TECHNISCHE EN ORGANISATORISCHE MAATREGELEN VOOR GOTOMYPC

CONTROLEMECHANISMEN VOOR BEVEILIGING EN PRIVACY

Publicatiedatum: Februari 2022

1 Producten en services

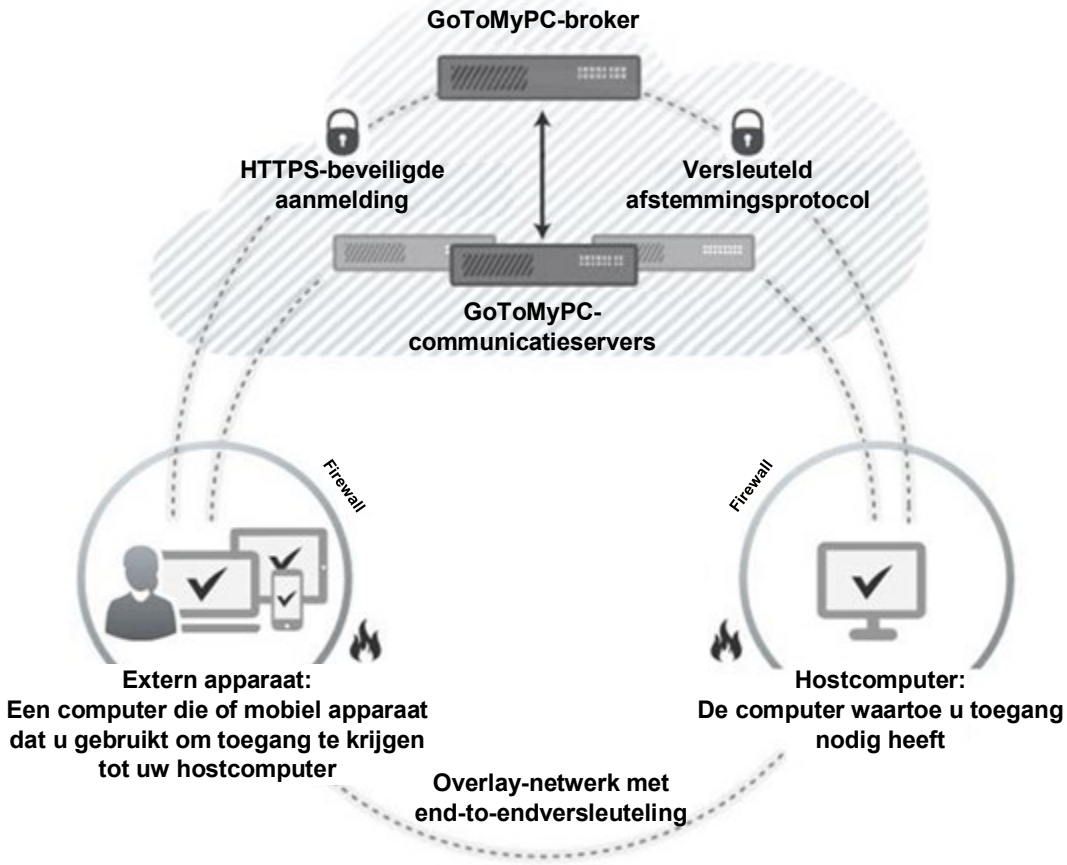
Dit document bevat de Technische en Organisatorische Maatregelen (TOM's) voor GoToMyPC, een gehoste service die veilige externe toegang mogelijk maakt tot een met internet verbonden Windows- of Mac-hostcomputer, vanaf elke computer en iPad en elk iPhone of Android-apparaat op afstand. De service biedt functies als een viewer voor schermdeling, bestandsoverdracht via slepen en neerzetten, afdrukken op afstand, gasten uitnodigen, gebruik met meerdere monitoren, mobiele apps en chatten. Er zijn drie versies van GoToMyPC beschikbaar, om te voldoen aan de behoeften van individuele professionals, teams en kleine en middelgrote bedrijven (MKB).

2 Productarchitectuur

GoToMyPC is een gehoste service die uit vijf componenten bestaat:

- *Hostcomputer:* Meestal een computer thuis of op kantoor met permanente internet-toegang waarop een server met een kleine voetafdruk is geïnstalleerd. Deze server registreert en verifieert zichzelf bij de GoToMyPC-broker.
- *Browser:* Vanaf de computer op afstand, de zogenaamde client, start de gebruiker een webbrowser op, gaat naar de beveiligde GoToMyPC-website, voert zijn gebruikersnaam en wachtwoord in en klikt vervolgens op 'Verbinden' om de broker een geverifieerd, versleuteld verzoek om toegang tot de gewenste hostcomputer te sturen. Als alternatief kan de gebruiker de GoToMyPC-app installeren op een ondersteunde tablet of smartphone, zijn accountgegevens invoeren, en op 'Verbinden' klikken om het verzoek te verzenden.
- *Broker:* De broker is een 'matchmaker' die verbindingsverzoeken ontvangt en deze koppelt aan geregistreerde computers. Als er een overeenkomst is, wijst de broker de sessie toe aan een communicatieserver. Vervolgens wordt de client-viewer (een sessie-specifieke uitvoerbare applet) automatisch geladen door onze automatische lanceringstool.
- *Communicatieserver:* De communicatieserver is een tussenliggend systeem dat een ondoorzichtige en sterk gecomprimeerde gecodeerde stream tussen de client en hostcomputers doorgeeft gedurende elke GoToMyPC-sessie.
- *Rechtstreekse verbindingen:* Zodra de gebruiker is geverifieerd en verbonden, probeert GoToMyPC een directe verbinding tussen de client en de host tot stand te brengen, waarbij de GoToMyPC-communicatieserver waar mogelijk wordt omzeild om de verbindingssnelheid te verhogen en de prestaties tijdens de sessie te verbeteren. Met de functie Rechtstreekse verbindingen krijgt zowel de client als de host de instructie om gedurende een beperkte tijd inkomende verbindingen te ontvangen, en te proberen uitgaande verbindingen tot stand te brengen; welk signaal het eerst binnenkomt, brengt dan de verbinding tot stand. De client en de host voeren vervolgens een op het SRP-protocol (Secure Remote Wachtwoord) gebaseerde geverifieerde sleutelovereenkomst uit, en brengen een beveiligde verbinding tot stand die zodanig is ontworpen dat de gevoeligheid voor 'man-in-the-middle'-aanvallen wordt verminderd of zelfs volledig geëlimineerd. Als de rechtstreekse verbinding wordt geblokkeerd of

onderbroken, blijft de verbinding die eerder tot stand is gebracht via de communicatieserver de service voor toegang op afstand onderhouden. De functie Rechtstreekse verbindingen is altijd ingeschakeld voor GoToMyPC- en GoToMyPC Pro-accounts en wordt optioneel aangeboden voor GoToMyPC Corporate.



De infrastructuur is zodanig ontworpen dat deze zowel voldoende krachtig als beveiligd is. Redundante routers, switches, serverclusters en back-upsystemen worden ontworpen en gebruikt om een hoge beschikbaarheid te garanderen. Voor schaalbaarheid en betrouwbaarheid verdelen switches inkomende aanvragen transparant over webservers. Om optimale prestaties te garanderen, verdeelt de GoToMyPC-broker de client/serversessies over geografisch verspreide communicatieservers.

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

Als de host al een TLS-verbinding met de gateway tot stand heeft gebracht, stuurt de gateway de TLS-sleuteluitwisseling van de client door naar de host via een verzoek om opnieuw te onderhandelen over de eigen sleutel. De client en de host kunnen zo TLS-sleutels uitwisselen zonder dat de gateway de sleutel te weten komt.

3 Technische beveiligingsmaatregelen van GoToMyPC

GoTo maakt gebruik van technische besturingselementen voor beveiliging die voldoen aan de industriestandaard, en die geschikt zijn voor de aard en het bereik van de services (zoals deze term wordt gedefinieerd in de Servicevoorwaarden). Ze zijn ontworpen om de infrastructuur van de service en de gegevens die zich daarin bevinden optimaal te beschermen. U vindt de Servicevoorwaarden op https://www.goto.com/company/legal/terms-and-conditions.

3.1. Logische toegangscontrole

Er zijn logische besturingselementen voor toegang geïmplementeerd, ingericht om ongeautoriseerde toegang tot toepassingen en gegevensverlies in bedrijfs- en productieomgevingen te voorkomen of te beperken. Medewerkers krijgen minimale toegang (met slechts zoveel rechten als nodig zijn) tot specifieke GoTo-systemen, toepassingen, netwerken en apparaten. Verder worden gebruikersrechten gescheiden op basis van functionele rol en omgeving.

3.2. Perimeterbescherming en inbraakdetectie

GoTo heeft tools, technieken en services voor perimeterbescherming geïmplementeerd, ingericht om te voorkomen dat onbevoegd netwerkverkeer de productinfrastructuur binnendringt. Het GoTo-netwerk is voorzien van externe firewalls en interne netwerksegmentatie.

Meer specifiek wordt meerlaagse perimeterbeveiliging geboden door een dubbele firewall: één tussen het internet en webservers en één tussen de GoToMyPC-broker en backenddatabases. Cloudbronnen maken ook gebruik van hostgebaseerde firewalls. Daarnaast maakt GoTo gebruik van maatregelen ter bescherming van de perimeter, waaronder een DDoS-preventieservice (Distributed Denial of Disaster) van een derde partij in de cloud ter bescherming tegen volumetrische DDoS-aanvallen; deze service wordt minstens één keer per jaar getest. Kritieke systeembestanden zijn ontworpen met bescherming tegen kwaadwillige aanvallen en onbedoelde blootstelling of vernietiging.

3.3. 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. Alleen geverifieerde partijen krijgen toegang tot relevante accounts.

3.4. Fysieke beveiliging

Fysieke beveiliging datacenters

GoTo werkt samen met datacenters om de fysieke beveiliging te waarborgen van serverruimtes waar productieservers staan. Deze beveiligingsmaatregelen omvatten:

- Videobewaking en -opname
- Meervoudige verificatie voor zeer gevoelige ruimtes
- Temperatuurregeling met verwarming, ventilatie en airconditioning
- Brandbestrijding en rookmelders
- Ononderbreekbare stroomvoorziening (UPS)

- Verhoogde vloeren of uitgebreid kabelbeheer
- Continue monitoring en waarschuwingen
- Bescherming tegen veel voorkomende natuurrampen en door de mens veroorzaakte rampen, zoals vereist afhankelijk van de locatie van het betreffende datacenter
- Gepland onderhoud en validatie van alle kritieke besturingselementen voor fysieke beveiliging.

GoTo 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. Het management van GoTo evalueert ten minste elk kwartaal de logbestanden voor fysieke toegang tot datacenters en serverruimten. Daarnaast worden eerder geautoriseerde personeelsleden die worden ontslagen, de fysieke toegang tot datacenters per direct ontzegd.

3.5. Back-up van gegevens, noodherstel en beschikbaarheid

GoToMyPC voert databasereplicatie vrijwel in realtime uit naar een secundaire site die zich op een geografisch andere locatie bevindt. 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 het systeem wordt periodiek getest.

3.6. Bescherming tegen malware

Op alle GoToMyPC-servers wordt malwarebeschermingssoftware met auditlogbestanden geïnstalleerd. Meldingen die duiden op mogelijke kwaadwillige activiteiten worden doorgestuurd naar het passende responsteam.

3.7. Versleuteling

GoTo houdt zich aan een cryptografische standaard die overeenkomt met aanbevelingen van brancheverenigingen, overheidspublicaties en andere relevante normgroepen. Cryptografische standaard wordt periodiek herzien en de standaarden op het gebied van versleuteling worden regelmatig opnieuw beoordeeld. Op basis hiervan kunnen gebruikte blokvercijferingen en technologieën worden bijgewerkt in overeenstemming met het ingeschatte risico en de marktacceptatie van nieuwe standaarden.

3.7.1. Versleuteling tijdens de overdracht

GoToMyPC Corporate heeft 256-bits AES-encryptie (Advanced Encryption Standard) ingebouwd. Al het verkeer tussen de GoToMyPC-browserclient en de hostcomputer is sterk gecomprimeerd en versleuteld. GoToMyPC genereert unieke, geheime sleutels voor elke verbinding met behulp van een sleutelovereenkomst met wederzijdse verificatie.

3.8. Beheersing van kwetsbaarheden

Maandelijks worden systemen en netwerken gescand op interne en externe kwetsbaarheden. Er worden daarnaast ook periodiek dynamische en statische tests uitgevoerd op de kwetsbaarheid van applicaties, evenals penetratietests voor getroffen omgevingen. Deze scan- en

testresultaten worden gerapporteerd in netwerkbewakingstools, en waar nodig worden herstelmaatregelen getroffen.

GoTo communiceert en beheert kwetsbaarheden door maandelijkse rapporten aan de ontwikkelingsteams en het management te leveren.

3.9. Rapporteren en waarschuwen

GoTo verzamelt geïdentificeerd afwijkend of verdacht verkeer in de relevante beveiligingslogbestanden van de betreffende productiesystemen.

4 Organisatorische besturingselementen

GoTo biedt een uitgebreide reeks organisatorische en administratieve controlemechanismen om de beveiliging en privacy van GoToMyPC te beschermen.

4.1. Beveiligingsbeleid en -procedures

GoTo heeft een uitgebreid beveiligingsbeleid, met beleidsregels en procedures die zijn afgestemd op bedrijfsdoelen, nalevingsprogramma's en algemeen verantwoord zakelijk bestuur. Deze beleidsregels en procedures worden periodiek herzien en waar nodig bijgewerkt om de voortdurende naleving ervan te garanderen.

4.2. Naleving van normen

GoTo voldoet aan de van toepassing zijnde wettelijke, financiële, gegevensprivacy- en regelgevende vereisten, en houdt zich aan de volgende certificeringen en externe auditrapporten:

- TRUSTe-certificaat inzake privacy en best practices voor gegevensbeheer voor ondernemingen, voor de operationele besturingselementen voor privacy- en gegevensbescherming die zijn afgestemd op de belangrijkste privacywetten en erkende privacyraamwerken. Raadpleeg voor meer informatie onze blogpost hierover.
- Attestatierapport Service Organization Control (SOC) 2 Type 2 van het American Institute of Certified Public Accountants (AICPA).
- Attestatierapport Service Organization Control (SOC) 3 Type II van het American Institute of Certified Public Accountants (AICPA)
- Compliance met de Payment Card Industry Data Security Standard (PCI DSS) voor de e-commerce- en betalingsomgevingen van GoTo
- Beoordeling van interne besturingselementen zoals vereist in het kader van de controle van de jaarrekeningen door de Public Company Accounting Oversight Board (PCAOB)

4.3. Het Security Operations Center en incidentbeheer

Het Security Operations Center (SOC) van GoTo wordt beheerd door het Team Beveiligingsoperaties, dat verantwoordelijk is voor het detecteren van en reageren op beveiligingsgebeurtenissen. Het SOC maakt gebruik van beveiligingssensoren en analysesystemen om potentiële problemen te identificeren, en heeft een gedocumenteerd Incidentenbestrijdingsplan om adequaat op incidenten te reageren.

Het Incidentenbestrijdingsplan is afgestemd op de kritieke communicatieprocessen van GoTo, het Beleidsreglement voor Incidentbeheer van Informatiebeveiliging, en de bijbehorende standaardwerkprocedures. Het is ontworpen om verdachte of potentiële beveiligingsgebeurtenissen in interne systemen en services, te beheren, te identificeren en op te lossen, waaronder GoToMyPC. In het Incidentenbestrijdingsplan is vastgelegd dat er technisch personeel aanwezig moet zijn om mogelijke gebeurtenissen en kwetsbaarheden met betrekking tot informatiebeveiliging te identificeren, en vermoedelijke of bevestigde gebeurtenissen naar het management te escaleren. Medewerkers kunnen beveiligingsincidenten melden via e-mail, telefoon en tickets, volgens het proces dat is gedocumenteerd op de GoTo-intranetsite. Alle geïdentificeerde of verdachte gebeurtenissen worden gedocumenteerd en geëscaleerd via gestandaardiseerde gebeurtenistickets, waarbij prioriteit wordt gegeven aan de meest alarmerende gebeurtenissen.

4.4. Beveiliging van toepassingen

Het applicatiebeveiligingsprogramma van GoTo is gebaseerd op de SDL (Security Development Lifecycle) van Microsoft om productcode te beveiligen. De kernelementen van dit programma zijn handmatige codebeoordelingen, bedreigingsmodellen, statische code-analyse, dynamische analyse en systeemverharding.

4.5. Screening van personeel

Er worden vóór de datum van indiensttreding algemene achtergrondcontroles uitgevoerd ten aanzien van nieuwe werknemers, voor zover toegestaan door de toepasselijke wetgeving en passend bij de functie. De resultaten worden bijgehouden in het functiedossier van de medewerker. De criteria voor achtergrondcontroles variëren afhankelijk van de wetgeving, de functieverantwoordelijkheid en het leiderschapsniveau van de potentiële werknemer, en zijn onderhevig aan de gangbare en aanvaardbare best practices van het betreffende land.

4.6. Bewustzijns- en trainingsprogramma's over beveiliging

Nieuwe medewerkers worden tijdens de oriëntatie geïnformeerd over het beveiligingsbeleid en de Gedragscode en Bedrijfsethiek van GoTo. Deze verplichte jaarlijkse beveiligings- en privacytraining wordt gegeven aan relevant personeel en beheerd door het Team Talentontwikkeling met ondersteuning van het Beveiligingsteam.

Vaste en tijdelijke medewerkers van GoTo worden regelmatig geïnformeerd over richtlijnen, procedures, beleidsregels en normen op het gebied van beveiliging en privacy via verschillende mediakanalen. Dit zijn bijvoorbeeld onboardingkits voor nieuwe medewerkers, bewustmakingscampagnes, webinars met de CISO, een programma voor 'beveiligingskampioenen', en posters en ander materiaal dat minstens twee keer per jaar wordt uitgewisseld en waarop de methoden voor het beveiligen van gegevens, apparaten en faciliteiten worden geïllustreerd.

5 Privacy

GoTo neemt de privacy van zijn klanten, de abonnees van de GoTo-services en eindgebruikers zeer serieus, en zet zich in om relevante best practices voor gegevensverwerking en -beheer op een open en transparante manier bekend te maken.

5.1. AVG

De General Data Protection Regulation (GDPR), in het Nederlands de Algemene Verordening Gegevensbescherming (AVG), is de Europese wet om de privacy en gegevens van alle EU-ingezetenen te beschermen. De GDPR is voornamelijk bedoeld om burgers en ingezetenen controle te geven over hun persoonlijke gegevens en om het regelgevingskader EU-breed te vereenvoudigen. GoToMyPC voldoet aan de toepasselijke bepalingen van GDPR. Ga voor meer informatie naar https://www.goto.com/company/trust/privacy.

5.2. CCPA

GoTo verklaart en garandeert hierbij dat het voldoet aan de California Consumer Privacy Act (CCPA). Ga voor meer informatie naar https://www.goto.com/company/trust/privacy.

5.3. Gegevensbescherming en Privacybeleid

GoTo heeft een uitgebreid en wereldwijd geldend Addendum gegevensverwerking ('DPA'; Data Processing Addendum) opgesteld dat beschikbaar is in het Engels en het Duits en die voldoet aan de eisen van de AVG en CCPA, en deze zelfs overstijgt, en waarin de verwerking van persoonsgegevens door GoTo is geregeld.

Concreet zijn in de DPA verschillende AVG-gerichte beveiligingsmechanismen voor de gegevensprivacy verwerkt, waaronder: (a) details over gegevensverwerking, openbaarmaking aan een andere gegevensverwerkende partij, enzovoorts, zoals vereist onder Artikel 28; (b) Europese modelbepalingen (standaardbepalingen voor overeenkomsten); en (c) de technische en organisatorische maatregelen voor gegevensbeveiliging van GoTo. Om in te spelen op het van kracht worden van de CCPA hebben we onze wereldwijde DPA bijgewerkt om de volgende aspecten hierin op te nemen: (a) aangepaste definities die aansluiten bij de CCPA; (b) recht op toegang en verwijdering; en (c) garanties dat GoTo de persoonlijke gegevens van onze gebruikers niet zal verkopen.

Voor bezoekers van onze webpagina's maakt GoTo in zijn Privacybeleid op de openbare website bekend welke soorten informatie worden verzameld en gebruikt om de Services te leveren, te onderhouden, te verbeteren en te beveiligen. Het bedrijf kan van tijd tot tijd het Privacybeleid bijwerken om wijzigingen in de verwerking van informatie en/of wijzigingen in de toepasselijke wetgeving weer te geven, maar zal op haar website melding maken van eventuele materiële wijzigingen voordat een dergelijke wijziging van kracht wordt.

5.4. Overdrachtskaders

GoTo heeft een krachtig wereldwijd gegevensbeschermingsprogramma ingericht, dat rekening houdt met de toepasselijke wetgeving, en rechtmatige internationale overdrachten binnen de volgende kaders ondersteunt:

5.4.1. Standaardcontractbepalingen

De Standaardbepalingen ('SCC's'; Standard Contractual Clauses) zijn gestandaardiseerde contractbepalingen die zijn erkend en aangenomen door de Europese Commissie. Het hoofddoel van deze bepalingen is om ervoor te zorgen dat alle persoonsgegevens die de Europese Economische Ruimte ('EER') verlaten, worden overgedragen in overeenstemming met de Europese wetgeving voor gegevensbescherming. GoTo heeft geïnvesteerd in een privacyprogramma van wereldklasse om te voldoen aan de strenge vereisten van de SCC's voor de overdracht van per-

soonsgegevens. GoTo biedt zijn klanten SCC's, soms ook bekend als de Model-bepalingen van de EU, die specifieke garanties bevatten aangaande de overdracht van persoonsgegevens voor de relevante GoTo-services. Ze zijn onderdeel van de wereldwijde DPA. Naleving van de SCC's garandeert dat klanten van GoTo veilig vrijuit gegevens kunnen overdragen vanuit de EER naar de rest van de wereld.

Aanvullende maatregelen

Naast de maatregelen die in deze TOM's zijn gespecificeerd, heeft GoTo de navolgende Veelgestelde vragen en de antwoorden daarop verzameld, om GoTo's aanvullende maatregelen te schetsen die zijn getroffen om rechtmatige overdrachten, zoals bedoeld in hoofdstuk 5 van de AVG, te ondersteunen. Hiermee bieden we ook de mogelijkheid om case-by-case-analyses, die door het Europese Hof van Justitie worden aanbevolen in verband met de SCC's, te bespreken en te begeleiden.

5.4.2. Certificeringen voor de CBPR en PRP van de APEC

GoTo heeft ook de certificeringen van de Asia-Pacific Economic Cooperation ('APEC') voor de Cross-Border Privacy Rules ('CBPR') en de Privacy Recognition for Processors ('PRP'). De CBPR en de PRP van APEC zijn de eerste standaarden voor gegevensbeveiliging die zijn goedgekeurd voor de overdracht van persoonsgegevens tussen lidstaten van de APEC. De certificeringen zijn behaald en onafhankelijk gevalideerd door TrustArc, een externe leider op het gebied van naleving van gegevensbeveiliging die is goedgekeurd door de APEC.

5.5. Klantcontent retourneren en verwijderen

Klanten van GoToMyPC kunnen te allen tijde om teruggave of verwijdering van hun Klantcontent vragen via gestandaardiseerde interfaces. Als deze interfaces niet beschikbaar zijn of als GoTo anderszins niet in staat is om een dergelijk verzoek in te willigen, zal GoTo een commercieel redelijke poging doen om de Klant, afhankelijk van de technische haalbaarheid, te helpen bij het ophalen of verwijderen van zijn Content.

De Klantcontent zal binnen dertig (30) dagen na het verzoek van de Klant worden verwijderd. De Klantcontent in GoToMyPC wordt automatisch binnen negentig (90) dagen na afloop of beëindiging van de laatste abonnementstermijn verwijderd. Op schriftelijk verzoek zal GoTo de verwijdering van dergelijke Content bevestigen.

5.6. Gevoelige gegevens

Hoewel GoTo ernaar streeft om alle Klantcontent te beschermen, zijn we door wettelijke en contractuele beperkingen genoodzaakt om het gebruik van GoToMyPC voor bepaalde soorten informatie te beperken. Tenzij de Klant schriftelijke toestemming van GoTo heeft ontvangen, mogen de volgende gegevens niet worden geüpload naar of ingevoerd of gegenereerd in GoToMyPC:

- 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 GoToMyPC te innen of te ontvangen.
- Alle informatie die speciaal beschermd wordt door toepasselijke wet- en regelgeving, in het bijzonder informatie over ras, etniciteit, religieuze of politieke overtuigingen, lidmaatschappen van organisaties, etc. van een individu.

5.7. Volgen en analyseren

GoTo verbetert zijn websites en producten voortdurend met behulp van webanalysetools van derden, waarmee GoTo inzichtelijk maakt hoe bezoekers zijn websites, desktopapplicaties en mobiele toepassingen gebruiken, en wat de voorkeuren en problemen van gebruikers zijn. Voor meer informatie verwijzen wij u naar het Privacybeleid.

6 Derde partijen

6.1. Gebruik van derde partijen

Als onderdeel van de interne beoordeling en processen met betrekking tot leveranciers en derde partijen, kunnen de evaluaties van leveranciers door meerdere teams worden uitgevoerd, afhankelijk van de relevantie en toepasbaarheid. Het Beveiligingsteam evalueert alle leveranciers die op informatiebeveiliging gebaseerde services leveren, en beoordeelt eveneens de hostingfaciliteiten van derde partijen. De teams Juridische zaken en Inkoop kunnen contracten, werkomschrijvingen en serviceovereenkomsten evalueren, indien vereist volgens interne processen. Er worden indien nodig passende nalevingsdocumentatie of -rapporten verkregen die ten minste jaarlijks worden geëvalueerd, om ervoor te zorgen dat de controleomgeving adequaat functioneert en alle noodzakelijke controles op gebruikers-overwegingen worden uitgevoerd. Daarnaast moeten derde partijen die gevoelige of vertrouwelijke gegevens hosten of die toegangsmachtigingen krijgen van GoTo, een schriftelijk contract ondertekenen waarin de relevante vereisten voor toegang tot of opslag of behandeling van de informatie (zoals van toepassing) zijn opgenomen.

6.2. Best practices bij contractering

Om de bedrijfscontinuïteit te waarborgen en ervoor te zorgen dat er passende maatregelen worden getroffen om de vertrouwelijkheid en integriteit van bedrijfsprocessen en gegevens-verwerking van derden te beschermen, beoordeelt GoTo allereerst de voorwaarden van relevante derde partijen. Vervolgens wordt beslist om ofwel GoTo's goedgekeurde inkoop-sjablonen te gebruiken, ofwel om te onderhandelen over dergelijke voorwaarden van derden, indien dat nodig blijkt.

7 Contact opnemen met GoTo

Klanten kunnen contact opnemen met GoTo op https://support.goto.com voor algemene vragen of privacy@goto.com voor privacy-gerelateerde vragen.