakt met een GoTo Resolve-sessie. De applicatie biedt besturing op afstand en andere geavanceerde functionaliteit, evenals de mogelijkheid om App voor onbeheerde eindgebruikers op de computer van de eindgebruiker te installeren.

Eindpunt van Eindgebruiker: Een collectieve term die verwijst naar elk eindpunt voor eindgebruikers, te weten de online app voor Eindgebruikers, de desktopapp voor Eindgebruikers, de mobiele app voor Eindgebruikers, en de app voor onbeheerde eindgebruikers.

Mobiele app voor Eindgebruikers: Een mobiele applicatie (Android en iOS) die op het mobiele apparaat/tablet van de Eindgebruiker draait en via de GoTo Resolve-service verbinding kan maken met een GoTo Resolve-sessie. De app biedt mogelijkheden voor externe weergave (Android en iOS) en besturing op afstand (alleen Android).

Online app voor Eindgebruikers: Een online toepassing die in elke ondersteunde browser op een computer/mobiel apparaat van de eindgebruiker draait en via de GoTo Resolve-service verbinding maakt met een GoTo Resolve-sessie. De app biedt mogelijkheden voor chatten, externe weergave, en het delen van camera's, evenals de mogelijkheid om de sessie op elk moment op afstand te besturen, door de desktopapp voor Eindgebruikers te downloaden of de mobiele app voor Eindgebruikers te installeren.

Mediaservice: Een vloot van load-balanced, wereldwijd verspreide servers die verschillende unicast- en multicast-communicatieservices bieden, met hoge beschikbaarheid en op basis van WebRTC-protocollen.

GoTo Resolve-sessies: Beheerde chat, externe weergave, besturing op afstand, delen van camera's, en onbeheerde besturing op afstand.

GoTo Resolve-service: Een vloot van load-balanced, wereldwijd gedistribueerde servers die veilige toegang bieden tot de online console voor medewerkers en Eindpunten van Eindgebruikers via een versleutelde WebSocket-verbinding en API-aanroepen.

App voor onbeheerde Eindgebruikers: Een installeerbare desktopapplicatie (Windows en iOS) die op de achtergrond op de computer van de Eindgebruiker draait. Met deze app kan de desktopapp voor Eindgebruikers worden gedownload en uitgevoerd om verbinding te maken met een geautoriseerde Onbeheerde sessie.

Onbeheerde sessie: Een ondersteuningssessie waarbij de Eindgebruiker niet aanwezig is. De sessie wordt geïnitieerd en tot stand gebracht door de medewerker, zonder tussenkomst van de Eindgebruiker zelf, via een geautoriseerde app voor onbeheerde Eindgebruikers.

Gebruiker: Personen met subaccounts binnen een klantaccount (zoals medewerkers of beheerders).

GoTo Resolve Ticketing-services: Een back-endtoepassing die de HelpDesk-functie van GoTo Resolve ondersteunt. Deze services zorgen ook voor soepelere communicatie tussen de MS Teams-app en GoTo Resolve.