Technische en organisatorische maatregelen (TOM's)
GoTo Connect

Samenvatting

Dit document met Technische en Organisatorische Maatregelen ('TOM's') beschrijft GoTo's privacy-, beveiligings- en verantwoordingsverplichtingen voor GoTo Connect. 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).
  - *Tijdens de opslag:* Advanced Encryption Standard (AES) 256-bits voor Klantcontent.
- **Datacenters:** Gevestigd in de Verenigde Staten, Brazilië, Duitsland, Australië, Singapore en het Verenigd Koninkrijk om redundantie en stabiliteit te ondersteunen.
- **Fysieke beveiliging:** Er zijn besturingselementen voor fysieke beveiliging en omgevingen beschikbaar, die zijn ontworpen om fysieke toegang te beschermen, te controleren en te beperken voor systemen en servers die Klantcontent onderhouden, om te kunnen voldoen aan uptime-, prestatie- en schaalbaarheidsverplichtingen.
- **Nalevingsaudits:** GoTo Connect beschikt 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 databaseniveau.
- **Perimeterbescherming en inbraakdetectie**: Er zijn tools, technieken en diensten voor perimeterbescherming beschikbaar, ingericht om te voorkomen dat onbevoegd netwerkverkeer de productinfrastructuur binnendringt. Het GoTo-netwerk is voorzien van externe firewalls en interne netwerksegmentatie.
- **Bewaring van gegevens:**
  - GoTo Connect-klanten kunnen te allen tijde verzoeken om retournering of verwijdering van Klantcontent, waaraan binnen dertig (30) dagen na het verzoek van de klant zal worden voldaan.
  - Klantcontent wordt dertig (30) dagen na het verstrijken van de op dat moment laatst betaalde abonnementstermijn van een Klant automatisch verwijderd. Gedurende de abonnementstermijn worden gespreksopnamen en gespreksverslagen dertien (13) maanden bewaard vanaf de datum waarop ze zijn gemaakt.

Inhoudsopgave

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

1 Productintroductie

GoTo Connect is een alles-in-één UCaaS-oplossing (Unified Communications as a Service) voor ondernemingen en bedrijven. GoTo Connect combineert op cloudgebaseerde VoIP-telefoonsystemen (Voice-over-Internet Protocol) en de online, audio- en videoconferentieservices van GoTo Meeting* in één eenvoudige, betrouwbare en flexibele samenwerkingsoplossing (de 'Service').

De Service biedt de volgende functionaliteit:

- De cloudgebaseerde telefoondienst van GoTo Connect is ontworpen om traditionele, lokale PBX-telefoonapparatuur (Private Branch Exchange) te vervangen. Via de PBX-beheerportal kunnen gebruikers met beheerdersmachtigingen de systeeminstellingen bekijken en universeel wijzigen vanaf elk apparaat met een internetverbinding;
- PSTN-vervangingsservices (Public Switch Telephone Network), waaronder telefoonnummers, minuten en aanverwante diensten, worden geleverd via partnerschappen met enkele van 's werelds grootste telecommunicatieaanbieders;
- De visuele doorschakelplanner is een hulpmiddel voor het bewerken van de oproepworkflow, waarmee oproepen naar specifieke voicemailboxen, automatische bedieningstools, of belgroepen kunnen worden geleid, of wachttijden kunnen worden ingesteld; en
- GoTo Connect-bedrijfscontinuïteit (voorheen bekend als 'JBC') is een optioneel, premium service- en hardwareaanbod dat wordt geïnstalleerd op het terrein van de persoon die de service gebruikt ('Gebruiker') en dat lokale telefoondiensten levert via een onafhankelijke derde partij wiens diensten afzonderlijk door een Gebruiker worden ingekocht in het geval van een netwerkstoring.

*Raadpleeg voor meer informatie over de GoTo Meeting-service en de technische en organisatorische maatregelen de GoTo Meeting-TOM's die beschikbaar zijn op https://www.goto.com/company/trust/resource-center.

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.

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;

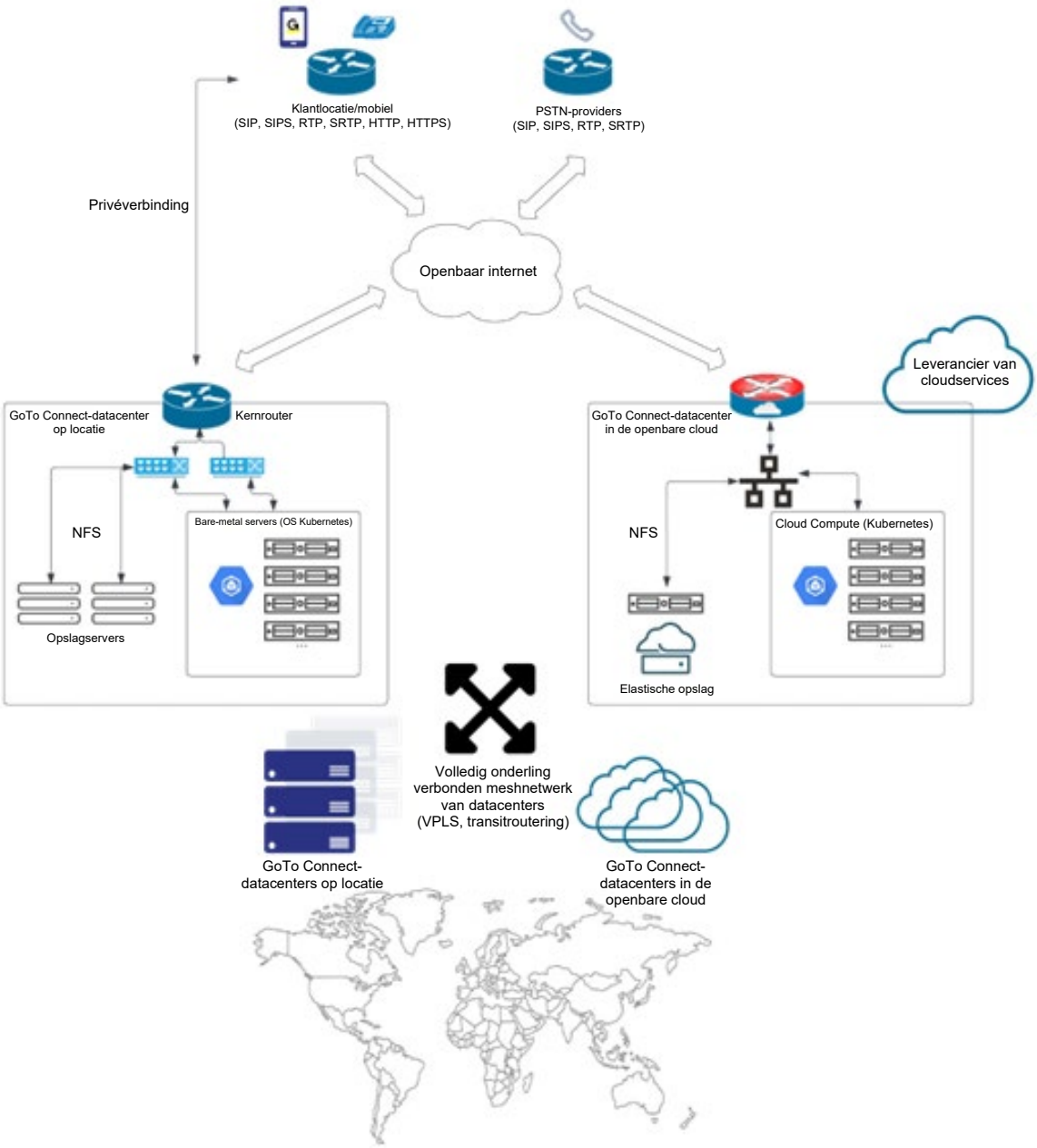
II. Inrichting van organisatorische besturingselementen voor de vorming van intern beleid en afstemming van interne procedures op naleving van standaarden, incidentbeheer, applicatiebeveiliging, personeelsbeveiliging en regelmatige trainingsprogramma's; en

III. Ervoor zorgen dat er privacyprocedures zijn geïmplementeerd voor gegevensverwerking en -beheer, in overeenstemming met de toepasselijke wetgeving, zoals met 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

Het onderstaande diagram (afbeelding 1) toont de netwerkarchitectuur van GoTo Connect.



Afbeelding 1: GoTo Connect-architectuur

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.

4.2 Versleuteling tijdens de overdracht

De Service is ontworpen met end-to-end gegevensbeveiligingsmaatregelen om ervoor te zorgen dat communicatiegegevens niet in onversleutelde vorm worden blootgesteld tijdens de overdracht via openbare of privénetwerken of naar communicatieservers.

De standaard TLS-protocollen van de Internet Engineering Task Force (IETF) worden gebruikt om de communicatie tussen eindpunten te beschermen. Al het netwerkverkeer dat datacenters in en uit gaat waar GoTo gegevens heeft opgeslagen, inclusief alle Klantcontent, wordt tijdens de overdracht versleuteld.

Wanneer TLS-verbindingen tot stand worden gebracht, verifiëren GoTo-servers zich bij clients (werkstations of apparaten) met behulp van openbare-sleutelcertificaten. Indien ondersteund door gebruikersapparatuur, wordt TLS gebruikt om het verkeer tussen gebruikersapparatuur en de infrastructuur van de Service te beveiligen. TLS beveiligt ook informatie benodigd voor de inrichting, waaronder fysieke telefoongegevens, tijdens de overdracht van de infrastructuur van de Service naar de telefoons. Media wordt verzonden via het Secure Real-time Transport Protocol (SRTP), terwijl audioverkeer wordt beveiligd met gedeelde sleutels die via Session Initiation Protocol Secure (SIPS) worden verzonden.

4.3 Versleuteling tijdens de opslag

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

4.4 Verificatie van gebruikers

GoTo Connect voorziet in gebruikerstoegang met behulp van GoTo's eigen platform voor identiteitsbeheer, gebruikt Security Assertion Markup Language (SAML) om single sign-on (SSO) aan te bieden, en biedt een rechtstreekse integratie met het GoTo-platform via API. Het platform voor identiteitsbeheer ondersteunt administratieve besturingselementen voor de gebruikersverificatie, waaronder het configureren van het wachtwoordbeleid, het verplicht resetten van wachtwoorden, en het vereisen van het gebruik van SAML voor verificatie.

Service PBX-beheerders (superbeheerders) kunnen specifieke machtigingen toekennen of weigeren in de PBX-beheerportal. Deze machtigingen omvatten de mogelijkheid om de PBX te configureren, E911-adressen en -locaties te bewerken, rapporten weer te geven, facturen te bekijken en te betalen, en instellingen en accounts bij te werken en te verwijderen voor:

- Gebruikers;
- Gebruikersgroepen;
- Extensies;
- Apparaten;
- Hardware;

- Locaties; en
- Telefoonnummers (het verwijderen en aanmaken van telefoonnummers wordt beheerd via het bestelproces voor telefoonnummers).

Voor meer details over groepsmachtigingen in PBX-beheer, kunt u de Aan de slag-handleiding voor beheerders raadplegen.

5 Bijwerken van beveiliging

GoTo controleert en actualiseert ons beveiligingsprogramma regelmatig, en schakelt onafhankelijke derden in om onze relevante besturingselementen voor beveiliging minstens eenmaal per jaar te beoordelen. Zo zorgt GoTo ervoor dat onze 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 Connect 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.

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

De Service maakt met name gebruik van een platform met microservices en containers, dat snelle implementatie en schaling van services mogelijk maakt, en redundantie, oproepdoorschakeling, schaalbaarheid en hoge beschikbaarheid aan Gebruikers biedt. Deze onderlinge verbondenheid zorgt ervoor dat microservices zichzelf kunnen ontdekken en herstellen bij een storing in een bepaald datacenter, of in het geval van een probleem dat geografisch gelokaliseerd is op het openbare internet. De service is ontworpen om automatisch uit te vallen tussen datacenters.

De infrastructuur is onderling verbonden tussen datacenters in de vorm van 'clusters', met interconnectiviteit van een VPLS-meshnetwerk (Virtual Private LAN Service) en transitroutering. VPLS-verbindingen kunnen overschakelen naar een gecodeerd Dynamic Multipoint Virtual Private Network (DMVPN) via internetverbindingen als de primaire verbindingen offline gaan. Clouddatacenters zijn verbonden met regionale locaties van cloudproviders via versleutelde tunnels, die gegevens beschermen door ze buiten het openbare internet te houden totdat ze nodig zijn. Alle productiedatacenters zijn met elkaar verbonden, zodat interne toepassingen vanaf elke locatie diensten kunnen bereiken. GoTo Connect-gegevens worden ter plaatse gehost in privéhardware (op rack- en bladeservers) of in datacenters van leveranciers van cloudhosting, volgens een vergelijkbare maar aangepaste architectuur. Elke datacenterlocatie maakt verbinding met meerdere PSTN-partners/-providers via SIP-trunks (Session Initiation Protocol) via het openbare internet.

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-actieve datacenters; of
b) datacenters van cloudhostingproviders.

Hostingdatacenters bevinden zich in de Verenigde Staten, Brazilië, Duitsland, Australië, Singapore en het Verenigd Koninkrijk.

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

7.1 Fysieke beveiliging datacenters

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

- Videobewaking en -opname;
- Temperatuurregeling met verwarming, ventilatie en airconditioning;
- Brandbestrijding en rookmelders;
- Ononderbreekbare stroomvoorziening;
- Verhoogde vloeren of uitgebreid kabelbeheer;
- Continue monitoring en waarschuwingen;
- Bescherming tegen veel voorkomende natuurrampen en door de mens veroorzaakte rampen, zoals vereist afhankelijk van de locatie van het betreffende datacenter; en
- 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.
- **Attestatierapport Service Organization Control (SOC) 2 Type II** incl. **BSI Cloud Computing-catalogus (C5)** van het American Institute of Certified Public Accountants (AICPA).
- Compliance met de **Payment Card Industry Data Security Standard (PCI DSS)** voor de e-commerce- en betalingsomgevingen van GoTo.
- Beoordeling van interne besturingselementen zoals vereist in het kader van de controle van de jaarrekeningen door de **Public Company Accounting Oversight Board (PCAOB)**.

9 Beveiliging van toepassingen

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

10 Rapporteren, monitoren en waarschuwen

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

11 Detectie en respons van eindpunten

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

12 Beheren van bedreigingen

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

13 Scannen op beveiliging en kwetsbaarheid en patchbeheer

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

14 Logische toegangscontrole

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

15 Scheiding van gegevens

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

16 Perimeterbescherming en inbraakdetectie

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

- Intrusiedetectiesystemen die systemen, diensten, netwerken en toepassingen monitoren op ongeautoriseerde toegang;
- Kritische systeem- en configuratiebestandsbewaking;
- Webtoepassingsfirewall (WAF) en DDoS-preventiediensten op de applicatieniveau die fungeren als proxy voor GoTo-verkeer
- Een firewall voor lokale toepassingen die een extra beschermingslaag biedt tegen de top tien van OWASP, en andere kwetsbaarheden van webtoepassingen en kwaadaardig verkeer; en
- 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 van GoTo is verantwoordelijk voor het detecteren van en reageren op beveiligingsgebeurtenissen. Het Security Operations Center 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 onze kritieke communicatieprocessen, beleidsregels en standaardwerkprocedures. Het is ontworpen om relevante verdachte of geïdentificeerde beveiligingsgebeurtenissen in interne systemen en diensten, inclusief GoTo Connect, te beheren, te identificeren en op te lossen. Het Incidentenbestrijdingsplan beschrijft mechanismen voor medewerkers om verdachte beveiligingsgebeurtenissen te melden, evenals escalatiepaden die indien nodig gevolgd moeten worden. Verdachte gebeurtenissen worden gedocumenteerd en indien nodig geëscaleerd via gestandaardiseerde gebeurtenistickets, waarbij prioriteit wordt gegeven aan de meest alarmerende gebeurtenissen.

18 Verwijderen en retourneren van Content

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

Schema voor het bewaren van Klantcontent: Tenzij anders vereist door de toepasselijke wetgeving, wordt Klantcontent automatisch verwijderd na dertig (30) 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. Gedurende de abonnementstermijn van de Klant worden gespreksopnamen en gespreksverslagen op voortschrijdende basis verwijderd, en dertien (13) maanden bewaard vanaf de datum waarop ze zijn gemaakt. 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 en Gebruikers 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

20.3 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.

20.4 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.

20.5 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.

20.6 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 en Gebruikers 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.

20.7 Overdrachtskaders

GoTo ondersteunt rechtmatige internationale gegevensoverdrachten onder de volgende kaders:

20.8 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.

20.9 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.

20.10 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.

20.11 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.

20.12 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.

20.13 Gevoelige gegevens Verwerkingsbeperkingen

Tenzij GoTo hier uitdrukkelijk om heeft verzocht of de Klant hierover anderszins schriftelijke toestemming van GoTo heeft ontvangen, mogen de volgende soorten gevoelige gegevens niet naar GoTo Connect 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.

20.14 Naleving in gereguleerde omgevingen

Klanten zijn zelf verantwoordelijk voor het implementeren van de juiste beleidsregels, procedures en beveiligingsmechanismen wanneer zij GoTo Connect gebruiken in gereguleerde omgevingen.

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.