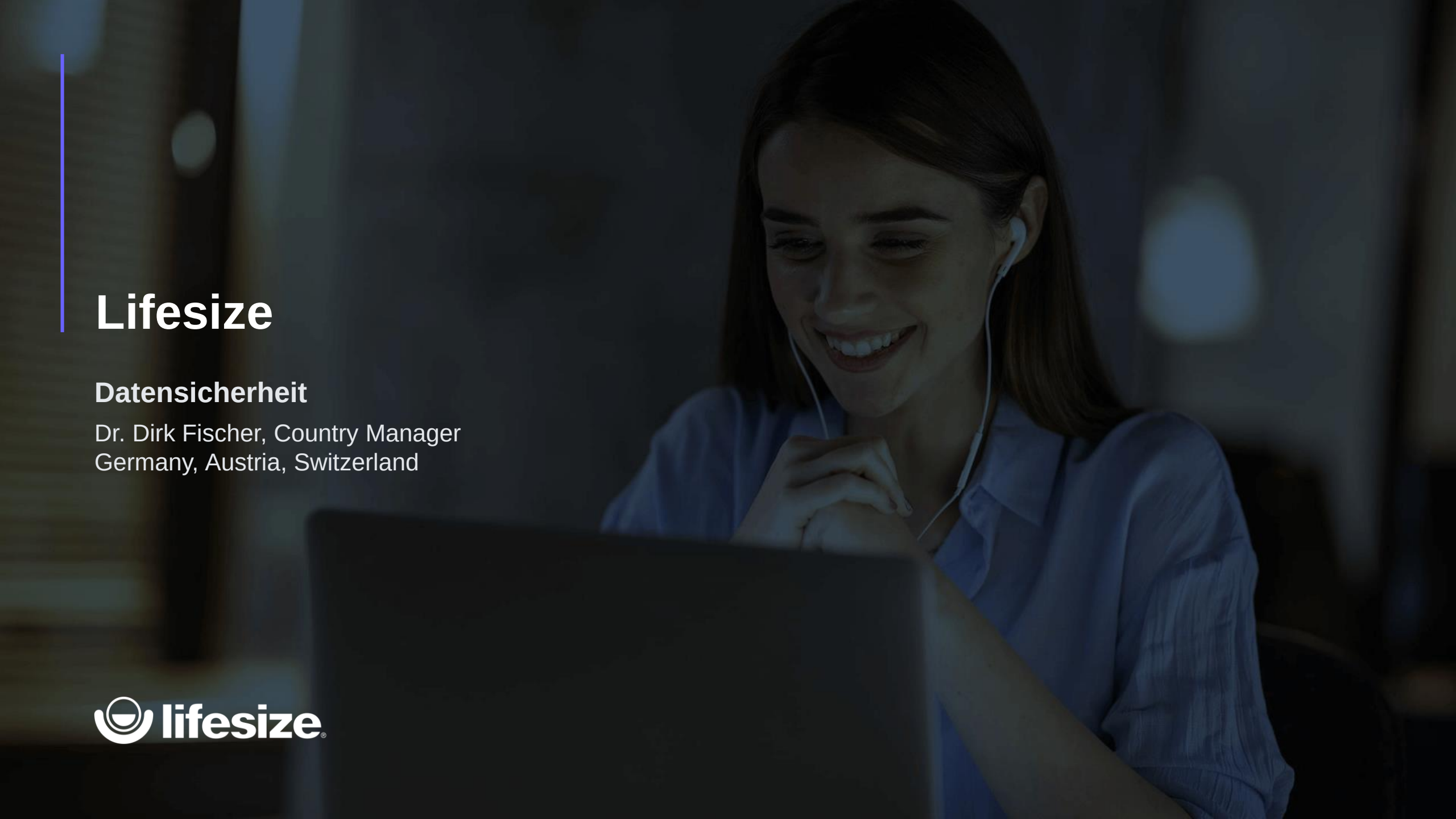

Lifesize

Datensicherheit

Dr. Dirk Fischer, Country Manager
Germany, Austria, Switzerland

lifesize

Lifesize & Datenschutz

- DPA **inkl. SCC** für **GDPR** Compliance**:** https://www.lifesize.com/~/media/Documents/Other%20Documents/Legal%20Compliance/data-processing/Lifesize%20%20Data%20Processing%20Addendum%20Customer%20%2008Sep20%20fillable%20LS%20signed.ashx?la=de
- Health Insurance Portability and Accountability Act-Konformität **(HIPAA):** blob:https://www.lifesize.com/199359cd-6a19-4099-b712-87b7f8d3d526
- Privacy Policy: https://www.lifesize.com/en/company/legal-notices/privacy
- Lifesize Security Overview: https://www.lifesize.com/~/media/Documents/Related%20Resources/Product%20Papers/Lifesize%20Cloud%20Security.ashx?la=en
- Mehr Informationen im Lifesize Trust Center: https://www.lifesize.com/en/trust-center

Schutz von Meta- und Mediadaten

- Grundsätzlich muss man bei Lifesize **unterscheiden** zwischen **Metadaten** (z. B. Stammdaten des Kunden, Call-Statistiken für kundenseitige Nutzungsreports, Name und E-Mail-Adresse des kundenseitigen IT-Administrators, Name und E-Mail-Adresse der kundenseitigen Lifesize Users, falls im Admin-Portal registriert) und **Mediadaten** (Video-, Audio-, Content-Traffic im Rahmen von Videokonferenzen).

- Die **Metadaten** werden auch in den USA zwischengespeichert (siehe auch Seite 5 im Lifesize Security Overview: https://www.lifesize.com/~/media/Documents/Related%20Resources/Product%20Papers/Lifesize%20Cloud%20Security.ashx).

- Allerdings werden alle Daten bei Lifesize gemäß GDPR und **Standard Contractual Clauses** geschützt (siehe Lifesize DPA für GDPR Compliance): https://www.lifesize.com/~/media/Documents/Other%20Documents/Legal%20Compliance/data-processing/Lifesize%20%20Data%20Processing%20Addendum%20Customer%20%2008Sep20%20fillable%20LS%20signed.ashx?la=de

- Die **Mediadaten** werden grundsätzlich nicht gespeichert, sondern zwecks Ermöglichung der Videokonferenz temporär verarbeitet („Video communication data is transient in nature and encrypted in flight. Lifesize does not view, record or otherwise store any video conference media (audio, video or presentation)“, siehe https://www.lifesize.com/~/media/Documents/Related%20Resources/Product%20Papers/Lifesize%20Cloud%20Security.ashx).

- Der Lifesize Cloud Service ist auf **Amazon Webservices (AWS)** gehostet (für die AWS Zertifizierungen, siehe https://aws.amazon.com/de/compliance/programs/). Die für Sie geografisch nächstgelegene AWS Mediaregion befindet sich in **Frankfurt am Main**. Die Mediadaten werden immer in der geographisch nächstgelegenen Mediaregion gehostet. Die zweitnächstgelegene Mediaregion befindet sich in **Dublin** und übernimmt im Falle eines Ausfalls oder einer Überlastung der Frankfurter Mediaregion. Darüber hinaus nutzt Lifesize 7 weitere Mediaregionen weltweit, um geringe Latenzen an jedem Standort zu bieten.

Verschlüsselung

- The Lifesize service uses the **WebRTC standard** for all video communications regardless of call scenario (point-to-point or multiple participants) or device (Icons, pc/mac, IOS/Android).
- The call signaling connection from a device to the Lifesize service uses secure websocket over HTTPS. This connection uses a **SSL certificate that has been signed by a well-known root CA**. The signaling connection SSL certificate chain is **strictly validated by the client/endpoint**. This ensures that the signaling traffic used to setup a call is secure and is established with the Lifesize service (and not with any malicious "man-in-the-middle" entity). The call signaling over secure websockets contains the fingerprint of an SSL certificate that shall be used when setting up the DTLS connection. That ensures that the two WebRTC media processing entities know the certificate to expect from the peer at run-time.
- In order to encrypt media (audio, video, and presentation), **an SRTP private key is then negotiated between WebRTC media processing entities** over this DTLS connection. That connection does not need to traverse the same path as the signaling. The DTLS connection can be direct between two devices (in case of a **point-to-point** call), or it can be between a device and the video bridge hosted by Lifesize (for **multi participant calls**). The result is that each participant on a call uses a **unique key to encrypt their own media**. Further, each of these participants will again negotiate a new SRTP private key for every subsequent call. In other words, **each call participant negotiates a unique single-use key for media encryption on each and every call**.

Zugangskontrollen

- Access to key stores are **least-access** and limited to a small number of senior employees in our service operations team only.
- Any access is **logged for auditing**. Audit logs are even further restricted to prevent manipulation.
- The media encryption approach is complex and occurs in real time. Nevertheless, we observe a segregation of duties as an additional layer of security. While our **engineering** team may have the skill set to develop tools, they do **not have access** to the key store. Conversely, the limited members of our operations team that do have access, do not have the skill set to develop software tools to decrypt participant media.
- Lifesize has **not** developed any tool with which to **view or monitor** a customer’s meeting.
- All employees are subject to **background screens.**
- All employees are bound by **acceptable use, code of conduct, and confidentiality agreements.**
- All employees are required to **complete security awareness training** at time of hire and on an ongoing annual basis.

Lifesize & US Cloud Act

- The US CLOUD Act applies in very narrow circumstances and should not have any effect on Lifesize's EU Customers. The CLOUD Act allows US law enforcement agencies to compel US-based technology companies to turn over electronic records of US citizens & residents pursuant to a court-issued subpoena or search warrant, regardless of whether the data is stored on servers located in the US or on foreign soil. The Act came about because of a 2013 drug-trafficking case in which the FBI issued a search warrant for emails that a US citizen had stored on one of Microsoft's remtve servers in Ireland. Microsoft refused to turn over the emails because it argued the search warrant did not cover data stored outside of the US. Congress intervened by passing the CLOUD Act specifically to address this situation. **However, the CLOUD Act only applies if all three of the following elements is present: (1) target of the investigation is a US citizen or US resident,** (2) data is stored by a US tech company, and (3) US law enforcement agency obtains a valid search warrant or subpoena for the data. The CLOUD Act does not enable US law enforcement agencies to obtain data of EU citizens or residents. **Thus, the CLOUD Act should not impact Lifesize's EU Customers.**

- In the unlikely event we were issued a warrant for data for one of our customers, as long as we were not prevented from doing so by law, we **would notify the customer** as quickly as possible providing them time **to respond/contest the warrant and its application to their data**.

- It’s important to remember, the CLOUD Act still allows parties to go to court to challenge search warrants when there is a conflict of laws. One of the CLOUD Act’s most relevant sections for EU customers should be **Section 103(c)** which explicitly states that nothing in the relevant section should “be construed to modify or otherwise affect the common law standards governing the availability or application of comity analysis” under the relevant provisions. The protection of comity rights is of even greater importance with the passage of GDPR. EU customers can interpret GDPR’s relevant provisions and determine whether there is a conflict of laws that would mandate comity analysis. Especially as the EU does, customers can use common law rights to go to court to raise comity issues and protect EU data.

Ausrichtung von Lifesize auf HIPAA

- Lifesize richtet seinen Cloud Service darauf aus, Kunden aus dem Healthcare-Sektor zu unterstützen, welche den HIPAA einhalten wollen (siehe https://www.lifesize.com/en/resources/product-papers/lifesize-healthcare-solutions-and-hipaa-compliance).

- Der HIPAA umfasst sowohl datenschutzrechtliche als auch sicherheitsbezogene Regelungen in Bezug auf PHI („protected health information“). Lifesize hat die Datenschutz- und Sicherheitsanforderungen des HIPAA überprüft und seine Produkte, Richtlinien und Verfahren so ausgerichtet, dass seine Healthcare-Kunden in Übereinstimmung mit dem HIPAA die Lifesize Cloud Services nutzen können.

- Auf Wunsch kann Lifesize hier auch ein sog. „HIPAA Business Associate Agreement” (BAA) mit seinen Healthcare-Kunden unterzeichnen.

- Wichtig*: “Lifesize enables customers who are subject to HIPAA to leverage Lifesize’s secure environment to transmit **protected health information (PHI)** during real-time video conferences among participants who can legally receive such PHI. However, **customers should not use Lifesize’s services to record or store PHI**. Customers must ensure that all recording features, including Lifesize **Record & Share, Live Stream and Chat, are not used for PHI**. These features may only be used for purposes unrelated to PHI. A customer’s account **administrator may elect to disable these features** to ensure they are not used for PHI by the customer’s account users. For assistance with disabling account features, please contact a Lifesize customer support advocate.*

Nutzungsempfehlungen bei medizinischen Daten

- Ausschließlich Verwendung von **Lifesize Raumsystemen (Lifesize Icons)** und **Lifesize App.**
- **Keine** Verwendung der Lifesize **Record & Share-** (Recording), **Live Stream- und Chat-Features**.
- **Keine** Verwendung des optionalen **Audio Conferencing Features** (PSTN-Einwahl).
- Verwendung von **Single-Sign-On** (somit werden im Rahmen der Metadaten keine Admin- oder Nutzer-Passwörter von Lifesize gespeichert).
- Optional kann der Zugang zu einem virtuellen Lifesize Meetingraum auch per **PIN-Code** gesichert werden.
- Nachdem alle Teilnehmer einem virtuellen Lifesize Meetingraum beigetreten sind, kann dieser vom Moderator/Organisator via **Meeting Lock-Funktion** für weitere Teilnehmer gesperrt werden (so kann z. B. die Übertragung von Content mit Patientendaten erst danach begonnen werden).

lifesize®

Datenschutz auf Ebene der operativen Geschäftsprozesse

- **In der Privacy Policy** unter 8. Protection of Information | Quelle: https://www.lifesize.com/de/Firma/Rechtliches/Datenschutz
- **Im DPA** unter Section 4.4 in Verbindung mit Appendix 2 | Quelle: https://www.lifesize.com/~/media/Documents/Other%20Documents/Legal%20Compliance/data-processing/Lifesize%20%20Data%20Processing%20Addendum%20Customer%20%2008Sep20%20fillable%20LS%20signed.ashx?la=de

ToS, EULA, SLA

- Lifesize Terms of Service (ToS): https://www.lifesize.com/~/media/Documents/Other%20Documents/Legal%20Compliance/End%20User%20License%20Agreements/Lifesize%20Cloud%20Terms%20of%20Service%20TOS.ashx?la=en
- Lifesize End User License Agreement (EULA): https://www.lifesize.com/~/media/Documents/Other%20Documents/Legal%20Compliance/End%20User%20License%20Agreements/Hardware%20End%20User%20License%20Agreement%20EN.ashx
- Lifesize Cloud Extreme Support Service Level Agreement (SLA): https://www.lifesize.com/~/media/Documents/Other%20Documents/Support/Lifesize%20SLA.ashx?la=en


lifesize®