Technische en organisatorische maatregelen (TOM's)
GoTo Meeting, GoTo Webinar, GoTo Training en GoTo Stage

Samenvatting

Dit document met technische en organisatorische maatregelen ("TOM's") beschrijft de privacy-, beveiligings- en verantwoordingsverplichtingen van GoTo voor GoTo Meeting, GoTo Webinar, GoTo Training en GoTo Stage. GoTo heeft 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) of Datagram Transport Layer Security (DTLS)
  - *Tijdens de opslag:* Transparent Data Encryption (TDE) en Advanced Encryption Standard (AES) 256-bits voor Klantcontent die wordt versleuteld tijdens de opslag.
- **Datacenters:** GoTo maakt gebruik van cloudhostingproviders die maatregelen nemen voor een hoge logische en fysieke beveiliging, beschikbaarheid en schaalbaarheid.
- **Nalevingsaudits:** GoTo Meeting, GoTo Webinar en GoTo Training beschikken over SOC 2 Type II, BSI C5, PCI DSS, PCAOB, TRUSTe-certificaat inzake privacy van ondernemingen en APEC- CBPR- en PRP-certificeringen.
- **Naleving van wet- en regelgeving:** GoTo heeft een uitgebreid gegevensbeschermingsprogramma met processen en beleidsregels die ervoor zorgen dat de Klantcontent wordt behandeld in overeenstemming met de toepasselijke privacywetgeving, waaronder de AVG, CCPA/CPRA en LGPD.
- **Beveiligingsbeoordelingen**: Naast interne tests sluit GoTo contracten af met externe bedrijven om regelmatig beveiligingsbeoordelingen en/of penetratietests uit te voeren.
- **Logische besturingselementen voor toegang:** Er zijn logische besturingselementen voor toegang geïmplementeerd, ingericht om ongeautoriseerde toegang tot toepassingen en gegevensverlies in bedrijfs- en productieomgevingen te voorkomen of te beperken.
- **Scheiding van gegevens**: GoTo maakt gebruik van een architectuur met meerdere tenants en scheidt klantaccounts logisch op het opslagniveau.
- **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.
- **Gegevens bewaren**
  - Klanten van GoTo Meeting, GoTo Webinar, GoTo Training en GoTo Stage kunnen te allen tijde verzoeken om retournering of verwijdering van klantinhoud, waaraan binnen dertig (30) dagen na het verzoek van de klant zal worden voldaan.
  - Klantcontent wordt Voor GoTo Meeting, GoTo Webinar en GoTo Training automatisch verwijderd tussen negentig en honderd (90-100) dagen na het verstrijken van de op dat moment laatst betaalde abonnementstermijn van een Klant.

Inhoudsopgave

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

1 Productintroductie

GoTo Meeting, GoTo Webinar, GoTo Training en GoTo Stage (samen de "Service") zijn online communicatieservices waarmee personen en organisaties kunnen communiceren met behulp van een uitgebreide functionaliteit, waaronder, afhankelijk van het serviceaanbod, het delen van computerschermen, videovergaderingen, en geïntegreerde audio. GoTo Meeting, GoTo Webinar, GoTo Training en GoTo Stage delen infrastructuur en worden via een CDN geleverd aan webbrowsers of installeerbare toepassingen.

- GoTo Meeting, GoTo Webinar en GoTo Training stellen organisatoren in staat om online sessies te plannen, bijeen te roepen en te modereren, inclusief audio, webcam, schermdeling en meer met behulp van de web-, desktop- en mobiele toepassingen van GoTo.
- GoTo Training biedt specifieke voorzieningen voor webtrainingen, zoals online toegang tot toetsen en materialen, en een gehoste cursuscatalogus.
- Met GoTo Webinar kunnen organisaties online presentaties geven aan lokale en/of wereldwijde deelnemers.
- GoTo Stage is een uitbreiding van GoTo Webinar waar organisatoren van GoTo Webinar aanpasbare kanalen kunnen maken en hun webinaropnamen kunnen publiceren. Gepubliceerde opnames worden weergegeven op de GoTo Stage-homepage, gesorteerd naar categorie. Organisatoren kunnen op ieder gewenst moment hun in GoTo Webinar gepubliceerde opnamen verwijderen. De video wordt dan zowel verwijderd van hun kanaalpagina als uit het systeem van GoTo Stage.

1.1 Conferentiebeheer en registratie

Organisatoren kunnen sessies direct in de Service plannen. Ze kunnen verschillende instellingen van komende sessies aanpassen en hun inhoud en deelnemers voorbereiden.

1.2 Audio

Geïntegreerde audioconferenties voor GoTo Meeting, GoTo Webinar en GoTo Training sessies zijn beschikbaar via Voice over Internet Protocol (VoIP) en het openbare telefoonnetwerk (PSTN).

1.3 Video

Alle producten bieden webcamvideo van hoge kwaliteit die zich aanpast aan de bandbreedte en latentie van de gebruiker.

1.4 Inhoud uploaden (alleen GoTo Webinar en GoTo Training)

Organisatoren kunnen bestanden en media uploaden voor gebruik tijdens sessies, zowel voorafgaand aan een sessie als tijdens de sessie.

1.5 Sessies vastleggen

Organisatoren kunnen deelnamestatistieken en andere sessiestatistieken bekijken in hun sessiegeschiedenis.

1.6 Opnamen en transcripties

Sessies kunnen lokaal en in de cloud worden opgenomen. Accountbeheerders en sessie-organisatoren kunnen ervoor kiezen om cloudopnamen in te schakelen naast of in plaats van lokale opnamen. Lokale opnamen worden opgeslagen op het systeem van de organisator en zijn niet onderhevig aan de bewaarbeperkingen van GoTo, zoals uiteengezet in Sectie 18 (Verwijderen en retourneren van Content) hieronder.

Cloud-opnamen zijn automatisch direct beschikbaar in de sessiegeschiedenis van de organisator en transcripties worden automatisch aangemaakt als deze functie is ingeschakeld door de beheerder. Transcripties van sessieopnamen worden gemaakt met behulp van de GoTo Voice AI of Google Cloud Speech-to-Text technologie.

Voor **GoTo Meeting** kan een accountbeheerder ervoor kiezen om opnamen in te schakelen en te beslissen of deze lokaal of in de cloud worden opgeslagen. Als cloud-opnamen zijn ingeschakeld, kan de organisator van de vergadering ervoor kiezen om een bepaalde vergadering op te nemen en in de cloud op te slaan. Voor cloudopnamen worden automatisch transcripties gemaakt.

Voor **GoTo Webinar** kunnen organisatoren ervoor kiezen om alle opnamen in de cloud automatisch te transcriberen. Alleen een organisator kan een opname starten en als de instelling voor automatisch transcriberen is ingeschakeld, wordt er een transcript gemaakt.

Voor **GoTo Training** kunnen accountbeheerders bepalen of organisatoren opnamen in de cloud kunnen opslaan. Accountbeheerders kunnen niet voorkomen dat organisatoren sessies lokaal opnemen. Trainingen kunnen niet worden getranscribeerd.

1.7 Business Messaging (alleen in GoTo Meeting)

Als uitbreiding van GoTo Meeting kunnen gebruikers van GoTo Meeting met Business Messaging de aanwezigheidsstatus van andere gebruikers binnen hun account zien, chatberichten uitwisselen en bestanden delen. De accountbeheerder definieert het bereik voor zichtbaarheid en traceerbaarheid van verschillende gebruikers.

Gebruikers van Business Messaging kunnen de aanwezigheidsstatus van elke andere gebruiker binnen hun account zien zodra deze is opgenomen in hun contactlijst. Berichten kunnen worden uitgewisseld met alle leden van een team en met externe gebruikers als zij expliciet zijn uitgenodigd via een e-mailuitnodiging. Externe gebruikers zijn gebruikers van Business Messaging die geen lid zijn van het interne team van een Klant (bijv. klant, prospect of partner). Berichten kunnen rechtstreeks zijn (tussen twee deelnemers), in een privégroep of in een openbare groep.

Gebruikers kunnen ook andere inhoud delen binnen Business Messaging door bestanden te uploaden en te downloaden. De gedeelde bestanden kunnen worden gedownload door alle gebruikers met toegang tot de berichten in een bepaald gesprek of bepaalde groep.

1.8 Webcast (alleen GoTo Webinar)

GoTo Webinar webcasts maken gebruik van broadcast gateways, streaming engines van derden en content delivery netwerken die ontworpen zijn om op betrouwbare wijze media voor schermdeling, audio en video te leveren aan deelnemers die deelnemen vanuit een webbrowser. De gateways ontvangen mediagegevens van de mediaservers en transcoderen deze naar standaard codecs. De streaming engine produceert HTTP Live Streaming (HLS) op meerdere bitrates om adaptieve levering mogelijk te maken voor gebruikers met suboptimale netwerkverbindingen.

1.9 GoTo Stage (alleen bij GoTo Webinar)

Video's die op GoTo Stage gepubliceerd zijn, kunnen ontdekt worden op de startpagina van GoTo Stage en in de resultaten van zoekmachines, tenzij de organisator de vindbaarheid beperkt via de beheerinstellingen op zijn chatroompagina. Niet-ontdekbare opnamen zijn toegankelijk voor iedereen die geregistreerd is bij GoTo Stage via een directe URL naar het kanaal of naar de unieke "Watch Now"-pagina van de video. Bezoekers registreren zich voor GoTo Stage met hun naam en e-mailadres of kunnen verbinding maken via bepaalde sociale media-accounts zoals LinkedIn, Facebook en Gmail. De URL's voor bezoekers om video's op te roepen, zijn voor een beperkte tijd live om ongewenst delen te beperken.

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 Meeting, GoTo Webinar, en GoTo Training.

GoTo's implementatie van beveiligingen, functies en praktijken omvat:

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. Waarborgen dat er privacypraktijken zijn om de verwerking en het beheer van gegevens te regelen in overeenstemming met de GDPR, CCPA/CPRA, LGPD en onze eigen Data Processing Addendum (DPA), evenals toepasselijk GoTo beleid en openbare bekendmakingen.

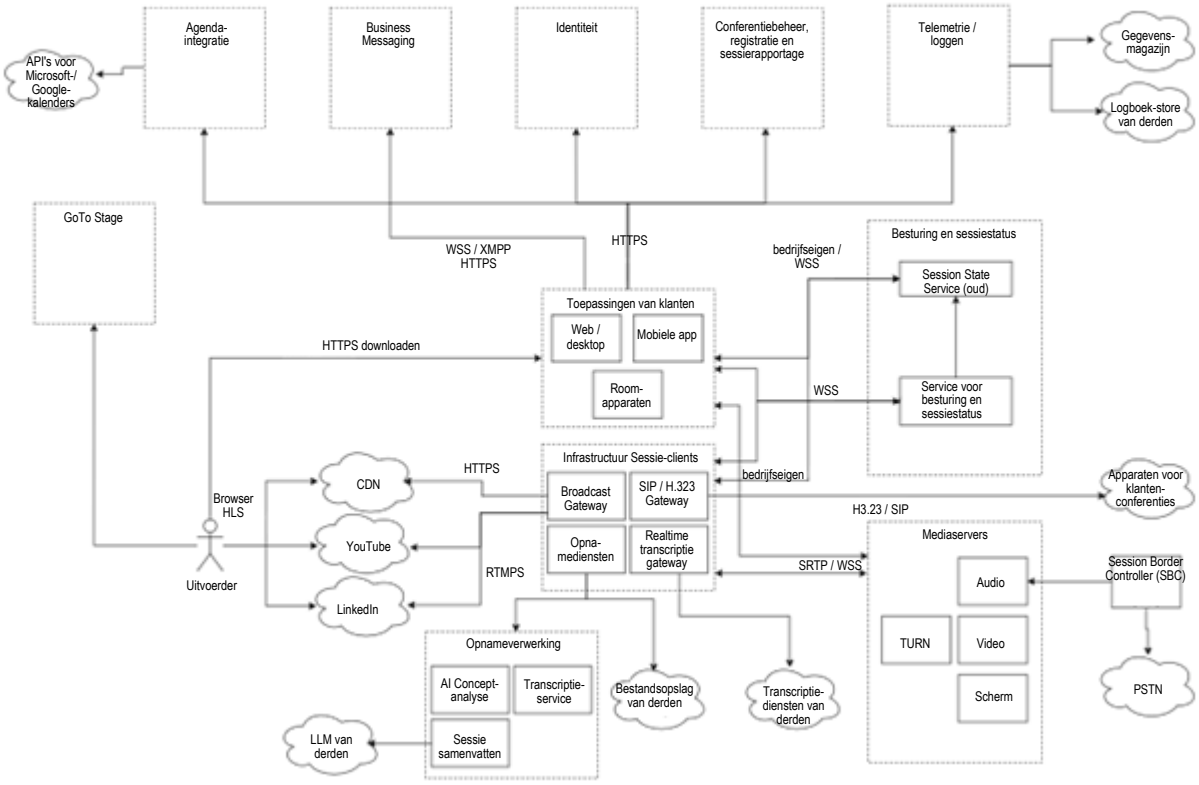
We ontwikkelen producten met beveiligingsmechanismen aan de basis, om Klantcontent van GoTo optimaal tegen bedreigingen te beschermen en ervoor te zorgen dat de voor beveiliging ingerichte besturingselementen ook echt geschikt zijn voor de aard en reikwijdte van de services. Beveiligingsfuncties die in de service geconfigureerd kunnen worden, helpen beheerders om bedreigingen en risico's voor Klantinhoud te minimaliseren.

3 Productarchitectuur

GoTo Meeting, GoTo Webinar, GoTo Training en GoTo Stage zijn Software as a Service (SaaS)-oplossingen die zijn ontworpen voor hoge prestaties, betrouwbaarheid, schaalbaarheid en beveiliging. Deze Services worden ondersteund door servers en netwerkapparatuur met hoge capaciteit, met passende beveiligingsmechanismen en redundante infrastructuur die ontworpen is om single points of failure uit te sluiten. Er zijn geclusterde servers en back-upsystemen aanwezig om applicatieprocessen te ondersteunen in het geval van een zware belasting of systeemstoring.

Applicatie/serversessies worden gebalanceerd over geografisch verspreide clusters die ontworpen zijn om prestaties en voldoende latentie te garanderen.

De infrastructuur en gegevens van de service worden gehost door cloudhostingproviders.



Afbeelding 1: Centrale architectuur

Klanttoepassingen (GoTo web-, desktop- en mobiele toepassingen of "clients"; een apparaat met de naam GoTo Room (alleen bij GoTo Meeting)): De Klanttoepassingen bieden de functionaliteit van de Service zoals hierboven beschreven in Sectie 1 (Productintroductie).

Identiteitsdiensten: Beheert gebruikersaccounts en maakt veilige en gestandaardiseerde accountautorisatie en aanmelding mogelijk.

Diensten voor conferentiebeheer, registratie en sessierapportage: Conferentiebeheer biedt informatie over geplande sessies en maakt het mogelijk om nieuwe sessies te plannen en bestaande sessies aan te passen. Registratiediensten maken registratie mogelijk voor sessies waar dit vereist is. Sessierapportage biedt informatie over eerdere sessies, inclusief opnamen, transcripties, aanwezigheid en meer.

Business Messaging: Beheer van kanalen en verzenden, ontvangen en opslaan van berichten en bijlagen; alleen gebruikt voor messaging buiten sessies om.

Agenda-integratie: Hiermee kunnen gebruikers hun Microsoft Outlook- of Google-agenda's synchroniseren om meldingen over GoTo-sessies te krijgen.

Telemetrie/Logging: Versturen van telemetriesondes of logverklaringen om gebruiksstatistieken te verzamelen en problemen te diagnosticeren.

Diensten voor besturing en sessiestatus: Leveren functionaliteit die gebruikt wordt door clienttoepassingen om niet-mediagerelateerde wijzigingen van de sessiestatus te initiëren en te ontvangen.

Mediaservers: Verantwoordelijk voor het ontvangen, wijzigen en distribueren van audio, video en inhoud voor schermdeling.

PSTN: Openbaar telefoonnetwerk stelt gebruikers in staat om in te bellen op sessies via fysieke of IP-telefoons.

Session Border Controller: Verbindt GoTo's Voice over Internet Protocol (VoIP) met commerciële telefonieaanbieders.

Opnamediensten: Maakt het opnemen van sessie-audio, video, schermdeling en Business Messaging mogelijk.

Broadcast Gateway: Wordt gebruikt voor GoTo Webinar Webcasts en ondersteunt lay-out, transcodering en packetizing van de mediastreams in HLS-streams, die via CDN naar browsergebaseerde clients gedistribueerd worden of naar RTMP-gebaseerde streaming-platforms zoals YouTube of LinkedIn geduwd worden.

H.323-/SIP-Gateway: Maakt verbinding mogelijk met sessie-audio via SIP- of H.323-conferentieapparaten.

Realtime Transcriptie (RTT) Gateway: Biedt live transcriptie van de spraak van deelnemers aan een sessie.

GoTo Stage-services: Beheer van GoTo Webinar video-inhoud door organisatoren; biedt bezoekers kijkervaring.

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 implementeert beveiligingsmaatregelen voor gegevens tijdens de overdracht, die ontworpen zijn om te beschermen tegen passieve en actieve aanvallen op vertrouwelijkheid, integriteit en beschikbaarheid. Maatregelen voor communicatiebeveiliging worden geïmplementeerd voor scherm- en videodeling, VoIP, webcamvideo, toetsenbord-/muisbediening, tekstgebaseerde chatinformatie en andere sessiegegevens.

GoTo gebruikt TLS-protocollen met Internet Engineering Task Force (IETF)-standaard om TCP-communicatie tussen eindpunten te beschermen.

HTTPS en WSS worden gebruikt om niet-mediagegevens te beschermen, terwijl mediagegevens in de sessie worden beschermd door SRTP, WSS of DTLS.

Intern gebruikt GoTo ook op wederzijdse certificaten gebaseerde verificatie (mTLS) op servers die mediagegevens verwerken.

4.1.1.1 Audio- en videobeveiliging

Om de vertrouwelijkheid en integriteit van VoIP-verbindingen tussen de eindpunten en servers te beschermen, wordt een protocol op basis van SRTP gebruikt dat werkt met standaard coderingsmechanismen met minimaal AES128.

4.1.1.2 Beveiliging van websites, API's en interne webservices

Alle verbindingen met de websites, API's en interne webservices van de Service zijn beveiligd met TLS. Dit omvat onder andere Inhoud uploaden, Sessierapportage, Opnamen en transcripties.

4.1.1.3 Business Messaging

Aanwezigheidsupdates, berichten en bestanden worden via een TLS-beveiligd kanaal verzonden naar chatdiensten en verder naar gebruikers. De inhoud wordt beschikbaar gemaakt via cryptografisch ondertekende URL's met een link naar de inhoud.

4.1.1.4 Webcast-beveiliging (alleen voor GoTo Webinar)

Webcast streaming gateways sturen het verkeer door naar de streaming engine via SRTP, allemaal binnen het beveiligde interne netwerk van GoTo. CDN's halen gegevens veilig via HTTPS op van de streaming engine. De clients halen ook veilig gegevens op van CDN's via HTTPS.

4.1.2 Versleuteling tijdens de opslag

4.1.2.1 Profielgegevens

De inhoud wordt opgeslagen in een relationele database met AES 256-bits versleuteling.

4.1.2.2 Conferentiebeheer, Registratie en Sessierapportage

De inhoud wordt opgeslagen in een relationele database met AES 256-bits versleuteling.

4.1.2.3 Uploaden van content

Geüploade content en gerelateerde metadata worden opgeslagen in AWS S3, Amazon Aurora en Amazon Dynamo DB, allemaal met AES 256-bits versleuteling. Hiernaast worden metadata in Apache Cassandra opgeslagen zonder versleuteling tijdens de opslag.

4.1.2.4 Opnamen en transcripties

Opnamen in de cloud worden opgeslagen in AWS S3. Bestanden worden in rust versleuteld met server-side versleuteling met AES256.

Audiobestanden voor transcriptie worden versleuteld met AES256 en onmiddellijk verwijderd nadat de spraak-naar-tekstverwerking is voltooid.

4.1.2.5 Beveiliging van Business Messaging

Berichten worden opgeslagen in een AWS Aurora-database en gedeelde bestanden worden opgeslagen in AWS S3, beide met AES 256-bits versleuteling voor de opslag.

4.1.2.6 GoTo Stage

Deze geüploade inhoud en gerelateerde metagegevens worden opgeslagen in AWS S3 met AES 256-bits versleuteling. De metadata worden opgeslagen in Apache Cassandra en de zoekindex in Elasticsearch, beide niet versleuteld in rust.

4.2 Compatibiliteit met firewalls en proxy's

De Service bevat ingebouwde logica voor proxydetectie en verbindingsbeheer om de software-installatie te automatiseren, de noodzaak voor complexe netwerk(her)configuratie te vermijden en de productiviteit van de gebruiker te maximaliseren. Firewalls en proxy's die al aanwezig zijn in het netwerk van een gebruiker, hebben over het algemeen geen speciale configuratie nodig om gebruik te kunnen maken van de Service.

Voor meer details, en de exacte domeinen, IP's en poorten die gebruikt worden, bezoekt u de respectievelijke ondersteuningspagina's voor Meeting, Webinar en Training.

4.3 Beveiligingsfuncties voor installeerbare clients

De installeerbare clients zijn ontworpen met passende beveiligingsfuncties en maken gebruik van sterke cryptografische maatregelen, waaronder ondertekende eindpuntsoftware en "client-only" verbindingen.

4.3.1 Ondertekende eindpuntsoftware

De uitvoerbare bestanden van de service zijn digitaal ondertekend voor integriteitsbescherming en authenticiteit. De software voor clienttoepassingen van GoTo volgt passende procedures voor kwaliteitscontrole, configuratiebeheer en een SDL-model (Security Development Lifecycle) tijdens de ontwikkeling en implementatie.

4.3.2 "Client-only" Verbindingen

Om het risico te verkleinen dat systemen op afstand ze kunnen aanvallen met malware en virussen, zijn de installeerbare clients niet geconfigureerd om inkomende verbindingen te ontvangen. Dit helpt gebruikers die deelnemen aan een sessie te beschermen tegen infectie door een gecompromitteerde host, die door een andere deelnemer wordt gebruikt.

4.3.3 Implementatie cryptografisch subsysteem

Cryptografische functies en beveiligingsprotocollen die geïmplementeerd zijn in de installeerbare clients, maken gebruik van de open source BoringSSL of OpenSSL cryptografische bibliotheken. Er zijn geen externe API's blootgesteld waarmee andere software toegang zou kunnen krijgen tot de cryptografische bibliotheken die in de client gebundeld zijn.

De webtoepassing gebruikt de cryptografische bibliotheken van de browser. Er zijn geen cryptografische instellingen die door de eindgebruiker geconfigureerd kunnen worden, zodat deze ook niet per ongeluk of opzettelijk verkeerd geconfigureerd kunnen worden.

4.4 Verificatie van gebruikers

Rolgebaseerde autorisatie en gepaste toegangscontroles zijn afhankelijk van de mogelijkheid om gebruikers te identificeren en verifiëren. Om ervoor te zorgen dat organisatoren en deelnemers passende rechten hebben, zijn er account- en sessieverificatiefuncties opgenomen in de Service.

4.4.1 Aanmelding bij een account

De Servicewebsites bieden de volgende aanmeldingsmethoden:

- Direct aanmelden met gebruikersnaam en wachtwoord;

- Aanmelden via een sociale of andere accountprovider met LastPass, Google, Facebook, LinkedIn, Microsoft of Apple. (https://support.goto.com/meeting/help/connect-your-social-or-other-account-for-sign-in); en
- SAML-gebaseerde single sign-on.

Voor direct aanmelden hebben alle wachtwoorden minimale teken- en complexiteitsvereisten. Er zijn mechanismen aanwezig om bescherming te bieden tegen brute-force aanmeldingsaanvallen en ongebruikelijke aanmeldingsactiviteit.

GoTo slaat accountwachtwoorden niet op in platte tekst. In plaats daarvan worden wachtwoorden opgeslagen met een salted cryptografische hashfunctie die ontworpen is om bestand te zijn tegen woordenboek- en brute force-aanvallen. Wachtwoorden worden via beveiligde verbindingen (TLS) verzonden.

4.4.2 Verificatie van sessiedeelnemers

Om sessies met beperkte een beperkt publiek mogelijk te maken, heeft elke sessie een uniek en willekeurig ID. Organisatoren kunnen er ook voor kiezen om deelnemers een wachtwoord te vragen om deel te kunnen nemen aan een sessie.

Om aan een sessie deel te nemen, moeten deelnemers de unieke ID opgeven door op een URL te klikken die de ID bevat of door de waarde handmatig in te voeren op een formulier dat door de Service wordt aangeboden. Bij het inbellen per telefoon moeten deelnemers de ID invoeren via de telefoontoetsen. Als de ID geldig is, krijgt elke deelnemer een roltoken dat vervolgens tijdens het toetredingsproces aan de communicatieservers wordt aangeboden.

4.4.3 Rolgebaseerde toegangscontrole

Toepassingsgedefinieerde rollen kunnen worden toegewezen aan servicegebruikers en ondersteunen klanten bij het afdwingen van het toegangsbeleid van het bedrijf met betrekking tot het gebruik van services en functies. Gebruikers hebben toegang tot besturingselementen en privileges op basis van de aan hen toegewezen rol:

Organisatoren (of trainers voor GoTo Training) zijn gemachtigd om vergaderingen, webinars en/of trainingssessies te plannen. Een organisator kan sessies plannen, deelnemers uitnodigen, de sessie starten en beëindigen en de huidige presentator aanwijzen.

Deelnemers zijn mensen die worden uitgenodigd om een sessie bij te wonen. Deelnemers kunnen het gedeelde scherm van de presentator bekijken, chatten met andere deelnemers en de deelnemerslijst bekijken.

Presentatoren zijn aanwezigen die hun scherm met andere aanwezigen kunnen delen. Presentatoren kunnen andere aanwezigen ook gedeelde controle over hun toetsenbord en muis geven.

Beheerders zijn personen die gemachtigd zijn om een account voor meerdere gebruikers te beheren. Externe beheerders kunnen accountfuncties configureren, organisatoren autoriseren en allerlei rapportagetools gebruiken.

Interne beheerders van GoTo zijn medewerkers van GoTo die gemachtigd zijn om GoTo Meeting-, GoTo Webinar- en GoTo Training-services en -accounts namens onze klanten te beheren.

4.5 Toegangscontrole voor opnamen

Organisatoren kunnen hun opnames na afloop van de sessie eenvoudig delen met deelnemers via unieke, directe links. Deelnemers kunnen de opname afspelen in hun browser.

Voor GoTo Webinar verlopen de URL's voor het delen niet, zolang de opname beschikbaar is. Om de toegang tot een opname uit te schakelen, kunnen organisatoren de opname op elk gewenst moment verwijderen.

Voor GoTo Meeting kunnen opnamen gedeeld worden via URL's die een willekeurig token met beperkte geldigheid gebruiken. Delen kan beperkt worden tot bepaalde delen van de inhoud, en kan beschikbaar zijn voor iedereen met de URL of alleen voor gebruikers met configureerbare e-mailadressen. Deze beperkingen kunnen worden aangepast, zelfs nadat de URL is gedeeld.

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 één enkel storingspunt te verminderen door gebruik te maken van datacenters van cloudhostingproviders.

Voor details over de leverancier en locatie van datacenters raadpleegt u het document Sub-Processor Disclosure (Openbaarmaking van subverwerkers) in GoTo's Trust & Privacy Center.

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

7.1 Fysieke beveiliging datacenters

Cloudhostingproviders bieden fysieke beveiliging en omgevingscontroles voor systemen en servers die Klantinhoud 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.

Cloudhostingproviders beperken de fysieke toegang tot productiedatacenters tot bevoegde personen. Voor toegang tot serverruimten moet een aanvraag worden ingediend via het relevante ticketingsysteem en moet deze worden goedgekeurd door de betreffende manager. Alle fysieke toegang tot datacenters en serverruimtes wordt tot een minimum beperkt, geregistreerd en minstens elk kwartaal door de providers gecontroleerd. 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, 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 klanteninhoud tussen APEC-lidstaten, verkregen en onafhankelijk gevalideerd via TrustArc, een door APEC goedgekeurde derde partij die toonaangevend is op het gebied van compliance met gegevensbescherming. Klik hier voor meer informatie over onze APEC-certificeringen.
- **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 hanteert beleidsregels en procedures voor loggen, bewaken en waarschuwen, waarin de principes en controles worden beschreven die worden uitgevoerd om ons vermogen om verdachte activiteiten te detecteren en tijdig te reageren, te versterken. 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 (Endpoint Detection and Response (EDR)), 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 kwetsbaarheden en beheer van patches

GoTo onderhoudt een formeel patchbeheerprogramma en voert minstens elk kwartaal patchbeheeractiviteiten uit op alle relevante systemen, apparaten, firmware en besturingssystemen die Klantinhoud verwerken. GoTo beoordeelt en scant op kwetsbaarheden op systeemniveau, host/netwerk ("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.

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 controles geïmplementeerd om te voorkomen dat gebruikers of eindgebruikers de gegevens van andere gebruikers kunnen zien.

16 Perimeterbescherming en inbraakdetectie

GoTo gebruikt perimeterbeschermingstools, -technieken en -services om te beschermen tegen ongeautoriseerd netwerkverkeer dat de productinfrastructuur van GoTo binnenkomt. Deze omvatten, maar zijn niet beperkt tot:

- Intrusiedetectiesystemen die systemen, diensten, netwerken en toepassingen monitoren op ongeautoriseerde toegang;
- Kritische systeem- en configuratiebestandsbewaking;
- Cloudnetwerk-firewalls die inkomende en uitgaande verbindingen filteren, inclusief interne verbindingen tussen GoTo-systemen; en
- 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 services, inclusief Central en Pro, 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 retournering: Klanten kunnen verzoeken om teruggave en/of verwijdering van hun klanteninhoud door een verzoek in te dienen via GoTo's Individual Rights Management Portal ("IRM"), 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.

Bewaarschema voor Klantinhoud: Tenzij anders vereist door de toepasselijke wetgeving, wordt Klantinhoud automatisch getagd voor verwijdering binnen negentig (90) dagen en succesvol verwijderd binnen honderd (100) dagen na beëindiging, annulering of afloop en, in elk geval, deprovisionering van het op dat moment laatste abonnement van de Klant. Op schriftelijk verzoek kan GoTo een schriftelijke bevestiging/verklaring van verwijdering van inhoud geven.

De bovenstaande tijdlijnen zijn van toepassing op alle Services, en aanvullende Service-specifieke verwijderingstijdlijnen worden hieronder uiteengezet:

GoTo Meeting

Tijdens abonnementstermijn: De geschiedenis van GoTo Meeting-sessies en opnamen in de cloud worden automatisch verwijderd op voortschrijdende basis van één (1) jaar tijdens de actieve abonnementstermijn van de klant, voor zowel betaalde als gratis accounts.

Na afloop van het abonnement: Na afloop van een betaald abonnement op GoTo Meeting worden de accounts van de klant die een gratis licentie bevatten, weer een gratis account en blijft de Inhoud behouden. Voor accounts die geen gratis licentie bevatten of die expliciet worden geannuleerd of beëindigd, wordt Inhoud automatisch gemarkeerd voor verwijdering binnen negentig (90) dagen en succesvol verwijderd binnen honderd (100) dagen na de beëindiging, annulering of afloop en, in elk geval, deprovisionering van het op dat moment laatste abonnement van de Klant. Bovendien worden gratis GoTo Meeting-accounts automatisch verwijderd na twee (2) jaar van inactiviteit van de gebruiker (bijv. geen aanmeldingen).

Verwijdering van gebruiker van betaalde account: Als een gebruiker wordt verwijderd van een actieve betaalde account, worden geplande sessies automatisch gemarkeerd voor verwijdering na negentig (90) dagen en succesvol verwijderd binnen honderd (100) dagen na verwijdering van de gebruiker.

GoTo Stage: GoTo Stage-gebruikers met een actief GoTo Webinar-abonnement kunnen gepubliceerde webinars op elk moment publiceren/verwijderen via zelfbediening via de GoTo Webinar-servicesomgeving en/of door een ondersteuningsverzoek in te dienen bij GoTo.

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 andere personen die GoTo-services gebruiken ('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 Addendum Gegevensverwerking ('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 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 Kader voor gegevensprivacy

De Data Privacy Frameworks (DPF) tussen de EU en de VS en tussen Zwitserland en de VS en de Britse Uitbreiding op de DPF tussen de EU en de VS zijn vrijwillige kaders die respectievelijk mechanismen bieden voor bedrijven om persoonlijke gegevens over te dragen van de EU, Zwitserland en het VK naar de VS in overeenstemming met de regelgeving voor gegevensbescherming in deze rechtsgebieden. GoTo voldoet aan elk van deze kaders met betrekking tot het verzamelen, gebruiken en bewaren van persoonlijke gegevens uit respectievelijk de EU, Zwitserland en het VK. Ga voor meer informatie over DPF en de certificering van GoTo naar de DPF-website.

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.

20.4.4 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.

20.5 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 specificeren 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 worden geüpload of anderszins aan GoTo worden verstrekt:

- Door de overheid uitgegeven identificatienummers en afbeeldingen van identificatie-documenten.
- 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.