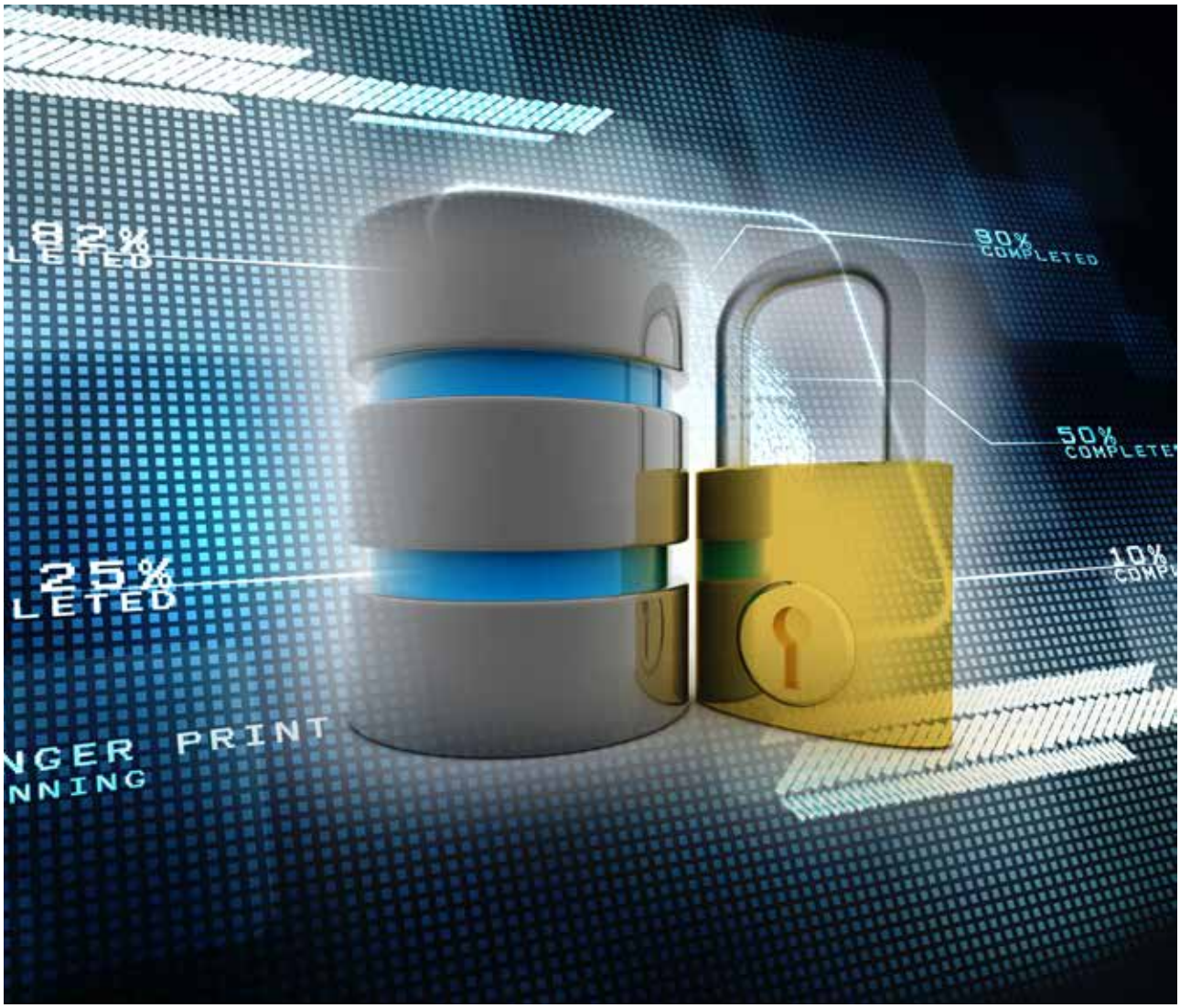
Insentis

NEW WORK
VIDEOKONFERENZEN – DATENSCHUTZ UND TECHNIK

DR. FRANK IMHOFF



Insentis

VIDEOKONFERENZEN – DATENSCHUTZ UND TECHNIK

Wichtige Regeln für sichere Videokonferenzen

Neben dem Telefon dürfte das mit Abstand häufigste genutzte Kommunikationswerkzeug im Homeoffice eine Videokonferenz-Lösung sein. Wobei diese heute in der Regel sehr viel mehr kann als nur Sprache und Kamerabilder zu übertragen. Mindestens das Teilen von Bildschirminhalten, zuletzt aber auch die enge Verknüpfung mit Cloud-Speicher und anderen Anwendungen ist eigentlich heute längst Stand der Technik. Je nach Arbeitsschwerpunkt, externen Kontakten, Kundenstrukturen oder Beteiligung an Projekten kommen dabei aber nicht selten auch unterschiedliche Videokonferenzsysteme zum Einsatz – je nachdem wer zu einem Termin eingeladen hat, wer welches System persönlich bevorzugt oder was ihm von seinem jeweiligen Unternehmen zur Verfügung gestellt wird.

Schon vor Corona waren einige dieser Kommunikationssysteme hinsichtlich Security und Datenschutz heftig umstritten. Das hat z.B. in den meisten Bundesländern und darüber hinaus auch noch von einzelnen kommunalen und regionalen Schulträgern für die die Schulen eigene Plattformen entwickelt wurden – häufig mit dem Argument, dass der Datenschutz ansonsten nicht zu gewährleisten sei. Leider scheitern diese Eigenentwicklungen dann aber oft an mangelnder Funktionalität und Kapazität der zugrundeliegenden Serverstrukturen.

Gliederung

Essentials

Wenig überraschend ist die Tatsache, dass die meisten Videoconferencing- und Collaboration-Lösungen in den USA entwickelt und dort auch betrieben werden. Videoconferencing ist naturgemäß eine Anwendung mit hohen Ansprüchen an die Übertragungsqualität und die zentralen Server. Daher lassen sich diese Lösung kaum im eigenen Haus betreiben, sondern nur in großen., weltweit verteilten Rechenzentren mit entsprechend leistungsfähigen Internet-Zugängen. Wenn dann auch noch der Anspruch hinzukommt, eine Zusammenarbeit über Kontinente hinweg, jederzeit komfortabel, hoch verfügbar und wirtschaftlich sinnvoll sicherzustellen, dann bleibt eigentlich nur die Nutzung entsprechender Cloud-Angebote.

Damit einher geht, dass unternehmenskritische Daten aber auch personenbezogene auf Server übertragen werden, die das nutzende Unternehmen nicht mehr unter Kontrolle hat und die zudem in den USA stehen oder zumindest von Firmen betrieben werden, die US-amerikanischen Gesetzten unterworfen sind. Das EU-US-Privacy Shield gibt es aber nicht mehr, daher ist für europäische Nutzer ein Vertrag über Auftragsverarbeitungs mit Standarddatenschutzklauseln nach Art. 46 Abs. 2 lit c DSGVO zwingend erforderlich. Viele Anbieter haben darauf reagiert und stellen entsprechende Muster zur Verfügung.

Aber damit allein ist es nicht getan. Weiterhin ergeben sich zahlreiche Fragestellungen hinsichtlich der sicheren Übertragung der Daten z.B. während einer Videokonferenz und die sichere Speicherung der Daten zwischen den einzelnen Konferenzen. Zwar verschlüsseln alle Anbieter irgendwie den sogenannten Payload, also die Video- und Audiodaten, aber was passiert z.B. damit auf den Servern, wenn eine Konferenz mit mehr als zwei Teilnehmern stattfindet? In diesem Fall muss eine entsprechende Mischung der Medienstreams stattfinden, so dass jeder Empfänger die jeweils anderen Teilnehmer sieht und den jeweiligen Sprecher hören kann.

Was passiert zudem mit den sogenannten Metadaten, also Daten zum Verbindungsaufbau der Videokonferenz, zu den beteiligten Teilnehmern, zur Nutzungsstatistik, zur Qualität der Übertragung, zu genutzten Adressbüchern, Profilen, zur genutzten Hardware, zu den Betriebssystemen oder Logdateien auf dieser Hardware etc.

Im Folgenden haben wir daher eine Übersicht über die derzeit häufig genutzten Videokonferenzlösungen zusammengestellt, um einen Überblick über die damit jeweils verbundenen Risiken und Möglichkeiten zur Reduzierung dieser Risiken zu geben. Dieser Überblick kann naturgemäß nicht vollständig und jederzeit auf dem aktuellen Stand sein, da sich z.B. die Nutzungsbedingungen der Hersteller und Betreiber fast schon täglich ändern und Updates, vom Nutzer zumeist unbemerkt, erfolgen. Es kann aber sehr wohl für Ihre Bewertung der Videokonferenzlösung in Hinsicht auf Ihre eigenen Anforderungen hilfreich sein.

Zoom

Die Videokonferenz-Software Zoom hat aufgrund der teilweise überstürzt eingeführten Homeoffice-Regelungen einen regelrechten Boom beim Einsatz in Unternehmen erfahren. Die monatlichen Nutzerzahlen stiegen innerhalb eines Jahres von 10 Millionen im Dezember 2019 auf über 200 Millionen im März 2020. Dennoch ist die Qualität von Zoom, gerade auch bei vielen Teilnehmern in einer Videokonferenz deutlich besser als bei den meisten anderen Anbietern. Auch sind in den letzten Monaten zahlreiche Kritikpunkte hinsichtlich der Technik beseitigt worden. Trotz dieser Anpassungen und Änderungen der Lizenzbestimmungen konnte Zoom bislang jedoch nicht alle Datenschutz-Anforderungen uneingeschränkt erfüllen. Das betraf zunächst vor allem die Gratis-Version von Zoom, bei der kostenlos Videokonferenzen von bis 45 Minuten durchgeführt werden konnten. Aber auch die kommerzielle Version gibt nach wie vor Anlass zur Kritik.

Zoom wird von Zoom Video Communications Inc., einem Softwareunternehmen mit Sitz im kalifornischen San José gehostet und betrieben. Inzwischen gibt es aber auch einen Europäischen „Cluster", der für neue Nutzer aus Europa genutzt wird. Ältere Nutzer müssen ggf. ihrem Wunsch Ausdruck verleihen, dorthin zu wechseln. Aber auch nach einem Wechsel in das „EU-Cluster" werden Betriebs- oder Metadaten in den USA verarbeitet. Zudem kann ein US - amerikanisches Unternehmen rechtlich nicht gänzlich ausschließen, dass US-Behörden nicht doch auch den Zugriff auf Rechenzentren im Ausland oder in der EU verlangen.

Um die Anforderungen der DSGVO hinsichtlich eines Auftragsverarbeitungsvertrags zu erfüllen, stellt Zoom einen aktualisierten Auftragsverarbeitungsvertrag mit Standardvertragsklauseln zur Verfügung. Teil davon ist ein eigenes Data-Processing-Addendum, das zum Download zur Verfügung steht. Die Berliner Behörde für den Datenschutz prüfte dieses „Zoom Global Data Processing Addendum" in der Version vom November 2020 und stellte dabei nach wie vor zahlreiche Mängel fest, die sich unter anderem aus unzulässigen Einschränkungen der Weisungsbindung, der Löschpflicht und der Kontrollrechte ergeben. Darüber hinaus behält sich die Zoom weiterhin unzulässige Datenexporte vor. Auf-

grund dieser rechtlichen Mängel erfolgte keine weitergehende technische Prüfung der Zoom-Lösung durch die Berliner Datenschutzbehörde.

Selbst viele US Firmen wie Google, NASA oder SpaceX haben Zoom verboten, weil die Sicherheitsbedenken der Unternehmen zu groß wurden. Unter anderem wurde aber Zoom in den letzten Monaten von zahlreichen Hacker-Angriffen heimgesucht, die über Sicherheitslücken in den Anwendungen ebenfalls Schadsoftware auf die Rechner der Nutzer schaffen konnten.

Aber auch hinsichtlich der technischen Möglichkeiten von Zoom ist Vorsicht geboten. So bietet Zoom die Möglichkeit, Gespräche und Video-Calls aufzuzeichnen. Solche Aufzeichnungsmöglichkeiten sind zwar hilfreich, bei Nutzung sollte dafür aber auch eine Einwilligung aller Beteiligten im Vornherein eingeholt werden. Alternativ müsste die Nutzung dieser Aufzeichnungsmöglichkeiten zentral unterbunden werden.

Zoom setzte darüber hinaus auch das sogenannte Attention Tracking ein. Dabei wird in einem Video-Call gemessen, ob der Teilnehmer die Videokonferenz aufmerksam verfolgt oder nebenbei etwas anderes macht (Prüfung, ob das Zoom-Fenster aktiv ist). Diese Einstellung ist jedoch eine datenschutzrechtlich höchst bedenkliche Einstellung und kann leicht missbraucht werden. Diese sollte nur verwendet werden, wenn Sie beispielsweise eine Fortbildungsveranstaltung anbieten, bei der Sie die Anwesenheit der Teilnehmer nachweisen müssen. Lt. einer Presseerklärung aus dem Frühjahr 2020 erklärte Zoom jedoch, dass das Attention-Tracking aus dem Tool entfernt wurde. Im Übrigen hat Zoom seine Datenschutzerklärung am 29.03.2020 aktualisiert und veröffentlicht seit 2020 auch Transparenzberichte zu ergriffenen Maßnahmen und Änderungen.

GoToMeeting

Ein weiteres aus der Praxis durchaus als leistungsfähig angesehenes Videoconferencing-Tool ist GoToMeeting des US-amerikanischen Herstellers LogMeIn, Inc. mit Sitz in Boston, der sich auf Fernwartungsdienste und Webconferencing-Dienste spezialisiert hat. Kern dieser Fernwartungs- und Konferenzdienste ist ein von LogMeIn entwickeltes, proprietäres, mit SSL verschlüsseltes Protokoll. Teilnehmer einer Webconference können sowohl eine Desktop-Software als auch eine Web-App nutzen oder sich auch ausschließlich per Telefon einwählen. Die Meeting-Einladungen können mithilfe einer für gängige E-Mail-Clints gut integrierten Kalender- und E-Mail-Integration verschickt werden. Neben dieser Integration bietet GoToMeeting HD-Video-Qualität mit bis zu 25 Webcams, Möglichkeiten zur Aufzeichnung, persönliche Meeting-Räume, Diagnosemöglichkeiten, eine Active-Directory-Integration und die Anbindung von In-Room-Lösungen.

Mit GoToMeeting wird in den USA gehostet und betrieben. Die Nutzung des Tools ist also mit einem Datentransfer in die USA verbunden. Dazu gibt es einen mehrfach schon aktualisierten Auftragsverarbeitungsvertrag mit Standardvertragsklauseln sowie ein eigenes Data-Processing-Addendum, um die Anforderungen an den Auftragsverarbeitungsvertrag nach Artikel 28 DSGVO zu erfüllen.

Die Berliner Behörde für den Datenschutz hat dieses Addendum in der Version vom 15. Dezember 2020 geprüft und kommt zu dem Ergebnis, dass nach wie vor Mängel bestehen, insbesondere hinsichtlich eines unzulässig beschränkten Anwendungsbereichs und unzulässiger Datenexporte. Die Kritikpunkte ergeben sich im Einzelnen wie folgt (siehe „Hinweise für Berliner Verantwortliche zu Anbietern von Videokonferenzdiensten", Version 2.0 vom 18. Februar 2021, https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/orientierungshilfen/2021-BlnBDI-Hinweise_Berliner_Verantwortliche_zu_Anbietern_Videokonferenz-Dienste.pdf)

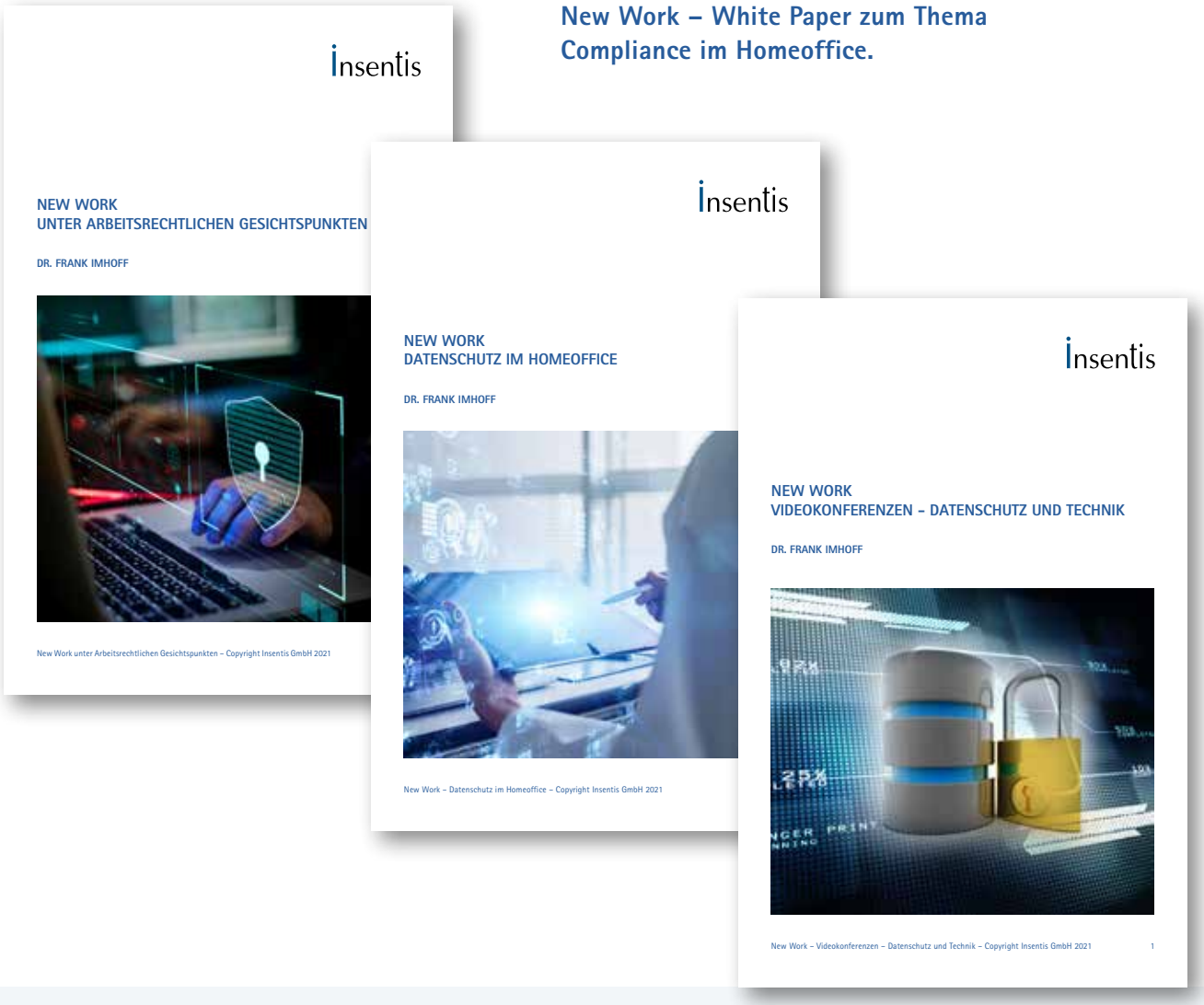
- Ziff. 5.1 des „Data Processing Addendum, Revised: December 15, 2020“ sieht entgegen Art. 28 Abs. 4 Satz 1 DSGVO Überprüfungen bei Unterauftragnehmern und vertragliche Vereinbarungen mit diesen nur dann vor, wenn es sich nicht um Konzernunternehmen von LogMeIn handelt. Zudem müssen entgegen Art. 28 Abs. 4 Satz 1 DSGVO die vertraglichen Datenschutz-Verpflichtungen nur „im Wesentlichen“ auch den Unterauftragnehmern auferlegt werden.
- Das Verfahren zur Information über gegenwärtige Unterauftragsverarbeiter in Ziff. 5.2 des „Datenverarbeitungsnachtrags“ stellt nicht sicher, dass Verantwortliche nachweisen (Art. 5 Abs. 2 i. V. m. Art. 5 Abs. 1 lit. a DSGVO) können, welche Unterauftragsverarbeiter mit Vertragsschluss genehmigt wurden. Das Verfahren zur Information über neue Unterauftragsverarbeiter in Ziff. 5.2 erfordert ein aktives Handeln der Verantwortlichen und genügt damit nicht Art. 28 Abs. 2 Satz 2 DSGVO. Verantwortliche, die die Benachrichtigungen nicht selbst aktiv abonnieren, können zudem nicht ihrer Rechenschaftspflicht (Art. 5 Abs. 2 i. V. m. Art. 5 Abs. 1 lit. a DSGVO) nachkommen.
- Ziff. 6.2 des „Datenverarbeitungsnachtrags“ genügt nicht den Anforderungen des Art. 28 Abs. 3 lit. h DSGVO an Nachweispflichten und Kontrollrechten.
- Ziff. 10 des „Datenverarbeitungsnachtrags“ beschränkt die Anwendbarkeit bestimmter, in diesem Abschnitt genannter, zwingend erforderlicher Regelungen auf einen Ausschnitt der Verarbeitungen personenbezogener Daten, die der DSGVO unterliegen; Art. 3 DSGVO ist viel weiter.
- Ziff. 10.3 i. V. m. Anhang 1 des „Datenverarbeitungsnachtrags“ sieht Einschränkungen der Standardvertragsklauseln vor, die zwar wegen einer Vorrangregelung für die Standardvertragsklauseln in Ziff. 12 zivilrechtlich nicht gelten dürften, aber dennoch zu einer unzulässigen Abwandlung führen, sodass diese den Datenexport nicht rechtfertigen können. Die Selbstzertifizierung nach dem Privacy Shield bezieht sich nicht auf HR-Daten.

Den Berliner Datenschützern haben diese Kritikpunkte gereicht, um ihre Ampel auf rot zu stellen. Das bedeutet, dass Mängel vorliegen, die eine rechtskonforme Nutzung des Dienstes ausschließen und eine technische Prüfung erst gar nicht erfolgt ist.

LogMeIn sieht das wenig überraschend anders und verweist u.a. auf ergänzende, freiwillige Datenschutzrahmenpläne wie APEC CBPR und PRP als Zeichen der Bereitschaft, Richtlinien wie die der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung („OECD“) und ähnliche einzuhalten, auf ein globales Datenschutzprogramm und ein Trust and Privacy Center, in dem sich Besucher und Kunden und Nutzer transparent zu den Datenschutzmaßnahmen informieren können. Zu diesen Datenschutzmaßnahmen gehört, dass alle Interaktionen von GoToMeeting per SSL-verschlüsselt sind, die Meetings selbst sind mit AES-256-Bit-verschlüsselt. Zusätzliche Sicherheit ergibt sich durch die angebotene risikobasierte Authentifizierung. Der Organisator eines Online-Meetings erhält damit eine Mitteilung, sobald eine Anmeldung über ein nicht-berechtigtes Gerät oder von einem neuen Standort vorliegt, sowie bei anderen auffälligen Vorgängen, die ein Sicherheitsrisiko darstellen könnten.

Insentis

New Work – White Paper zum Thema Compliance im Homeoffice.



Insentis Managementberatung

Hansenbergallee 30
65366 Geisenheim
Telefon: +49 6722 409051
info@insentis.com