

TECHNISCHE EN ORGANISATORISCHE MAATREGELEN VOOR RESCUE LIVE GUIDE

Controlemechanismen voor beveiliging en privacy

Publicatiedatum: Februari 2022

1 Producten en services

In dit document worden de Technische en Organisatorische Maatregelen (TOM's) voor Rescue Live Guide beschreven.

Rescue Live Guide is een webgebaseerde ondersteuningstool die door professionals in de klantenservice wordt gebruikt om op afstand visuele begeleiding in de browser te bieden, zonder dat er een script aan de ondersteunde website hoeft te worden toegevoegd, of software hoeft te worden gedownload. Met de toestemming van de eindgebruiker stelt Rescue Live Guide een klantenserviceprofessional in staat om samen met de Eindgebruiker op een veilige manier door websites te bladeren, en biedt de medewerker begeleidende hulpmiddelen daarvoor.

2 Productarchitectuur

GoTo Rescue Live Guide is een SaaS-gebaseerde oplossing (Software-as-a-Service) voor visuele betrokkenheid, die de eindgebruiker koppelt aan de medewerker in een beveiligde cloudbrowser.

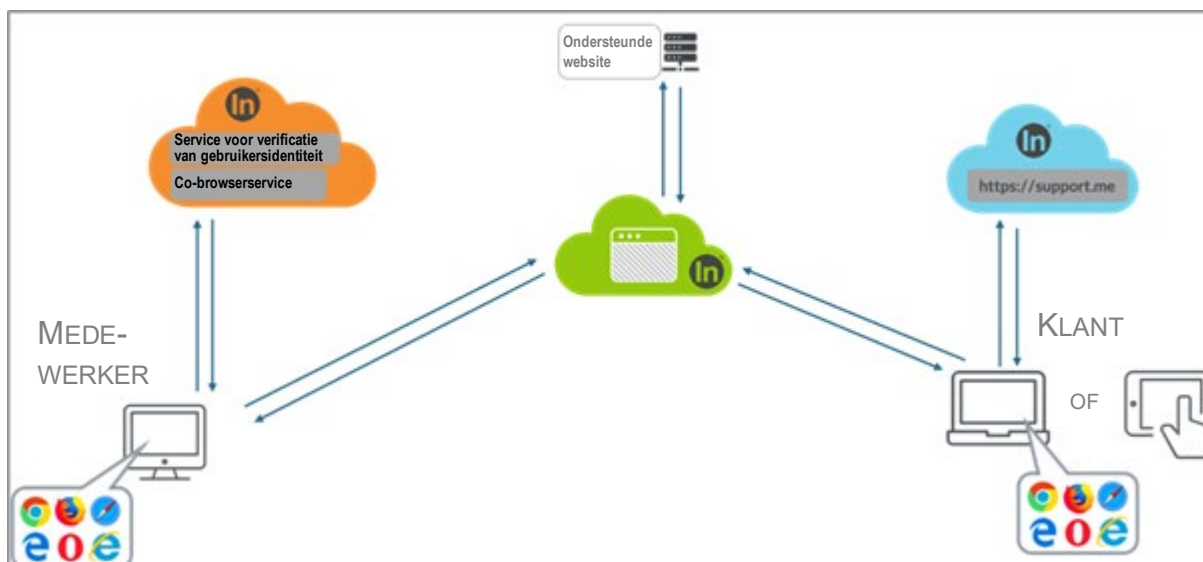
Zowel de applicaties van de medewerker als die van de eindgebruikers zijn webapplicaties die draaien in een ondersteunde en door de gebruiker gekozen browser. De backends die deze toepassingen bedienen, worden gehost in GoTo's AWS-cloud (Amazon Web Services), waarbij peers aan elkaar worden gekoppeld in een co-browsingsessie.

De sessie wordt aangemaakt wanneer een eindgebruiker een gedeelde browsersessie start. Aan het begin van de sessie wordt een sessie-PIN gegenereerd en weergegeven voor de eindgebruiker. De eindgebruiker kan de medewerker aan de sessie laten deelnemen door de sessie-PIN te delen. Zodra een co-browsingsessie tot stand is gebracht tussen eindgebruiker en medewerker, wordt de ondersteunde website geladen in een geïsoleerde headless browser in de GoTo-cloud.

Het daadwerkelijke surfen op het web, en alle communicatie met de ondersteunde website, vindt plaats in de cloudbrowser. Het beeld wordt naar de webtoepassingen van beide gebruikers gestreamd en de gebruikersacties worden teruggestuurd om in de cloudbrowser te worden uitgevoerd.

De cloudbrowser-instanties zijn volledig geïsoleerd, en afgezien van rapportagegegevens, opname (indien ingeschakeld) en sessie-informatie, worden de gegevens na afloop van een co-browsingsessie gewist.

Meer informatie over de beveiligingsmaatregelen van de oplossing vindt u in het volgende hoofdstuk (Technische beveiligingsmaatregelen) van dit document.



Afbeelding 1: Infrastructuur van Rescue Live Guide

3 Technische beveiligingsmaatregelen

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.

Medewerkers in Rescue Live Guide zijn gebonden aan bedrijfsaccounts en moeten zichzelf verifiëren met hun gebruikersnaam en een sterk wachtwoord. Als optionele extra veiligheidsmaatregel kan de accountbeheerder verplichte tweeledige verificatie instellen voor alle medewerkers in zijn account. De medewerkersconsole is alleen toegankelijk na verificatie.

De beschikbaarheid van extra functies (zoals rapportage, opnames, accountbeheer) voor geverifieerde medewerkers/beheerders kan worden beheerd en beperkt met toegewezen rollen.

3.2. Bescherming van eindgebruikers

Bij het maken van deze service is rekening gehouden met de privacy van de eindgebruikers van Rescue Live Guide. De sessiepincode is daarom eigendom van de eindgebruiker en een supportmedewerker kan alleen aan een sessie deelnemen als de eindgebruiker zijn sessiepincode met hem heeft gedeeld. Bovendien is de sessiepincode bedrijfsspecifiek: een sessie

die op een bepaalde website wordt gestart, kan alleen worden bijgewoond door medewerkers die deel uitmaken van de account die aan de betreffende ondersteunde website is toegewezen.

GoTo slaat de content van de eindgebruiker die tijdens de ondersteuningssessie wordt gegenereerd niet op; zoals eerder vermeld, zijn cloudbrowser-instanties volledig geïsoleerd, en afgezien van rapportagegegevens, opname (indien ingeschakeld) en sessie-informatie, worden de gegevens na afloop van een co-browsersessie gewist.

Er is ook een *Stop*-knop beschikbaar voor de eindgebruiker tijdens de gehele ondersteuningssessie – de eindgebruiker kan de ondersteuningssessie op elk moment beëindigen door op deze knop te klikken.

3.3. Perimeterbescherming en inbraakdetectie

De GoTo-netwerkarchitectuur op locatie is onderverdeeld in openbare, privé- en iLO-beheernetwerkzones (Integrated Lights-Out). De openbare zone bevat servers die op het internet zijn gericht, en al het verkeer dat dit netwerk binnenkomt moet door een firewall. Hierbij is alleen vereist netwerkverkeer toegestaan; al het andere netwerkverkeer wordt geweigerd en er wordt geen netwerktoegang toegestaan vanuit de openbare zone naar de privé- of iLO-beheernetwerkzones.

De privénetwerkzone host administratieve en monitoringssystemen op applicatieniveau, en de iLO-beheernetwerkzones zijn ingericht voor het beheren en monitoren van de hardware en netwerken. Toegang tot deze netwerken is beperkt tot bevoegde medewerkers via tweeledige verificatie.

Daarnaast maakt GoTo gebruik van maatregelen ter bescherming van de perimeter, waaronder een DDoS-preventieservice (Distributed Denial of Service) van een derde partij in de cloud, die ontworpen is om te voorkomen dat onbevoegd netwerkverkeer onze productinfrastructuur binnendringt.

3.4. 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.

3.5. Fysieke beveiliging

Fysieke beveiliging van 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 GoTo-management controleert minstens elk kwartaal de logbestanden ten aanzien van de fysieke toegang tot datacenters en serverruimtes. Daarnaast verliest eerder geautoriseerd personeel bij ontslag direct het recht op fysieke toegang tot de datacenters.

3.6. Back-up van gegevens, noodherstel en beschikbaarheid

De productiedatacenters maken gebruik van redundante snelle netwerkverbindingen. Er zijn pools van web- en gateway servers in geografisch verspreide datacenters. Loadbalancers verdelen het netwerkverkeer en houden de beschikbaarheid van deze servers in stand in het geval van storingen van servers of datacenters.

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.

3.7. Bescherming tegen malware

Op alle servers van Rescue Live Guide wordt malwarebeschermingssoftware met auditlogbestanden geïnstalleerd. Meldingen die duiden op mogelijke kwaadwillige activiteiten worden doorgestuurd naar het passende responsteam.

3.8. Versleuteling

GoTo houdt zich aan een cryptografische standaard die overeenkomt met aanbevelingen van brancheverenigingen, overheidspublicaties en andere erkende normgroepen. De cryptografische standaard wordt periodiek herzien en gebruikte technologieën en vercijferingen kunnen worden bijgewerkt in overeenstemming met het ingeschatte risico en de marktacceptatie van nieuwe standaarden.

3.8.1. Versleuteling tijdens de overdracht

Al het netwerkverkeer dat GoTo-datacenters in en uit gaat, inclusief alle Klantcontent, wordt tijdens de overdracht versleuteld. Ter bescherming tegen afluisteren, wijzigingen of replay-aanvallen, worden IETF-standaard TLS-protocollen (Transport Layer Security) gebruikt om alle communicatie tussen eindpunten en onze services te beschermen. Onze services ondersteunen de volgende of nog betere versleutelingprotocollen (indien van toepassing): TLS 1.2, 2048-bits RSA en sterke AES-256-blokvercijferingen met een 384-bits SHA-2-algoritme.

3.8.2. Versleuteling tijdens de opslag

Rescue Live Guide-configuraties, sessiegegevens en opnamebestanden worden tijdens de opslag versleuteld met 256-bits AES.

3.9. 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 en afhankelijk van de ernst van de geïdentificeerde kwetsbaarheden worden herstelmaatregelen getroffen.

Kwetsbaarheden worden ook gecommuniceerd en beheerst met maand- en kwartaalrapporten voor zowel de ontwikkelingsteams als het management.

3.10. 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 Rescue Live Guide 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 voor de Rescue-service in het kader van Service Organization Control (SOC) 2 Type 2 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 geïdentificeerde beveiligingsgebeurtenissen in interne systemen en services, te beheren, te identificeren en op te lossen, waaronder de Rescue Live Guide-service. 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 indien nodig naar het management te escaleren. Medewerkers kunnen beveiligingsincidenten melden via e-mail, telefoon en/of 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 codeanalyse, 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. Rescue Live Guide 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.

Met de Data Residency-optie van Rescue Live Guide kunt u een locatie kiezen voor de opslag van gegevens van eindgebruikers: in de EU (Frankfurt, Dublin) of in de VS. GoTo garandeert dat diegenen die kiezen voor gegevensopslag in de EU exclusief verbinding maken met datacenters binnen de EU, en dat gebruikersgegevens uitsluitend binnen de gekozen regio worden bewaard.

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 persoonsgegevens. GoTo biedt zijn klanten SCC's, soms ook bekend als de Modelbepalingen 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 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 Rescue Live Guide 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 Rescue Live Guide voor bepaalde soorten informatie te beperken. Tenzij de Klant schriftelijke toestemming van GoTo heeft, mogen de volgende gegevens niet worden geüpload naar of gegenereerd in Rescue Live Guide (noch door de Klant, noch door hun eindgebruikers):

- Door de overheid uitgegeven identificatienummers en afbeeldingen van identificatiedocumenten.
- Informatie met betrekking tot de gezondheid van een persoon, inclusief maar niet beperkt tot Beschermd Gezondheidsinformatie (PHI; Protected Health Information), zoals geïdentificeerd in de Amerikaanse Health Insurance Portability and Accountability Act (HIPAA) van 1996, en daaraan gerelateerde 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 Rescue Live Guide 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.

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. 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 gebruikersoverwegingen 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 gegevensverwerking 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.