Internationale Übermittlung von Daten: Häufig gestellte Fragen

Datum der Veröffentlichung: 27. September 2021

EINLEITUNG

Als das globale Unternehmen für „ortsunabhängiges Arbeiten“ bietet LogMeIn Produkte an, die die Art und Weise vereinfachen, wie Menschen miteinander und mit der Welt um sich herum in Kontakt treten. Sie helfen sowohl Fachleuten als auch Unternehmen, Interaktionen sinnvoller zu gestalten, Beziehungen zu vertiefen und bessere Ergebnisse zu erzielen. Mit Nutzern in nahezu jedem Land weltweit pflegen wir ein globales Datenschutzprogramm. Dieses soll die rechtmäßige Übermittlung von Daten, die uns von unseren Kunden, Nutzern und deren Endnutzern anvertraut werden, schützen und ermöglichen.

Dieses Dokument soll unseren geschätzten Kunden, Nutzern und Endnutzern Antworten auf einige häufig gestellte Fragen zu den Datenübertragungspraktiken von LogMeIn bei der Übermittlung personenbezogener Daten in Gebiete außerhalb der Europäischen Union („EU“), des Europäischen Wirtschaftsraums („EWR“) und des Vereinigten Königreichs („UK“) geben, darunter:

- Mechanismen der Datenübermittlung (z. B. die Standardvertragsklauseln);
- Transparente Informationen über den Ort und die Art der Verarbeitung;
- Informationen, die bei einer eventuell erforderlichen Folgenabschätzung der Datenübermittlung helfen sollen;
- Informationen über die Datenschutz- und Sicherheitspraktiken von LogMeIn; und
- Ergänzende Maßnahmen zum Datenschutz.

HÄUFIG GESTELLTE FRAGEN („FAQ“)

Welche Kategorien von personenbezogenen Daten erfasst und verarbeitet LogMeIn für die Kunden von LogMeIn?

LogMeIn ist bestrebt, die Arten und Kategorien personenbezogener Daten, die das Unternehmen von seinen Nutzern erhebt und im Namen seiner Nutzer verarbeitet, auf die Informationen zu beschränken, die für die Bereitstellung und den Betrieb der LogMeIn-Dienstleistungen erforderlich sind. Letztendlich hängt die Art der von LogMeIn erhobenen und verarbeiteten Informationen von der jeweiligen LogMeIn-Dienstleistung und dem Anwendungsfall des jeweiligen Kunden ab.

Darüber hinaus ist es wichtig zu wissen, dass die Verarbeitung Personenbezogener Daten durch LogMeIn bei der Bereitstellung unserer Dienstleistungen im Einklang mit den Anweisungen der Nutzer erfolgt, die, sofern nicht in einem separaten Schreiben anders vereinbart, in Form der LogMeIn-Nutzungsbedingungen (einschließlich aller in diesem Zusammenhang ausgefertigten Datenverarbeitungsnachträge) vorliegen. Weitere Informationen zu den Kategorien und Arten von Informationen, die LogMeIn verarbeiten kann, finden Sie in den rechtlichen Nutzungsbedingungen und dem Datenverarbeitungsnachtrag von LogMeIn unter www.logmein.com/legal sowie in der entsprechenden Dokumentation zu den betrieblichen Datenschutz- und Datensicherheitskontrollen unter www.logmein.com/trust.

Wo befinden sich die Rechenzentren von LogMeIn?

Um eine ausreichende Dienstverfügbarkeit, Betriebszeit und Redundanz zu gewährleisten, die erforderlich sind, um unserer globalen Nutzerbasis die bestmögliche Nutzererlebnis zu bieten, setzt LogMeIn eine Kombination aus Kolokationseinrichtungen und Cloud-Hosting-Anbietern in Australien, Brasilien, Deutschland, Indien, Irland, dem Vereinigten Königreich, den Vereinigten Staaten und Singapur ein. In gleicher Art und Weise hat LogMeIn Angestellte und/oder Betriebsstätten in Australien, Brasilien, Kanada, Guatemala, Deutschland, Ungarn, Indien, Irland, Israel, Mexiko, dem Vereinigten Königreich und den Vereinigten Staaten. Dies bedeutet jedoch nicht, dass

personenbezogene Daten in all diesen Regionen gehostet, verarbeitet oder zugänglich gemacht werden. Die dienstleistungsspezifischen Datenzentren sind in der entsprechenden Offenlegung der Unterauftragsverarbeiter im Abschnitt „Produktressourcen“ in unserem Trust and Privacy Center unter www.logmein.com/trust aufgeführt.

Wo kann ich Informationen über die Unterauftragsverarbeiter von LogMeIn finden?

Dienstleistungsspezifische Offenlegungen bezüglich Rechenzentrum und Regionen der externen Unterauftragsverarbeiter, die zur Erbringung unserer Dienstleistungen eingesetzt werden, sind in den maßgebenden Offenlegungen zu den Unterauftragsverarbeitern näher angegeben, die im Abschnitt Produktressourcen unseres Trust & Privacy Center (www.logmeininc.com/de/trust) zu finden sind. In ähnlicher Weise veröffentlicht LogMeIn eine Offenlegung seiner hundertprozentigen Tochtergesellschaften, die in der Offenlegung der Konzernunternehmen zu finden ist, die in LogMeIn's Trust & Privacy Center verfügbar ist.

EU-Übermittlung von personenbezogenen Daten

Was ist eine internationale Übermittlung von personenbezogenen Daten?

Eine internationale Datenübermittlung liegt vor, wenn personenbezogene Daten in Gebiete außerhalb der EU bzw. des EWR übermittelt werden. Derzeit sehen die Datenschutzgesetze der EU bzw. des EWR vor, dass internationale Übermittlungen in ein „Drittland“, zum Beispiel, nur unter einer der in Kapitel 5 der DSGVO genannten Bedingungen erfolgen dürfen. Dazu gehören: a) ein formeller Angemessenheitsbeschluss der Europäischen Kommission in Bezug auf ein „Drittland“, dessen Gesetze als im Wesentlichen ähnlich oder „angemessen“ eingestuft werden; b) die Zustimmung wird erteilt; oder c) es werden angemessene Schutzmaßnahmen vereinbart, wie z. B. im Rahmen der Standardvertragsklauseln („SVK“).

Übermittelt LogMeIn personenbezogene Daten in Gebiete außerhalb der EU?

Mit Betriebsstätten in über 15 Ländern bietet LogMeIn Dienstleistungen an, die Millionen von Menschen und Unternehmen auf der ganzen Welt in die Lage versetzen, einfach und sicher ihre beste Arbeit zu erledigen – auf jedem Gerät, von jedem Ort und zu jeder Zeit. Abhängig von der jeweiligen Dienstleistung, kann LogMeIn gegebenenfalls Daten außerhalb der EU speichern und/oder verarbeiten. Für diese Übermittlungen hat LogMeIn Schritte unternommen, um sicherzustellen, dass angemessene Maßnahmen zum Schutz personenbezogener Daten in Übereinstimmung mit der DSGVO und den geltenden Datenschutzgesetzen und -verordnungen getroffen werden.

Unser Datenverarbeitungsnachtrag („DVN“) erklärt zusammen mit unseren standardmäßigen Nutzungsbedingungen wie LogMeIn in der Funktion als Dienstanbieter und Auftragsverarbeiter, personenbezogene Daten verarbeitet, um unsere Dienstleistungen bereitzustellen und zu betreiben. Weitere Informationen zu den Standorten der LogMeIn-Konzernunternehmen und Unterauftragsverarbeiter finden Sie in den Offenlegungen zu den Konzernunternehmen und Unterauftragsverarbeitern von LogMeIn im Trust and Privacy Center.

Was ist die rechtliche Grundlage (nach Kapitel 5 der DSGVO) für diese Übermittlungen?

Am 4. Juni 2021 veröffentlichte die Europäische Kommission eine aktualisierte Version der SVK, die für internationale Übermittlungen personenbezogener Daten verwendet werden sollen. Diese SVK wurden eigens abgefasst, um die zusätzlichen Anforderungen der DSGVO für die internationale Übermittlung personenbezogener Daten zu berücksichtigen. LogMeIn hat zwar im Allgemeinen verschiedene Übermittlungsmechanismen verwendet, um rechtmäßige Datenübermittlungen aus dem Gebiet und in das Gebiet der EU bzw. des EWR gemäß Kapitel 5 der DSGVO zu vereinfachen, aber wir werden uns weiterhin auf die SVK als primäre Rechtsgrundlage für EU/EWR-Datenübermittlungen stützen. Die aktuellste Version der SVK ist im DVN von LogMeIn integriert, der vorunterzeichnet und online zur Ausfertigung verfügbar ist.

Darüber hinaus ist es wichtig zu beachten, dass ein Kunde, der LogMeIn-Dienstleistungen aus der EU bzw. dem EWR erwirbt*, einen Vertrag mit der irischen Tochtergesellschaft von LogMeIn, LogMeIn Ireland Unlimited Company, abschließt. Der Dienstleistungsvertrag unterliegt irischem (mitgliedstaatlichem) Recht, einschließlich der geltenden Datenschutzgesetze (wie DSGVO und Data Protection Act 2018), und alle verarbeiteten Daten werden daher gemäß den geltenden Gesetzen Irlands geschützt.

*Beachten Sie bitte, dass Nutzer von LastPass, die in der EU bzw. dem EWR ansässig sind, einen Vertrag mit LastPass Ireland Limited abschließen. Darüber hinaus schließen Nutzer aus dem Vereinigten Königreich einen Vertrag mit LogMeIn Technologies UK Limited ab und die Vereinbarung unterliegt englischem Recht, unter anderem dem Data Protection Act.

Welche Schritte muss ich unternehmen, wenn mein Unternehmen Daten auf der Grundlage der SVK an LogMeIn übermittelt?

LogMeIn hat den DVN von LogMeIn aktualisiert, um die neuesten SVK einzubeziehen, und wir haben vorab unterzeichnete ausfertigbare Versionen online unter www.logmein.com/legal zur Verfügung gestellt.

Darüber hinaus ist zu beachten, dass die Europäische Kommission zwar bestätigt hat, dass alle vor dem 27. September 2021 ausgefertigten SVK bis zum 27. Dezember 2022 weiterhin für die rechtmäßige Übermittlung personenbezogener Daten verwendet werden können, dass aber alle Kunden, die den überarbeiteten DVN von LogMeIn mit den aktuellsten SVK früher ausfertigen möchten, dies unter www.logmein.com/legal tun können.

Sind die Unterauftragsverarbeiter von LogMeIn an die SVK gebunden?

Ja. LogMeIn führt nicht nur eine angemessene Due-Diligence-Prüfung aller seiner Unterauftragsverarbeiter durch, sondern unternimmt auch Schritte, um sicherzustellen, dass diese an einen Artikel 28-konformen Datenverarbeitungsnachtrag gebunden sind, der nicht weniger Schutz bietet als unser DVN und die SVK für rechtmäßige Übermittlungen personenbezogener Daten enthält und anwendet. LogMeIn arbeitet aktiv daran, sicherzustellen, dass die neuesten SVK die vorherigen SVK innerhalb der zulässigen Übergangsfrist (die am 27. Dezember 2022 endet) in Bezug auf die geltenden bestehenden Verträge des Unternehmens zur Unterverarbeitung ersetzen.

Stützt sich LogMeIn noch immer auf den Datenschutzschild für die Übermittlung personenbezogener Daten?

Nein. LogMeIn stützt sich nicht mehr länger auf die EU-US- und Schweiz-US-Datenschutzschild, um die Übermittlung personenbezogener Daten zu ermöglichen. Zusätzlch enthält der DVN des Unternehmens nicht mehr den Datenschutzschild als das verwendete Rahmenwerk und stützt sich stattdessen auf andere rechtmäßige Mittel der Datenübermittlung, die gemäß Kapitel 5 des DSGVO zulässig sind, einschließlich der SVK. Weitere Informationen zu den Übermittlungsmechanismen von LogMeIn finden Sie in unserem Trust and Privacy Center.

Hat der Brexit Auswirkungen auf die internationale Datenübermittlungen von LogMeIn?

Nein. Am 28. Juni 2021 erließ die Europäische Kommission zwei Angemessenheitsbeschlüsse für das Vereinigte Königreich, die die rechtmäßige Übermittlung personenbezogener Daten aus der EU in das und aus dem Vereinigten Königreich ermöglichen, ohne dass LogMeIn oder unsere Kunden etwas unternehmen müssen. Wir beobachten weiterhin die Entwicklungen im Vereinigten Königreich in Bezug auf potenzielle neue britische SVK, die, wenn sie genehmigt und als notwendig erachtet werden, in eine spätere überarbeitete Version unseres DVN aufgenommen werden, um sicherzustellen, dass unsere Kunden im Vereinigten Königreich weiterhin rechtmäßige Datenübermittlungen vornehmen können. In der Zwischenzeit können Kunden weiterhin unseren aktuelle DVN ausfertigen (zu finden unter www.logmein.com/legal), der

darauf ausgelegt ist, eine rechtmäßige Übermittlung nach und aus dem Vereinigten Königreich zu ermöglichen.

Welche technischen und organisatorischen Maßnahmen hat LogMeIn zum Schutz personenbezogener Daten ergriffen?

Im Rahmen des Engagements von LogMeIn für den Datenschutz und die Datensicherheit haben wir zusätzliche technische Maßnahmen zur Datensicherheit und zum Schutz der Privatsphäre, einschließlich Verschlüsselung, eingeführt, die über die Mindestanforderungen der SVK hinausgehen. Jedes unserer Produktangebote hat seine eigenen produktspezifischen technischen und organisatorischen Maßnahmen implementiert, darunter insbesondere:

- **Verschlüsselung**: Die Verwendung der Transportschichtsicherheit (der „TLS"-Verschlüsselung) v1.2 zum Schutz und zur Reduzierung des Risikos des Abhörens oder Abfangens von Daten während der Übertragung (z. B. der Kommunikation während eines „Computer Audio"- oder „VoIP"-Anrufs).
- **Grundsätze der Sicherheit und des Datenschutzes**: Ein unternehmensweites Secure Development Lifecycle („SDL") Programm, das Sicherheits- und Datenschutzprinzipien in relevanten Phasen des Entwicklungsprozesses berücksichtigt und Entwickler bei der Erstellung hochsicherer Software, der Einhaltung von Sicherheitsanforderungen und der Reduzierung von Entwicklungskosten unterstützt.
- **Privacy-by-Design**: Ebenso halten wir die Standards und Anforderungen des Privacy-by-Design, d. h. der Datenvermeidung und Datensparsamkeit, sowie die allgemeinen Sicherheits- und technischen Datenschutzstandards ein, um sicherzustellen, dass unsere Produkte die Datenschutz- und Sicherheitsrichtlinien in allen Aspekten des Geschäftsbetriebs berücksichtigen.
- **Sicherheits- und Datenschutzbeurteilungen/Frameworks von Dritten**: Die Datensicherheits- und/oder Datenschutzprogramme von LogMeIn werden regelmäßig anhand anerkannter, von Dritten geprüfter und validierter Standards bewertet, darunter:
    - Das Amerikanische Institut für Wirtschaftsprüfer („AICPA") Service Organization Control Report #2 („SOC2") Typ II
    - AICPA Service Organization Control Report #3 („SOC3") Type II
    - Bundesamt für Sicherheit in der Informationstechnik („BSI") Kriterienkatalog C5 (Cloud Computing Compliance Criteria Catalogue)
    - ISO 27001 (für LogMeIn Rescue und GoToAssist Remote Support v5)
    - TRUSTe - Datenschutzzertifizierung für Unternehmen
    - APEC Cross Border Privacy Rules („CBPR") und Privacy Recognition for Processors („PRP")

  Zu den oben genannten Sicherheitsstandards gehören robuste Zugangskontrollen und -verfahren sowie Verfahren zur Verschlüsselung, Zugangsverwaltung, Vertraulichkeit und Sicherheit.
- **Belastbare interne Programme zur Einhaltung von Datenschutz und gesetzlichen Vorschriften:** Diese Programme, die von Fachexperten und geschulten Fachleuten aus den Rechts-, Sicherheits- und Governance-, Risiko- und Compliance-Gruppen („GRC") von LogMeIn überwacht werden, helfen uns, Richtlinien, Verfahren und Abläufe aufrechtzuerhalten, um sicherzustellen, dass LogMeIn über die geltenden Datenschutzregeln und -verordnungen informiert ist und diese einhält. Die internen Teams von LogMeIn bewerten und verbessern kontinuierlich unsere Datenschutzprogramme und führen unter anderem jährliche interne Datenschutzaudits durch (um die Einhaltung der DSGVO, des CCPA sowie anderer anwendbarer Datenschutzgesetze zu überprüfen), um dieses Ziel zu erreichen.

Detaillierte und produktspezifische Informationen zu diesen zusätzlichen technischen Datensicherheits- und Datenschutzmaßnahmen finden Sie in der Dokumentation der betriebliche Datenschutz- und Datensicherheitskontrollen von LogMeIn, die im Abschnitt „Produktressourcen" unseres Trust & Privacy Center (www.logmeininc.com/de/trust) verfügbar ist. Eine Auswahl an technischen und organisatorischen Maßnahmen für einige unserer beliebtesten Produkte haben wir in Anhang A zusammengestellt.

Folgenabschätzungen für die Übermittlung

Was ist eine Folgenabschätzung für die Übermittlung (Folgenabschätzung)?

Im Anschluss an die Entscheidung des Europäischen Gerichtshofs in der Rechtssache C-311/18, die häufig als „Ungültigkeitserklärung des Privacy Shield" oder „Schrems II" bezeichnet wird, hat die Europäische Kommission überarbeitete SVK veröffentlicht, und der Europäische Datenschutzausschuss (European Data Protection Board – „EDPB") hat seine endgültigen Empfehlungen für zusätzliche Maßnahmen zur Gewährleistung der Einhaltung der Datenschutzgesetze bei der Übermittlung personenbezogener Daten in Gebiete außerhalb der EU bzw. des EWR veröffentlicht. Infolgedessen wurde empfohlen, dass „Datenexporteure" (d. h. LogMeIn-Kunden) von Fall zu Fall prüfen, ob die Gesetze des Drittlandes ein Schutzniveau für personenbezogene Daten bieten, das im Wesentlichen dem der EU bzw. des EWR entspricht. Falls dies nicht der Fall ist, muss der Datenexporteur feststellen, ob der „Datenimporteur" (d. h. LogMeIn) geeignete zusätzliche Maßnahmen ergriffen hat, um das erforderliche Schutzniveau zu gewährleisten.

LogMeIn hat die Datenschutz- und Sicherheitsprogramme des Unternehmens so konzipiert, dass ein angemessenes Datenschutzniveau im Einklang mit geltendem Recht gewährleistet ist. Wir haben die zusätzlichen Maßnahmen und Sicherheitsvorkehrungen, die wir getroffen haben, um diese Zusicherungen zu geben, in dieser FAQ beschrieben (siehe „*Welche technischen und organisatorischen Maßnahmen hat LogMeIn zum Schutz personenbezogener Daten ergriffen?*", sowie die Richtlinien, Verfahren und Unterlagen, auf die im Folgenden direkt verwiesen wird).

Welche weiteren Ressourcen stellt LogMeIn seinen Kunden für die Durchführung einer Folgenabschätzung zur Verfügung?

Die folgenden Ressourcen können LogMeIn-Kunden bei der Durchführung einer Folgenabschätzung in Bezug auf unsere Dienstleistungen helfen:

- Trust and Privacy Center
- EDPB-Empfehlungen 01/2020 zu ergänzenden Maßnahmen
- Offenlegung von Unterauftragsverarbeitern
- Produktressourcen
- Richtlinie zu Anfragen staatlicher Stellen
- DSGVO-Whitepaper
- Whitepaper des US-Justizministeriums zu Schrems II
- LogMeIn Datenverarbeitungsnachtrag

Anfragen staatlicher Stellen

Fällt LogMeIn unter den 50 U.S. Code § 1881a („FISA 702“) oder unterliegt das Unternehmen auf andere Art und Weise den Anforderungen der Executive Order 12333?

LogMeIn unterliegt den geltenden Gesetzen und Vorschriften der einzelnen Länder, in denen wir tätig sind. Es ist wichtig zu beachten, dass LogMeIn zwar seinen Hauptsitz in den Vereinigten Staaten haben kann, Kunden mit Sitz in der EU jedoch mit einem in einem Mitgliedstaat ansässigen LogMeIn-Unternehmen (LogMeIn Ireland Unlimited Company*) Verträge abschließen und Datenschutzbestimmungen vereinbaren. Deshalb müssten alle von der Regierung der Vereinigten Staaten oder den Strafverfolgungsbehörden eingehenden Anfragen unbeschadet der Frage, ob sie Teil der obenstehenden Bestimmungen, des US-amerikanischen Cloud Act oder in sonstiger Weise sind, rechtsgültig innerhalb und nach dem Recht der Republik Irland oder des jeweiligen Mitgliedsstaates anerkannt werden. Weitere Informationen über die Vorgehensweise von LogMeIn bei Anfragen von staatlichen Stellen zum Datenzugriff finden Sie in unserer Richtlinie zu Anfragen staatlicher Stellen.

*Beachten Sie bitte, dass Nutzer von LastPass aus der EU bzw. dem EWR, einen Vertrag mit LastPass Ireland Limited abschließen. Darüber hinaus schließen Nutzer aus dem Vereinigten Königreich einen Vertrag mit LogMeIn Technologies UK Limited ab und die Vereinbarung unterliegt englischem Recht, unter anderem dem Data Protection Act.

Welchen Ansatz verfolgt LogMeIn bei Anträgen von staatlichen Stellen auf Datenzugriff?

LogMeIn hat eine Richtlinie zu Anfragen staatlicher Stellen veröffentlicht, die erstellt wurde , um eine größere Transparenz im Hinblick auf die Leitlinien zu schaffen, die von LogMeIn verwendet werden, um festzulegen, wie und wann wir Anfragen von Strafverfolgungsbehörden, Behörden der nationalen Sicherheit und anderen Aufsichtsbehörden („Staatliche Stellen“) bearbeiten, die sich auf Informationen zu unseren Kunden, ihren Mitarbeitern und/oder deren Nutzern beziehen. LogMeIn wird alle internationale Anfragen staatlicher Stellen auf Länder- und Einzelfallbasis prüfen, um unsere lokalen gesetzlichen Verpflichtungen im Vergleich zu unseren Zusagen zur Förderung der öffentlichen Sicherheit und Privatsphäre der Anwender in Erwägung ziehen und abwägen zu können. LogMeIn gibt grundsätzlich keine Kundendaten an staatliche Stellen weiter, es sei denn, die dies verlangende Partei ist nach geltendem Recht ordnungsgemäß autorisiert diese Informationen zu verlangen und hat LogMeIn eine gültige Vollmacht, eine Vorladung (mit Strafandrohung), eine gerichtliche Verfügung oder einen gleichwertigen rechtlichen Vorgang vorgelegt.

An wen kann ich mich wenden, wenn ich Fragen zu den Datenschutzpraktiken von LogMeIn habe?

Wenn Sie weitere Fragen zu den Datenschutzpraktiken von LogMeIn haben, wenden Sie sich bitte an privacy@logmein.com. Bitte beachten Sie, dass LogMeIn den Kunden des Unternehmens keine Rechtsberatung anbieten darf. Wir empfehlen Ihnen, bei Fragen zur Rechtmäßigkeit Ihrer eigenen Datenschutz-Compliance-Programme Ihren eigenen Rechtsbeistand zu konsultieren.

Anhang A – Technische und organisatorische Maßnahmen

Im Folgenden finden Sie eine Auswahl „zusätzlicher" technischer und organisatorischer Maßnahmen, die bei einigen unserer beliebtesten Angebote zum Einsatz kommen (vollständige Informationen zu allen LogMeIn-Dienstleistungen finden Sie unter www.logmein.com/trust):

Der gesamte **GoToConnect**-Netzwerkverkehr, der in die und aus den LogMeIn-Rechenzentren fließt, einschließlich aller Kundeninhalte, wird während der Übertragung mit Verfahren bis hin zu TLS v1.2 (sofern unterstützt) verschlüsselt. Voicemail-Aufzeichnungen von Kunden, Voicemail-Ansagen ebenso wie Aufzeichnungen, Protokolle und Notizen von Besprechungen oder Anrufaufzeichnungen werden bei der Speicherung in der Cloud-Hosting-Umgebung von LogMeIn mit einer 256-Bit-Verschlüsselung nach dem Advanced Encryption Standard („AES") verschlüsselt. Wenn ein Kunde eine genauere Kontrolle über seine Informationen benötigt, kann er sich dazu entschließen, die Aufzeichnungen von Besprechungen lokal an einem Ort seiner Wahl zu speichern, und er kann sich auch dazu entschließen, seine eigene Amazon Web Service („AWS") S3-Cloud-Hosting-Instanz (an einem AWS-Standort seiner Wahl) für Anrufaufzeichnungen zu nutzen. Das integrierte Dienstleistungsangebot von GoToConnect nutzt die proprietäre Identitätsverwaltungsplattform von LogMeIn für die Kundenbereitstellung, bietet Single Sign-On („SSO") unter Verwendung der Security Assertion Markup Language („SAML") und ist über eine Anwendungsprogrammierschnittstelle („API") direkt mit der GoToMeeting-Plattform von LogMeIn integriert. GoToConnect bietet auch zuverlässige administrative Kontrollen, wie z. B. die Möglichkeit für Administratoren von Kundenkonten, Passwortrichtlinien zu konfigurieren und die Verwendung von SAML für die Anmeldung zu verlangen.

GoToMeeting ermöglicht die Nutzung der Bildschirmfreigabe und der Chat-Sitzungen über einen End-to-End-verschlüsselten („E2EE") Kanal unter Verwendung eines Sitzungskennworts – was dazu führt, dass die Informationen zur Bildschirmfreigabe und zum Chat weder für LogMeIn noch für andere Personen außer dem Kunden und seinen Teilnehmern, die über dieses vom Kunden bereitgestellte Kennwort verfügen, verfügbar sind. Darüber hinaus können GoToMeeting-Nutzer wählen, ob sie die Sitzungsaufzeichnungen lokal auf ihrem Gerät (oder an einem anderen Ort ihrer Wahl) speichern möchten, sodass sie die Informationen sowohl innerhalb der Grenzen der EU als auch in einer Weise aufbewahren können, die für LogMeIn (oder andere über LogMeIn) unzugänglich ist. Soweit sich GoToMeeting-Nutzer für die Nutzung des Cloud-Hostings von LogMeIn entscheiden, werden ihre Sitzungsaufzeichnungen, Protokolle und Notizen in einer US-basierten AWS-Instanz gespeichert und im Ruhezustand mit AES-256-Bit verschlüsselt. Zusätzliche Optionen stehen auch zur Verfügung, um Chat-Protokolle lokal bei einem Nutzer zu speichern und die Chat-Erfassung oder das Business Messaging zu deaktivieren.

LastPass verwendet für alle Ebenen seines Angebots ein Zero-Knowledge-Modell, was bedeutet, dass die Entschlüsselung der sensiblen Vault-Inhalte eines Nutzers vollständig auf Nutzer- und Nutzergerätebene erfolgt (so genannte „rein lokale Verschlüsselung"). Mit anderen Worten: LogMeIn hat keinen Zugriff auf entschlüsselte sensible Vault-Informationen jeglicher Art – dies wird nicht nur durch die Entschlüsselung und Verschlüsselung auf Nutzerebene ermöglicht, sondern auch dadurch, dass nur der Nutzer das Master-Kennwort verwaltet, das als Verschlüsselungsschlüssel dient, auf das LogMeIn niemals in unverschlüsselter Form Zugriff hat. Die Verschlüsselung auf Geräteebene von LastPass implementiert eine AES-256-Bit-Verschlüsselung, PBKDF2 SHA256 Bit, die gesalzen und gehasht wird, um vollständige Sicherheit in der Cloud zu gewährleisten. Erfahren Sie hier mehr darüber, wie LastPass die Vault-Daten sichert. Darüber hinaus können LastPass-Nutzer bei der Erstellung eines neuen Kontos wählen, ob ihr verschlüsselter Vault entweder in Australien, Europa, Singapur oder den Vereinigten Staaten gehostet werden soll.

Rescue verwendet eine AES-256-Bit-Verschlüsselung für benutzerdefinierte Berichte und Chatsitzungen und setzt außerdem eine proprietäre Peer-to-Peer-Architektur ein, bei der Remote-Sitzungen, die zwischen einem LogMeIn-Kunden und seinem Endnutzer oder der betroffenen Person initiiert werden, nicht nur bei der Übertragung mit TLS v1.2 (sofern unterstützt) verschlüsselt werden, sondern auch direkt zwischen den Parteien – Rescue stellt die Verbindung über ein Gateway her und trennt sich, sobald die Verbindung hergestellt ist. Das proprietäre Weiterleitungsprotokoll für den Schlüsselaustausch von Rescue ist so konzipiert, dass es selbst gegen ein Abfangen oder das Abhören der LogMeIn-Infrastruktur abgesichert ist. Die Verbindung zwischen dem Client und dem Host wird durch das Gateway unterstützt, um sicherzustellen, dass der Client unabhängig vom Netzwerkaufbau eine Verbindung

zum Host herstellen kann. Da der Host bereits eine TLS-Verbindung zum Gateway aufgebaut hat, leitet das Gateway den TLS-Schlüsselaustausch des Clients über eine proprietäre Anforderung zur Neuaushandlung des Schlüssels an den Host weiter. Dies führt dazu, dass der Client und der Host TLS-Schlüssel austauschen, ohne dass das Gateway den Schlüssel erfährt. Bei der Erstellung eines neuen Kontos können Kunden bei LogMeIn Rescue auch zusätzlich beantragen, dass ihr Konto so konfiguriert wird, dass Kundeninhalte (einschließlich aller darin enthaltenen personenbezogenen Daten) in der EU oder den Vereinigten Staaten gespeichert werden. Rescue sammelt nicht nur standardmäßig begrenzte Informationen während einer Remote-Sitzung, sondern bietet seinen Nutzern auch zusätzliche Möglichkeiten zur Datenminimierung, wie z. B. die Möglichkeit, die Chat-Funktion zu deaktivieren, sowie die Möglichkeit, die Sammlung von IP-Adressen von Nutzern oder ihren betroffenen Personen zu Berichtszwecken zu deaktivieren.