Technische en organisatorische maatregelen (TOM's)

Rescue en Rescue Lens

Samenvatting

In dit document met Technische en Organisatorische Maatregelen ('TOM's') worden GoTo's privacy-, beveiligings- en verantwoordingsverplichtingen voor Rescue en Rescue Lens 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:* Transparent Data Encryption (TDE) met 256-bits Advanced Encryption Standard (AES) voor Klantcontent.
- **Datacenters:**[1] datacenterlocaties in de Verenigde Staten, Duitsland en Ierland, 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:** Rescue beschikt over SOC 2 Type II, PCI DSS, PCAOB, het 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:**
  - Rescue-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 negentig (90) dagen na het verstrijken van de op dat moment laatst betaalde abonnementstermijn van een Klant automatisch verwijderd.

[1] Hostinglocaties kunnen variëren (d.w.z. afhankelijk van de gekozen verblijfplaats van de gegevens). Raadpleeg de toepasselijke openbaarmaking van subverwerkers van Rescue, 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

Rescue is een online service voor support op afstand, die door technici wordt gebruikt om ondersteuning op afstand te bieden via het internet, zonder dat vooraf geïnstalleerde software nodig is. Met toestemming van de Gebruiker, of een ander persoon die Rescue gebruikt/ support ontvangt van een technicus (Eindgebruiker), geeft Rescue een technicus toegang tot en inzage in en/of controle over de computer van een Eindgebruiker. Door te communiceren via een chatvenster kan de technicus problemen op de computer onderzoeken, diagnosticeren en repareren, of de Eindgebruiker op een andere manier ondersteunen bij probleemoplossing voor zijn besturingssysteem of softwaretoepassingen.

Rescue Lens biedt Eindgebruikers de mogelijkheid om de camera's van hun mobiele apparaat op afstand naar een technicus te streamen (via de mobiele app van Rescue Lens), zodat de technicus op afstand problematische hardware kan bekijken, zoals een verkeerd geconfigureerde router of een beschadigd auto-onderdeel. Rescue Lens is een optionele functie binnen Rescue en kan worden geactiveerd in het Beheerderscentrum van Rescue. Raadpleeg voor meer informatie de gebruikershandleiding van Rescue Lens.

Termen in dit document die met een hoofdletter beginnen maar niet in de tekst worden gedefinieerd, worden gedefinieerd in de Servicevoorwaarden.

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 Rescue en Rescue Lens.

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

Rescue is een SaaS-gebaseerde oplossing (Software-as-a-Service) voor support op afstand, die uit drie hoofdonderdelen bestaat: een technicusconsole, een mobiele app of desktop-applet voor Eindgebruikers en een Beheercentrum.

De technicusconsole is de interface waarmee technici support op afstand kunnen bieden. Technici kunnen nieuwe sessies starten of reageren op online verzoeken van Eindgebruikers die in een gedeelde wachtrij staan. Technici communiceren met en bieden support aan Eindgebruikers via de mobiele app (Android, iOS of Linux) of desktopapplet (Windows of MacOS) van Rescue. De applet wordt gedownload op de externe pc van de Eindgebruiker en is zo ontworpen dat hij zichzelf verwijdert wanneer de sessie eindigt.

De Rescue-technicusconsole communiceert met de Rescue-app of -applet via een peer-to-peer-netwerkverbinding (P2P) (zie afbeelding 1 in sectie 3.1). Wanneer de applet wordt gestart, wordt het P2P-proces geïnitieerd en wordt er verbinding gemaakt met een Rescue-gateway, waar met de technicusconsole wordt onderhandeld over de sessie.

GoTo's eigen protocol voor het doorsturen van sleuteluitwisselingen is ontworpen om de service te beveiligingen tegen het onderscheppen of afluisteren van de GoTo-infrastructuur. Specifiek wordt de verbinding tussen de Eindgebruiker en de host beheerst door de gateway om ervoor te zorgen dat de Eindgebruiker onafhankelijk van de netwerkinstellingen verbinding kan maken met de host.

De host brengt een TLS-verbinding met de gateway tot stand, waarna de gateway de TLS-sleuteluitwisseling van de Eindgebruiker doorstuurt naar de host, via een verzoek om opnieuw te onderhandelen over de eigen sleutel. De Eindgebruiker en de host kunnen zo TLS-sleutels uitwisselen zonder dat de gateway de sleutel te weten komt.

3.1 Sleutelovereenkomst

Wanneer er een supportsessie wordt gestart en er een verbinding is gemaakt tussen de ondersteunde Eindgebruiker en de technicus, moeten hun computers een encryptiealgoritme en een corresponderende sleutel overeenkomen die gedurende de sessie worden gebruikt.

De computers gebruiken certificaten om hun identiteitsgegevens te valideren. Aangezien noch de technicus noch de eindgebruiker software hebben die in staat is om de verbinding tot stand te brengen en de op hun computers geïnstalleerde beveiligingscertificaten en SSL-certificaat te valideren, maken ze beiden gebruik van een van de Rescue-servers om de eerste fase van de sleutelovereenkomst uit te voeren. Door verificatie van het certificaat door zowel de technicusconsole als de applet van de Eindgebruiker, kan alleen een Rescue-server bemiddelen in het proces.

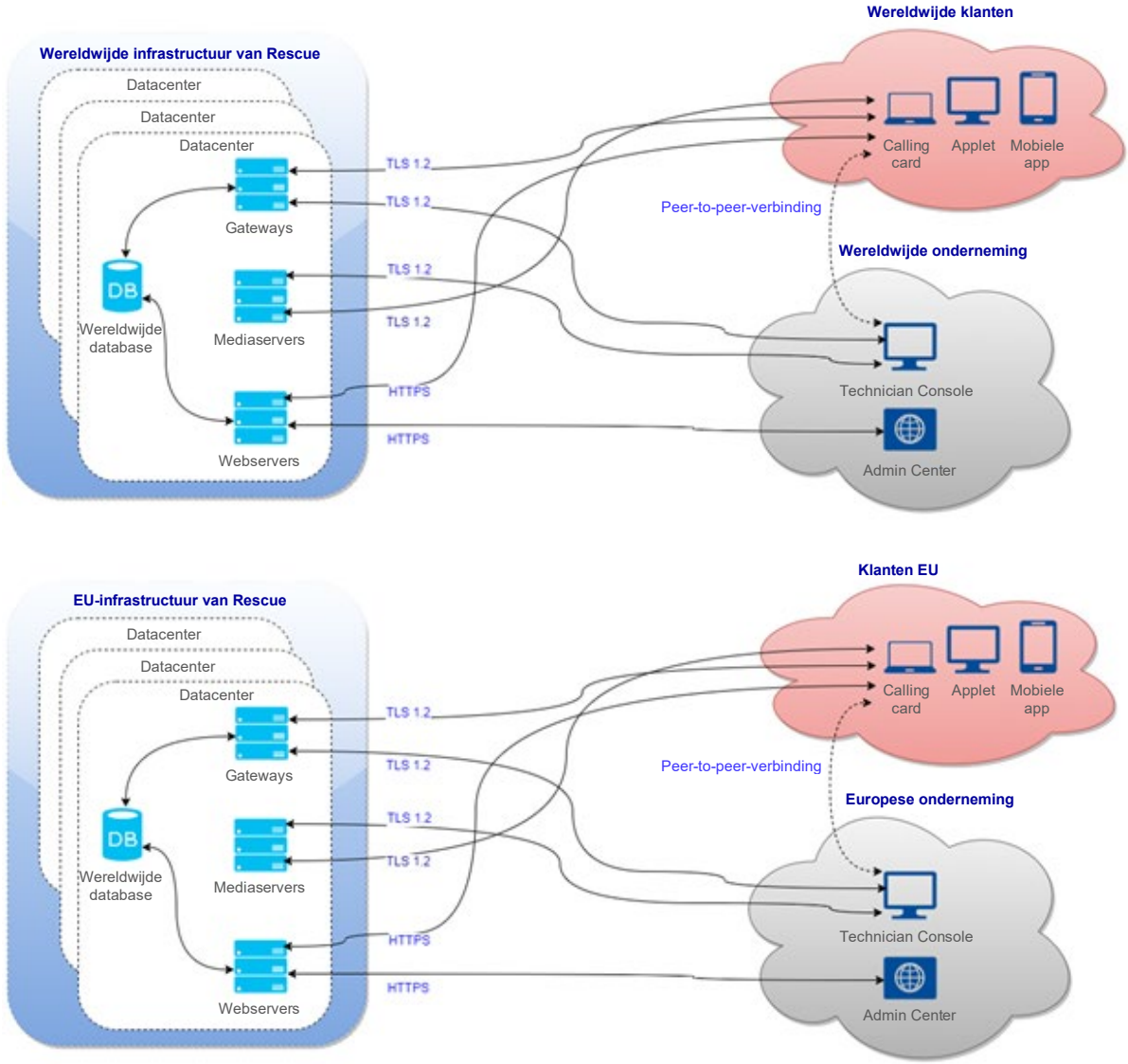
3.2 Overzicht van het hand-offproces van de Rescue-gateway

Wanneer de digitaal ondertekende Rescue-app of -applet op een apparaat wordt gestart, bevat deze een wereldwijd unieke identificatiecode (Globally Unique Identifier; GUID) voor de sessieverificatie. De GUID wordt door de website ingesloten in een uitvoerbare app of applet (bijv. als .exe-bestand) bij het downloaden. De app of applet downloadt dan een lijst met beschikbare gateways van secure.logmeinrescue.com, kiest een gateway uit de lijst, en maakt er verbinding mee via TLS. De gateway wordt vervolgens door de applet geverifieerd met behulp van zijn SSL-certificaat. De gateway verifieert de applet in de database met de GUID en registreert dat de Eindgebruiker op een technicus wacht.

Wanneer een technicus een sessie aanneemt in de Rescue-console, wordt er een aanvraag naar de gateway gestuurd met de GUID voor sessieverificatie om verbindingen tussen de technicusconsole en de app of applet van de Eindgebruiker door te geven. De gateway fungeert als tussenpersoon, en verifieert de verbinding en geeft gegevens door op overdrachtsniveau (wat wil zeggen dat de doorgegeven gegevens niet worden ontsleuteld).

Als een verbindingsrelay wordt gestart proberen de partijen een peer-to-peer-verbinding (P2P) te maken. Het proces verloopt als volgt:

- Het applet zoekt naar een TCP-verbinding (Transmission Control Protocol) op een door Windows of macOS toegewezen poort.
- Als de TCP-verbinding niet kan worden gemaakt binnen 10 seconden, wordt er een poging gedaan om een UDP-verbinding (User Datagram Protocol) te maken met hulp van de gateway.
- Als er een TCP- of UDP-verbinding wordt gemaakt, verifiëren de partijen het P2P-kanaal (met behulp van de sessieverificatie-GUID) en neemt dit het verkeer over van de doorgegeven verbinding.
- Als er een UDP-verbinding is gemaakt, wordt TCP met XTCP (een eigen protocol van GoTo op basis van de BSD-TCP-stack (Berkeley Software Distribution)), geëmuleerd bovenop de UDP-datagrammen.
- Elke verbinding is beveiligd met het TLS-protocol (met AES256-versleuteling met SHA256-MAC (Media Access Controls)). De sessieverificatie-GUID is een 128-bits, cryptografisch willekeurig geheel getal.



Afbeelding 1: infrastructuur van Rescue

3.3 De architectuur van Rescue Media

De Rescue-mediaservice is een op zichzelf staande service op basis van realtime web-communicatie (WebRTC) die de videostreaming van Rescue Lens mogelijk maakt. Deze service beheert de vergaderingen voor Rescue-sessies waarbij de Lens-functie wordt ingezet. Deelnemers aan de vergadering (peers) kunnen vergaderingen binnengaan en verlaten, en Eindgebruikers kunnen video- en audiostreams verzenden, die andere deelnemers kunnen ontvangen. Lens verstuurt videocontent als éénrichtingsstream vanuit de Lens-app naar de technicusconsole.

De mediaservice bestaat uit drie hoofdonderdelen: een softwareontwikkelingspakket voor media (Media Software Development Kit (Media SDK)), de sessiebeheerder, en de streamingsserver. Met deze onderdelen wordt het proces van het aanmaken en verwijderen, en binnengaan en verlaten van vergaderingen beheerd. De onderdelen communiceren via de bestaande beveiligde verbindingen tussen de technicusconsole en de website, en tussen de Lens-app en de website.

3.3.1 Media SDK

De mediaservice is ingericht op basis van WebRTC, met een dunne schil rond de WebRTC-code. De technicusconsole en de mobiele Lens-app gebruiken Media SDK.

3.3.2 Sessiebeheerder

De sessiebeheerder is een eenvoudige load-balanced website met een REST-API (Representational State Transfer) voor het beheren (aanmaken/verwijderen/deelnemen/verlaten) van vergaderingen. De sessiebeheerder accepteert alleen verzoeken van de website.

3.3.3 Streamingsserver

De mediadienst gebruikt de open-source streaming serveroplossing Jitsi om streams tussen peers (de technicusconsole en de Lens-app) af te handelen. De technicusconsole en de Lens-app zijn allebei verbonden met de streamingsserver. Een Lens-sessie heeft twee streams (één wordt verzonden, de andere wordt ontvangen): de Lens-app streamt zijn videocontent omhoog naar de streamingsserver, terwijl de technicusconsole videocontent omlaag streamt vanaf de server. Jitsi fungeert als relayserver tussen de peers.

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 Vertrouwelijkheid van gegevens

Het beveiligde online systeem van Rescue wordt ondersteund door een Secure Sockets Layer en Transport Layer Security (SSL/TLS) en voldoet aan de volgende doelstellingen:

- Verificatie van de communicerende partijen
- Uitwisseling van encryptiesleutels zonder een tussenpersoon die ze kan onderscheppen
- Vertrouwelijke uitwisseling van berichten
- Kunnen detecteren wanneer een bericht tijdens de overdracht is bewerkt

Rescue gebruikt OpenSSL; op het moment van publicatie is de versie die Rescue gebruikt 1.0.2j.

4.2 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.

4.2.1 Versleuteling tijdens de overdracht

Al het netwerkverkeer dat de Rescue-datacenters in en uit gaat, inclusief alle Klantcontent, wordt tijdens de overdracht versleuteld met TLS 1.2 en HTTPS. Daarnaast worden Rescue Support-sessies beveiligd met 256-bits AES-versleuteling en MD5-hash voor betere traceerbaarheid van bestandsoverdrachten.

Aangezien alle drie de onderdelen van het Rescue-communicatiesysteem onder controle van GoTo staan, is de vercijferingsmethode die door deze onderdelen wordt gebruikt altijd dezelfde: AES256-SHA met blokvercijfering en RSA-sleutelovereenkomst. Dat betekent:

- Het AES-algoritme wordt gebruikt voor de versleuteling/ontsleuteling
- De encryptiesleutel is 256 bits lang
- De encryptiesleutels worden uitgewisseld met privé- en algemene RSA-sleutelparen, zoals beschreven in de vorige sectie

- De basis van MAC is SHA-2. Een MAC is een kort stukje informatie dat wordt gebruikt om een bericht te verifiëren. De MAC-waarde beschermt zowel de integriteit van een bericht als de authenticiteit ervan, doordat communicerende partijen alle wijzigingen aan het bericht kunnen detecteren.
- De blokvercijfering zorgt ervoor dat ieder versleuteld tekstblok afhankelijk is van de leesbare tekstblokken tot op dat punt. Soortgelijke berichten kunnen niet worden onderscheiden op het netwerk.

Gegevens die worden overgedragen tussen de ondersteunde gebruiker en de technicus zijn end-to-end versleuteld; alleen de betrokken partijen hebben toegang tot de informatie binnen de berichtenstroom.

4.2.2 Versleuteling tijdens de opslag

Klantcontent in Rescue wordt tijden de opslag versleuteld op zowel server- als databaseniveau met AES256 en TDE. Klantcontent bevat bijvoorbeeld chatlogbestanden en aangepaste velden; dit zijn velden die zijn aangemaakt door de hoofdaccounthouder of hoofdbeheerder.

4.3 Besturingselementen voor toegang tot Rescue

Beheerders van Rescue kunnen de besturingselementen voor toegang aanpassen. Zo kunnen zij een wachtwoordbeleid configureren met een minimaal vereiste wachtwoordsterkte en een maximale wachtwoordleeftijd, het opnieuw instellen van wachtwoorden afdwingen, tweeledige verificatie afdwingen voor aanmeldingen bij Rescue, de toegang van technici tot Rescue beperken tot IP-adressen die vooraf zijn goedgekeurd voor specifieke taken, of technici alleen toegang verlenen tot vooraf gedefinieerde toepassingen met behulp van één enkele SSO-ID voor aanmelding bij die toepassingen. Indien nodig kunnen beheerders de SSO-ID van een technicus uitschakelen.

Aanvullende besturingselementen en controlemaatregelen voor toegang zijn onder meer:

- Op toestemming gebaseerde toegang, die tot op detailniveau kan worden geregeld (bijvoorbeeld om sommige technici toegang te geven tot weergave op afstand (externe weergave) maar niet tot besturing op afstand)
- Geen gegevens van externe apparaten opslaan op GoTo-servers. Alleen sessielogbestanden, IP-adressen van eindgebruikers, en chatlogbestanden worden opgeslagen – chattextlogbestanden kunnen uit de sessiegegevens worden verwijderd
- Voorkomen dat technici bestanden overdragen
- Vereisen dat de Eindgebruiker aanwezig is op het apparaat op afstand, voordat toegang op afstand is toegestaan.
- Vereisen dat de Eindgebruiker de controle behoudt, en de sessie op elk moment kan beëindigen
- Voorkomen dat technici bepaalde functies gebruiken totdat de eindgebruiker hen daartoe expliciet toestemming heeft gegeven (zoals besturing op afstand, bureaubladweergave, bestandsoverdracht, systeeminformatie, opnieuw opstarten en opnieuw verbinding maken)
- Automatische intrekking van toegangsrechten wanneer de sessie wordt beëindigd
- Automatisch afmelden forceren na een bepaalde periode van inactiviteit.
- Een account vergrendelen na vijf mislukte aanmeldpogingen

4.3.1 Toegangscontrole op basis van toestemming

Rescue-beheerders kunnen ook specifieke machtigingen toekennen of weigeren in het beheercentrum. Deze groepsmachtigingen betreffen onder meer:

- Synchronisatie van klembord toestaan
- Delen van schermen met Gebruikers en Eindgebruikers toestaan
- Scripts implementeren
- Bureaubladweergave starten
- Bestandsbeheer starten
- Besturing op afstand starten
- Opnieuw opstarten
- Sessies opnemen
- Aanmeldingsgegevens aanvragen
- Bestanden verzenden en ontvangen
- URL's verzenden
- Privésessies starten
- Sessies overdragen
- Enkele vraag naar alle toegangsrechten gebruiken
- Systeeminformatie bekijken

Raadpleeg de Handleiding voor Beheerders van Rescue voor meer informatie over groepsmachtigingen. Technici van Rescue Lens worden geïdentificeerd aan de hand van hun e-mailadres en geverifieerd met een wachtwoord.

4.3.2 Verificatie

De verificatiemaatregelen voor de beveiliging van Rescue zijn zo ontworpen, dat alleen technici of beheerders zich kunne aanmelden bij het systeem. Technici krijgen van hun beheerders een ID om zich aan te melden (bijvoorbeeld hun e-mailadres) en een bijbehorend wachtwoord. Technici voeren deze aanmeldingsgegevens minimaal aan het begin van hun dienst in op het aanmeldingsformulier op de Rescue website. Beheerders kunnen besturingselementen configureren om verificatie op een frequentere basis te vereisen (bijv. na vijf minuten van inactiviteit).

Het Rescue-systeem wordt eerst geverifieerd op de webbrowser van de technicus met zijn 2048-bits premium RSA SSL-certificaat, om ervoor te zorgen dat de technicus zijn gebruikersnaam en wachtwoord op de juiste website invoert. De technicus meldt zich vervolgens aan bij het systeem met zijn aanmeldgegevens. Rescue slaat geen wachtwoorden op maar gebruikt in plaats daarvan scrypt om hashes van wachtwoorden te maken die vervolgens in de Rescue-database worden opgeslagen. De hashes zijn voorzien van ('gesalt' met) een tekenreeks van 24 tekens, die voor ieder uniek wachtwoord is aangemaakt door CSPRNG.

Het Rescue-systeem wordt ook geverifieerd voor de Eindgebruiker die de support ontvangt. De applet die wordt gedownload en door de gebruiker wordt ondertekend met GoTo's certificaat voor codeondertekening (op basis van een 2048-bits RSA-sleutel). Deze informatie wordt doorgaans in de webbrowser van de gebruiker weergegeven wanneer deze de software gaat uitvoeren. Rescue verifieert de Eindgebruiker niet bij de technicus.

Met Rescue kunnen Beheerders ook een SSO-beleidsregel (Single Sign-On) implementeren. Er wordt gebruikgemaakt van SAML (Security Assertion Markup Language), een XML-standaard (Extensible Markup Language) voor het uitwisselen van verificatie- en autorisatiegegevens tussen beveiligingsdomeinen, dus tussen een identiteitsleverancier en een serviceprovider.

Beheerders kunnen ook tweeledige verificatie vereisen voor het aanmelden bij Rescue. Tweeledige verificatie kan worden uitgevoerd via e-mail of sms, of met een Tijdelijk eenmalig wachtwoord (Time-based One-time Password; TOTP), om een tweede beveiligingslaag aan te brengen voor een Rescue-account. Geselecteerde leden van de organisatie worden hierbij verplicht een extra methode in te stellen om

hun identiteit te verifiëren. Het instellen van de verificatie-app wordt in de volgende gevallen geactiveerd:

- Het geselecteerde lid probeert om zich bij zijn Rescue-account aan te melden op de beveiligde website.
- Het geselecteerde lid probeert zich aan te melden bij de technicusconsole op het bureaublad.
- Het geselecteerde lid probeert zijn Rescue-wachtwoord te veranderen.

4.3.3 Verificatie

Elke supportsessie op afstand wordt minstens één keer geverifieerd. Na het downloaden en uitvoeren van de applet neemt een technicus contact op met de ondersteunde Eindgebruiker. De technicus kan via de applet chatten met de Eindgebruiker, maar voor iedere andere handeling, zoals het verzenden van een bestand of het weergeven van het bureaublad van de Eindgebruiker, is diens expliciete toestemming vereist. De 'Enkele vraag naar alle toegangsrechten' is bedoeld voor langdurige support op afstand, waarbij Eindgebruikers mogelijk niet aanwezig zijn gedurende de hele sessie. Als deze instelling is ingeschakeld voor een technicusgroep, kunnen de technici in deze groep een 'algemene' toestemming aanvragen bij de Eindgebruiker. Als deze wordt verleend, kunnen ze bijvoorbeeld systeeminformatie weergeven, of een sessie met besturing op afstand starten, zonder dat daarvoor toestemming van de Eindgebruiker nodig is. Beheerders kunnen ook IP-adresbeperkingen opleggen zodat technici die aan een bepaalde taak zijn toegewezen alleen vanaf vooraf goedgekeurde IP-adressen toegang hebben tot Rescue en die taak kunnen uitvoeren. De beheerder van een technicusgroep kan ook bepaalde functies in het beheercentrum uitschakelen.

De machtigingen die een beheerder kan verlenen of weigeren zijn onder meer:

- Besturing op afstand starten
- Opnieuw opstarten
- Bureaubladweergave starten
- Sessies opnemen
- Bestanden verzenden en ontvangen
- Privésessies starten
- Bestandsbeheer starten
- Verzoeken om aanmeldingsgegevens
- URL's versturen
- Synchronisatie van klembord toestaan
- Systeeminformatie bekijken
- Scripts uitvoeren
- Eenmalige vragen voor alle toegangsrechten gebruiken
- Sessies overdragen
- Delen van schermen met Gebruikers en Eindgebruikers toestaan

4.4 Interne controlebeheersing

De volgende besturingselementen voor interne controlebeheersing zijn beschikbaar voor Gebruikers en Eindgebruikers van Rescue:

- De optie om het opnemen van sessies te forceren, met de mogelijkheid om bestanden voor de interne controle op een beveiligd gedeeld netwerk op te slaan
- Activiteit van sessies met technici en sessies op afstand worden bijgehouden op de hostcomputer, om de gedegen beveiliging en kwaliteitscontrole te garanderen (gelukte en mislukte aanmeldingen, start- en eindtijd van de besturing op afstand, momenten van opnieuw opstarten, en afmelden)

- Verificatie van persoon of entiteit
- Verificatie van technici met hun unieke e-mailadres of SSO-ID
- Technici alleen toestaan zich laten aan te melden vanaf goedgekeurde IP-adressen

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.

De Rescue-database wordt elke vijf minuten gesynchroniseerd met een ander datacenter. Daarnaast wordt er elke nacht een differentiële back-up gemaakt en worden er elk weekend volledige back-ups gemaakt. De back-updatabase wordt opgeslagen met dezelfde versleuteling als het origineel. Back-ups worden één maand op locatie bewaard en vervolgens geroteerd naar een cloudservice, en niet langer actief verwerkt en bewaard overeenkomstig ons interne beleid voor het bewaren van bestanden. In het geval van een volledige uitval van het datacenter waar de primaire database gehost wordt, is de Rescue-architectuur ontworpen om snel hersteld te worden.

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 Rescue ervoor kiezen om de Europese of wereldwijde gegevensinfrastructuur van GoTo te gebruiken om hun Klantcontent in op te slaan. De hosting- en opslaglocaties zijn hieronder gespecificeerd:[2]

- **Europese Unie:** Duitsland en Ierland
- **Wereldwijd:** de Verenigde Staten

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

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

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.

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** 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.

De chatlogbestanden van Rescue worden opgeslagen in de Rescue-database. Het chatlogbestand wordt door de technicusconsole in realtime overgedragen aan de Rescue-servers, en bevat zowel gebeurtenissen als chatberichten die bij een bepaalde supportsessie horen. Logbestanden geven de volgende handelingen van technici weer: begin- en eindtijd van een op afstand bestuurde sessie, momenten wanneer technici bestanden deelden met Eindgebruikers en metadata met betrekking tot die bestandsdeling (zoals de naam en MD5 Hash-thumbprint van een verzonden bestand). De database met chatlogbestanden kan worden geraadpleegd via het Beheercentrum.

Voor actieve accounts blijft de inhoud van de logbestanden tot twee jaar na het einde van een supportsessie online beschikbaar, en wordt daarna nog twee jaar in het archief bewaard.

Om de integratie met CRM-systemen te faciliteren, kan Rescue sessiegegevens naar een URL posten, en beheerders kunnen ervoor kiezen om chattekst van deze gegevens uit te sluiten. Chattekst is standaard inbegrepen bij de overdracht, maar Klanten kunnen die instelling wijzigen in het beheercentrum. Bovendien kunnen alle registraties van chatteksten tussen technici en Eindgebruikers automatisch worden weggelaten uit de sessiegegevens die zijn opgeslagen in een Rescue-datacenter. Rescue staat technici toe om de gebeurtenissen die zich voordoen tijdens een bureaubladweergave of een op afstand bestuurde sessie in een videobestand op te nemen. De opnamebestanden worden in een map opgeslagen die door de technicus wordt opgegeven.

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 van GoTo

Er zijn procedures ingericht voor logische toegangscontrole om het risico van onbevoegde toegang tot toepassingen en gegevensverlies in bedrijfs- en productieomgevingen te beperken. GoTo-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.

15 Scheiding van gegevens

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

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 systeem- en configuratiebestanden om ongeoorloofde wijzigingen te voorkomen of de kans daarop te verkleinen;

- Webtoepassingsfirewall (WAF) en DDoS-preventieservice met toepassingslaag, waardoor GoTo-verkeer via een proxy loopt om kwaadwillig serververkeer te blokkeren
- Een firewall voor lokale toepassingen die een extra beschermingslaag biedt tegen de top tien van OWASP, en andere kwetsbaarheden van webtoepassingen en kwaadaardig verkeer
- Hostgebaseerde firewalls op GoTo-webservers die inkomende en uitgaande verbindingen filteren, inclusief interne verbindingen tussen GoTo-systemen

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 Rescue, 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.logmeinrescue.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: Tenzij anders vereist door de toepasselijke wetgeving, wordt Klantcontent automatisch verwijderd na negentig (90) 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.

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 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 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.

20.6 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.

20.7 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.

20.8 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 Rescue 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.

20.9 Naleving in gereguleerde omgevingen

Klanten zijn zelf verantwoordelijk voor het implementeren van de juiste beleidsregels, procedures en beveiligingsmechanismen wanneer zij Rescue 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 privacy-procedures 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 gegevens-verwerking 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. Op dezelfde manier worden met relevante leveranciers beveiligingsaddenda met passende vereisten voor besturingselementen en systemen opgesteld. De DPA voor leveranciers van GoTo regelt beperkingen rond het 'verkopen' van gegevens zoals gedefinieerd onder de CCPA.

22 Contact opnemen met GoTo

Klanten kunnen contact opnemen met GoTo op https://support.goto.com voor algemene vragen. 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.