Auftragsverarbeitung gem. Art. 28 EU-DS-GVO

Vereinbarung

zwischen

Firma / Behörde: _____

Name Ansprechpartner: _____

Straße und Hausnummer: _____

Postleitzahl und Ort: _____

(nachstehend Auftraggeber genannt)

und

Form-Solutions GmbH
Bahnhofstraße 10
76137 Karlsruhe

(nachstehend Auftragnehmer genannt)

wird folgender Vertrag über Auftragsverarbeitung nach Art. 28 Abs. 3 und den weiteren Bestimmungen der Verordnung 2016/79 EU (EU-Datenschutz-Grundverordnung) [i.F.: „EU-DS-GVO"] sowie sonstiger anwendbarer datenschutzrechtlicher Bestimmungen geschlossen:

Dieses Dokument besteht aus dieser Vereinbarung und den folgenden Anlagen:

Anlage 1: Technisch organisatorische Maßnahmen Form-Solutions
Anlage 2: Technisch organisatorische Maßnahmen Hetzner Online
Anlage 3: Technisch organisatorische Maßnahmen T-Systems International
Anlage 4: Technisch organisatorische Maßnahmen 1und1
Anlage 5: Technisch organisatorische Maßnahmen TeamViewer
Anlage 6: Technisch organisatorische Maßnahmen LogMeIn
Anlage 7: Unterauftragsverarbeiter des Auftragnehmers

§ 1 Gegenstand und Dauer des Auftrags, Auftragsinhalt

1. Inhalt

Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Inhalt des Vertrages ist die Regelung aller datenschutzrechtlichen Fragen zwischen Auftraggeber und Auftragnehmer.

Definitionen:

Die Parteien sind übereingekommen, dass in Ergänzung zu den in diesem Text verwendeten Begrifflichkeiten, für deren Bedeutung ihre Verwendung im Kontext der anwendbaren datenschutzrechtlichen Bestimmungen maßgeblich sein soll, für Zwecke dieser Vereinbarung über die Verarbeitung personenbezogener Daten im Auftrag die folgenden Begriffe die nachstehend gefasste Bedeutung haben sollen:

„Leistungsvereinbarung“

Dies ist eine zivilrechtliche Vereinbarung ungeachtet ihrer vertragstypologischen Einordnung, welche sich auf den Austausch von Leistungen zwischen dem Auftraggeber und dem Auftragnehmer bezieht, die eine Verarbeitung personenbezogener Daten zum Gegenstand haben oder eine solche Leistung zum Gegenstand haben, bei denen eine Kenntnisnahme von personenbezogenen Daten durch den Auftragnehmer oder von diesem beauftragte Dritte jedenfalls nicht ausgeschlossen werden kann.

Eine solche zivilrechtliche Vereinbarung kann jeder Leistungs-(Rahmen)-Vertrag sein, aber auch der jeweils gültige, zeitlich erstdatierende von mehreren Leistungsscheinen entsprechend der nachfolgenden Definition eines Leistungsscheins.

„Leistungsschein“

Dies ist ungeachtet ihrer vertragstypologischen Einordnung eine zivilrechtliche Vereinbarung über die Erbringung von Leistungen durch den Auftragnehmer für den Auftraggeber, welche in der Regel die Bereitstellung einer Softwarelösung oder mehrerer Softwarelösungen für den kommunalen Bereich aus dem Portfolio des Auftragnehmers einschließlich ihrer ggfs. auch im Einzelfall beauftragten Nebenleistungen zum Gegenstand hat, wobei eine Verarbeitung personenbezogener Daten durch den Auftragnehmer gegenständlich ist oder eine Kenntnisnahme von personenbezogenen Daten durch den Auftragnehmer oder von diesem beauftragten Dritten jedenfalls nicht auszuschließen ist. Im Regelfall wird für die Bereitstellung eines Softwareprodukts durch den Auftragnehmer ein Leistungsschein abgeschlossen.

2. Gegenstand des Auftrags

Gegenstand des Auftrags zum Datenumgang ist die Bereitstellung der Anwendung Form-Solutions Antragsmanagement 4.0.

3. Dauer des Auftrags

Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit des bestehenden Vertragsverhältnisses.

4. Art und Zweck der vorgesehenen Verarbeitung von Daten

Bereitstellung und Veröffentlichung elektronischer Frageapplikationen zur Erhebung, Übermittlung und Bereitstellung von Daten jeglicher Art. *(Beispiele: Erheben, Erfassen, Organisation, Ordnen, Speicherung, Anpassung oder Veränderung, Auslesen, Abfragen, Verwendung, Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, Abgleich oder Verknüpfung, Einschränkung, Löschen oder Vernichtung von Daten).*

5. Ort der Datenverarbeitung

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen schriftlichen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. EU-DS-GVO erfüllt sind.

6. Art der Daten

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten / -kategorien: Formularinhaltsdaten jeglicher Art zum Zwecke der Weiterleitung an die jeweilige Kommune im Auftrag. Für welche Geschäftsprozesse dieser Dienst in Anspruch genommen wird unterliegt im Einzelfall der Entscheidungsbefugnis der nutzenden Behörde.

7. Kategorien betroffener Personen

Der Kreis der Betroffenen wird von den nutzenden Behörden im Einzelfall festgelegt.

§ 2 Pflichten / Kontrollrecht des Auftraggebers

1. Der Auftraggeber ist allein verantwortlich für die Beurteilung der rechtlichen Zulässigkeit der im Rahmen des Auftragsverhältnisses durchzuführenden Verarbeitung durch den Auftragnehmer im Hinblick auf die Regelungen der EU-Datenschutz-Grundverordnung und anderer einschlägiger Vorschriften über den Datenschutz.
2. Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

   Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 EU-DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

   Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann z.B. auch erfolgen durch:

   - Die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 EU-DS-GVO
   - Die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 EU-DS-GVO
   - Aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren)
   - Eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz, ISO 27001).

   Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch in angemessener Höhe geltend machen.

   Die Verarbeitung von Daten in Privatwohnungen ist gestattet. Auch dort werden die datenschutzrechtlichen Vorschriften eingehalten.
3. Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

§ 3 Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 EU-DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

1. Schriftliche Bestellung eines Datenschutzbeauftragten, soweit gesetzlich erforderlich. Als Datenschutzbeauftragter ist beim Auftragnehmer Herr Frederick Kubin, datenschutz.com GmbH, Pappelallee 78/79 10437 Berlin, E-Mail: datenschutzbeauftragter@form-solutions.de, bestellt. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.
2. Die Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 EU-DS-GVO wird gewahrt. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Diese gelten auch nach Beendigung des Auftrags fort.
3. Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 EU-DS-GVO [Einzelheiten in Anlage 1].
4. Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
5. Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Personen gewährleistet wird.
6. Der Auftragnehmer verarbeitet personenbezogene Daten des Auftraggebers ausschließlich im Rahmen der vertraglich festgelegten Weisungen und der speziellen Einzelweisungen des Auftraggebers, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder der Mitgliedsstaaten, dem der Auftragnehmer unterliegt, hierzu verpflichtet ist (beispielsweise bei Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden). In einem solchen Fall teilt der Auftragnehmer dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet. Er verwendet die zur Datenverarbeitung überlassenen Daten nicht für andere Zwecke und bewahrt sie nicht länger auf, als es der Auftraggeber bestimmt. **Die Obergrenze für die Vorhaltezeit jeglicher Antragsdaten beträgt 180 Tage; nach dieser Frist noch vorhandene Antragsdaten werden automatisiert gelöscht.**

   Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen Datenschutzvorschriften verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen.

   Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie durch den Weisungsberechtigten beim Auftraggeber bestätigt oder geändert wird.

   Der Auftragnehmer ist verpflichtet, dem Auftraggeber jederzeit Auskünfte zu erteilen, soweit dessen Unterlagen und Daten betroffen sind.
7. Der Auftragnehmer führt das Verzeichnis der Verarbeitungstätigkeit gem. Art. 30 Abs. 2 EU-DS-GVO und stellt dies auf Anfrage dem Auftraggeber zur Verfügung. Der Auftraggeber stellt dem Auftragnehmer die hierzu erforderlichen Informationen zur Verfügung.

   Der Auftragnehmer unterstützt den Auftraggeber seinerseits bei der Erstellung des Verzeichnisses nach Art 30 Abs. 1 EU-DS-GVO.
8. Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der EU-DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten.

9. Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung in angemessener Höhe beanspruchen.

10. Der Auftragnehmer informiert den Auftraggeber unverzüglich über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

    Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

    Etwaig anfallende Mehrkosten für den Auftragnehmer im Rahmen dieser Pflichten sind diesem durch den Auftraggeber zu ersetzen.

§ 4 Rückgabe und Löschung

Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Kopien, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungsfristen erforderlich sind.

Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial.

Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

§ 5 Unterauftragsverhältnisse

1. Der Auftragnehmer darf Unterauftragsverarbeiter (weitere Auftragsverarbeiter) nur nach vorheriger Zustimmung des Auftraggebers beauftragen.

2. Der Auftraggeber stimmt der Beauftragung der in Anlage 2 aufgeführten Unterauftragsverarbeiter zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2 bis 4, 9 EU-DS-GVO, welche sowohl schriftlich als auch in einem elektronischen Format erfolgen kann.

3. Vor Hinzuziehung weiterer oder Ersetzung aufgeführter Unterauftragsverarbeiter informiert der Auftragnehmer den Auftraggeber eine angemessene Zeit (mindestens vier Wochen) vorab schriftlich oder in Textform.

4. Der Auftraggeber kann gegen die Änderung – innerhalb einer angemessenen Frist, jedoch nicht länger als 2 Wochen – aus wichtigem datenschutzrechtlichem Grund – gegenüber der vom Auftragnehmer bezeichneten Stelle Einspruch erheben. Erfolgt kein Einspruch innerhalb der Frist gilt die Zustimmung zur Änderung als gegeben. Bei unberechtigtem Einspruch kann es zu entsprechenden Verzögerungen bei der Erbringung der Leistung nach dem Hauptvertrag kommen. Für eine aus einem unberechtigten Einspruch resultierende Einschränkung der Vertragsleistungen ist der Auftragnehmer nicht verantwortlich.

5. Hat der Auftraggeber aufgrund eines wichtigen datenschutzrechtlichen Grundes berechtigt Einspruch gegen einen Unterauftragsverarbeiter erhoben und ist eine einvernehmliche Lösungsfindung zwischen den Parteien auch auf anderem Wege aufgrund von wichtigen datenschutzrechtlichen Gründen nicht möglich, steht dem Auftragnehmer ein Sonderkündigungsrecht zu.
6. In Ausnahmefällen ist auch eine nachträgliche Einigung zwischen den Parteien möglich. Der Auftragnehmer hat den Auftraggeber in diesem Fall unverzüglich über den Einsatz eines Unterauftragsverarbeiters zu informieren.
7. Erbringt der Unterauftragsverarbeiter die vereinbarte Leistung außerhalb der EU / des EWR, stellen Auftraggeber und Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher.
8. Eine weitere Auslagerung durch den Unterauftragsverarbeiter bedarf der ausdrücklichen Zustimmung des Hauptauftragnehmers (mindestens Textform); sämtliche vertragliche Regelungen zu den Datenschutzpflichten in der Vertragskette sind auch dem weiteren Unterauftragsverarbeiter aufzuerlegen.
9. Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

§ 6 Weisungsrechte

Die Verarbeitung der Daten erfolgt ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisung des Auftraggebers. Der Auftraggeber erteilt alle Weisungen und Aufträge in der Regel schriftlich oder in einem dokumentierten elektronischen Format. Der Auftraggeber behält sich im Rahmen der in dieser Vereinbarung getroffenen Auftragsbeschreibung ein umfassendes Weisungsrecht über Art, Umfang und Verfahren der Datenverarbeitung vor, das er durch Einzelweisungen konkretisieren kann. Änderungen des Verarbeitungsgegen-standes und Verfahrensänderungen sind gemeinsam abzustimmen und in schriftlicher oder elektronischer Form zu dokumentieren.

Mündliche Weisungen bestätigt der Auftraggeber unverzüglich schriftlich oder in einem dokumentierten elektronischen Format.

§ 7 Rechte betroffener Personen

1. Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.
2. Etwaige dem Auftragnehmer hierdurch entstehende Mehrkosten sind diesem durch den Auftraggeber zu erstatten.

§ 8 Technisch-organisatorische Maßnahmen

1. Die in der Anlage 1 beschriebenen technischen und organisatorischen Maßnahmen werden als verbindlich festgelegt.

   Der Auftragnehmer hat damit die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 EU-DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 EU-DS-GVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 EU-DS-GVO zu berücksichtigen.

2. Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Über wesentliche Änderungen ist der Auftraggeber vorab zu informieren; diese sind vom Auftragnehmer schriftlich oder in einem elektronischen Format nachvollziehbar zu dokumentieren.

3. Soweit die beim Auftragnehmer getroffenen Sicherheitsmaßnahmen den Anforderungen des Auftraggebers nicht genügen, benachrichtigt er den Auftraggeber unverzüglich. Entsprechendes gilt für Störungen, Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie bei Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten.

§ 9 Haftung

Für die Haftung aufgrund von Verletzungen der Datenschutzbestimmungen oder diesem Auftragsverarbeitungsvertrag gelten die gesetzlichen Vorschriften, sofern in den für die vertragsgegenständlichen Leistungen geltenden Vertragsdokumenten keine abweichende Haftungsvereinbarung getroffen wurde.

Der Auftraggeber ist gemäß den datenschutzrechtlichen Bestimmungen verpflichtet, seine veröffentlichten Frageapplikationen z.B. durch Datenschutzerklärung, Impressum und Einwilligungserklärung zu deklarieren. Der Auftragnehmer hält zu diesem Zweck in der Administrationsoberfläche entsprechende Verwaltungsmöglichkeiten vor. Kommt er dieser Verpflichtung nicht nach, so stellt er den Auftragnehmer bezüglich diesbezüglicher Rechts- und Haftungsrisiken frei.

§ 10 Sonstiges

1. Änderungen und Ergänzungen dieses Auftragsverarbeitungsvertrags und seiner Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung, die auch in einem elektronischen Format (Textform) erfolgen kann, und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

2. Der Gerichtsstand für beide Parteien ist der Sitz des Auftragnehmers.

3. Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

Für den Auftraggeber:

Datum, Ort, Unterschrift

Name, Rolle

Für den Auftragnehmer:

Olaf Rohstock
Geschäftsführer
Form-Solutions GmbH

Frank-Olaf Wilhelm
Geschäftsführer
Form-Solutions GmbH

ANLAGE 1

Technische organisatorische Maßnahmen Form-Solutions GmbH

1. Zutrittskontrolle

- **Lage der Räume:** Büros und EDV - Raum sind abgesichert durch: Türschlösser, elektronische Türöffner, elektronische Zugangskontrolle ist in Vorbereitung. Der Serverraum (Server der Form-Solutions Büroinfrastruktur, Testserver, Demoserver) verfügt über eine zusätzliche Riegeltür, zu der nur die Geschäftsführung und Administratoren Zutritt haben. Das Fenster des Serverraums ist zusätzlich vergittert. Der Serverraum befindet sich in einem geschützten Gewölbekeller mit Hochwasserschutzmaßnahmen. Der Serverraum ist zusätzlich videoüberwacht mit Alarmierungsfunktion.
- **Verschließbarkeit der Räume:** Es erfolgt ein Auf- und Abschließen bei Arbeitsbeginn und -ende. Quittierung der Schlüsselausgabe bei der Geschäftsführung. Ein geregeltes Konzept der Schlüsselverwaltung liegt vor.
- **Überwachungseinrichtung:** Serverraum und Eingangsbereich werden videoüberwacht inkl. Bewegungssensoren und Alarmfunktion
- **Schriftliche Festlegungen zur Zugangsberechtigung:** Klare Trennung von Publikums - und Bearbeitungszonen. Besucher müssen sich anmelden und einen Besucherausweis tragen. Dokumentation der Besucher. Alle Mitarbeiter sind mit einem Transponder für die elektronische Zutrittsgewährung ausgestattet.
- **Reinigungs- und Wartungsarbeiten:** Eine Datenschutzerklärung und -verpflichtung des Reinigungsunternehmens liegt vor. Sonstige Dienstleister nur mit entsprechender Beaufsichtigung.
- **Anwesenheitskontrollen:** Wird protokolliert durch Ein- und Ausstempeln zu Arbeitsbeginn und -ende sowie bei den Pausenzeiten.
- **Sicherheit bei Heimarbeiten/Telearbeiten:** Datenverarbeitung von personenbezogenen Daten nur auf Geräten, die von der Firma zur Verfügung gestellt werden. Verschlüsselung der Festplatten der Geräte. Zugriff auf Firmennetzwerk nur über VPN. USB Speicher zur Datenhaltung verboten. Voraussetzung für die Erlaubnis von „mobilem arbeiten“ ist die Akzeptanz einer Vereinbarung zum „mobilen arbeiten“. Diese regelt unter anderem die Verantwortlichkeit für die sichere Infrastruktur sowie die Kontrollrechte des Arbeitgebers und der Datenschutzbehörden.

2. Zugangskontrolle

- **Firewall und Datenschutz:** Zentrale Firewall. Die Clients verfügen über einen Virenschutz.
- **Benutzeridentifikation und Passwortverfahren:** Ausreichend sichere Passwörter werden verwendet. Ein regelmäßiger Passwortwechsel ist verpflichtend. Eine Anforderungsdefinition zu sicheren Passwörtern liegt vor.
- **Systemsperrung:** Sperrung der Bildschirme nach 15min Inaktivität. Sperren der Bildschirme bei Verlassen des Arbeitsplatzes ist Pflicht. Falscheingabe eines Passworts hat eine zeitliche Verzögerung für einen Neuversuch zur Folge.

- **Benutzerkennungen:** Jeder Mitarbeiter hat ein eigenes Benutzerkonto mit individuellen Zugriffsrechten. Zentrale Verwaltung via ActiveDirectory.
- **Verschlüsselung:** Festplatten in mobilen Endgeräten werden verschlüsselt via AES256 Verfahren.
- **Geräteanschlüsse:** Der Einsatz von externen Speichermedien wie z.B. USB-Sticks ist verboten.

3. Zugriffskontrolle

- **Berechtigungskonzept und Zugriffsrechte:** Es existieren verschiedene Berechtigungen für Auswertungen, Kenntnisnahmen und Löschungen sowie Datenexport.
- **Schutz gegen unberechtigte Zugriffe:** Sämtliche Datenhaltung erfolgt verschlüsselt. Firewall System ist vorhanden. Penetrationstests unseres Antragsmanagements werden von diversen Kunden in regelmäßigen Abständen in deren Auftrag realisiert. Erkenntnisse dieser Penetrationstests laufen in die aktuellen Entwicklungen mit ein.
- **Überwachung und Protokollierung:** Sowohl Zugriffe als auch Zugriffsversuche werden protokolliert. Die Protokolle werden mindestens ein Jahr lang aufbewahrt.
- **Datenträgerverwaltung:** Sämtliche Datenträger sind inklusive des Geräts, in dem sie verbaut sind, inventarisiert. Nachweise über den Eingang, Ausgang sowie Bestand von Datenträgern wird festgehalten. Mobile Festplatten und USB -Sticks sind verboten. Es findet eine Auslagerung von Sicherungsdatenträgern statt (Verschlüsselt, Aufbewahrung im Safe).
- **Datentrennung:** Geräte inklusive Festplatten sind inventarisiert und gekennzeichnet. Datenträger von Auftraggebern liegen nicht vor. Die Benutzung privater Datenträger an Firmengeräten ist verboten.
- **Datenlöschung:** Datenträger werden nur an einen Fachbetrieb mit entsprechendem Datenschutzmanagement zur Entsorgung bzw. Wiederaufbereitung verkauft.
- **Entsorgung/Vernichtung:** Daten Schredder mit Partikelschnitt (Sicherheitsstufe 5) liegen für jeden Mitarbeiter zugänglich vor. Dokumente mit personenbezogenen Daten müssen vor der Entsorgung geschreddert werden. Veraltete Datenträger werden an eine Fachfirma mit entsprechendem Datenschutzmanagement verkauft.
- **Regelung für das Kopieren von Datenträgern:** Die Exportmöglichkeit von Daten steht innerhalb des CRM-Systems nur bestimmten, schriftlich oder in einem elektronischen Format nachvollziehbar ausdrücklich berechtigten Mitarbeitern zur Verfügung. Externe Datenträger wie USB -Sticks und Festplatten sind verboten.
- **Regelungen für mobile Geräte:** Personenbezogene Daten dürfen ausschließlich auf von der Firma bereitgestellten Geräten verarbeitet werden. Die Verwendung von mobilen Datenträgern wie z.B. USB-Sticks, externen Festplatten, Disketten ist untersagt. Die Benutzung eigener Endgeräte im Firmennetzwerk ist verboten.
- **Fernwartung:** Wartungszugriff grundsätzlich nur im 4-Augen-Prinzip.

4. Weitergabekontrolle

- **Datenträgertransportart:** Datentransporte nur über sicheren Webdownload bzw. verschlüsselten E-Mails.
- **Versendungsarten:** s.o. Datenträgertransportart.
- **Transportsicherung:** Der Transport personenbezogener Daten erfolgt ausschließlich via passwortgesichertem und SSL gesichertem Download bzw. durch SSL-verschlüsselte Webservices bzw. durch verschlüsselte E-Mails oder innerhalb eines Virtuellen Privaten Netzwerks (VPN).
- **Dokumentation:** Verschlüsselte E-Mails werden im CRM-System archiviert. Protokollierung durch Log-Files.

5. Eingabekontrolle

- **Protokollierung:** Das Journal in CAS genesisWorld ist für jeden Datensatztyp in CAS genesisWorld auch für eigene verfügbar. Das Journal protokolliert und dokumentiert jede Änderung am Datensatz. Dabei wird vermerkt, wer wann einen Datensatz erzeugt oder gelöscht hat, oder wer wann welches Feld mit welchem Wert geändert hat. Eine Undo-Funktion sorgt dafür, dass ungewollte Änderungen wieder rückgängig gemacht werden können.
- **Dokumentation:** Ein Organigramm liegt vor.

6. Auftragskontrolle

- **Auswahl von Auftragnehmer:** Auftragnehmer werden vor Auftragserteilung aufwendig auf Eignung und Zuverlässigkeit hin geprüft.
- **Schriftliches Auftragsverhältnis:** Beauftragung von Firmen zur Bearbeitung personenbezogener Daten nur mit schriftlichem Auftrag.
- **Kontrolle:** Die Kontrolle der Arbeitsergebnisse erfolgt regelmäßig. Der Datenschutzbeauftragte ist auch mit der Kontrolle der Auftragnehmer beauftragt.

7. Verfügbarkeitskontrolle

- **Brandschutz:** Feuerlöscher sind auf jedem Stockwerk und im Serverraum vorhanden.
- **Stromversorgung:** Im Serverraum ist eine USV etabliert.
- **Sicherungen:** Intervall-Sicherungsdatenträger werden außerhäuslich in einem Tresor verwahrt. Eine Online-Sicherung liegt auf eigenem Server in einem externen Rechenzentrum sicher und verschlüsselt vor.
- **Virenschutz/Firewall:** Virenschutz sowie Firewall liegen vor.
- **Notfallplan:** Notfallplan liegt vor.

8. Trennungskontrolle

- **Getrennte Speicherung:** Im Antragsmanagement können je Veröffentlichungsprozess die Datenübergaben im Einzel-fall dediziert festgelegt werden. Die Festlegung wird im Einzelfall vom Kunden getroffen.
- **Mandantenfähigkeit:** Im Antragsmanagement können bis zu 9.999 Mandanten parallel nebeneinander betrieben werden. Ein Konzept zur Mandantentrennung besteht.
- **Funktionstrennung:** Produktions-, Test-, Demo-, und Entwicklungsumgebungen werden stets voneinander getrennt und auf separaten Servern betrieben. Zu Entwicklungszwecken werden nur fiktive Daten verwendet.

9. Organisationskontrolle

- **IT-Sicherheitskonzept:** Die IT-Richtlinien werden in einem internen IT-Wiki dokumentiert und fortgeschrieben. Ein Datensicherungsschema liegt ebenfalls vor.
- **Revision:** Stichprobenkontrollen durch die Geschäftsführung und den Datenschutzbeauftragten
- **Mitarbeiter:** Klare Vertretungsregelung für Krankheit und Urlaub (s. Organigramm). Die Mitarbeiter wer-den im Umgang mit sensiblen Daten geschult. Ein Mitarbeiterhandbuch mit den entsprechenden Regelungen liegt vor. Datenschutzaspekte werden regelmäßig thematisiert. In mobilen Geräten verbaute Datenträger werden standardmäßig verschlüsselt. Funktionstrennung liegen im eingesetzten CRM-System vor.

ANLAGE 2

Technisch organisatorische Maßnahmen Hetzner Online AG

Bestandteil Backupstrategie des Form-Solutions Formularservers. (nur relevant für Kunden, die das Antragsmanagement auf pdf.form-solutions.net nutzen) Die auf dem Formularserver vorhandenen Daten jedes einzelnen Mandanten werden auf einem Server bei der Hetzner Online AG in einer Backup-Cloud gespeichert. Ziel ist es, an einem entfernten Ort eine Kopie der Daten vorzuhalten und so einen evtl. Verlust z.B. durch Brand oder Diebstahl vorzubeugen.

Die Zertifizierung nach einem genehmigten Zertifizierungsverfahren, siehe unter:
https://www.hetzner.com/de/unternehmen/zertifizierung/

Die technisch organisatorischen Maßnahmen der Firma Hetzner Online AG sind nachfolgend abgedruckt.

HETZNER ONLINE

Anlage 2 zur Vereinbarung nach § 11 BDSG:
Technische und organisatorische
Maßnahmen nach § 9 BDSG und Anlage

1. Zutrittskontrolle

- elektronisches Zutrittskontrollsystem mit Protokollierung
- Hochsicherheitszaun um den gesamten Datacenterpark
- dokumentierte Schlüsselvergabe an Mitarbeiter und Colocation-Kunden für Colocation Racks (jeder Auftraggeber ausschließlich für seinen Colocation Rack)
- Richtlinien zur Begleitung und Kennzeichnung von Gästen im Gebäude
- 24/7 personelle Besetzung der Rechenzentren
- Videoüberwachung an den Ein- und Ausgängen, Sicherheitsschleusen und Serverräumen

2. Zugangskontrolle

- bei Hauptauftrag „Dedicated Server", „vServer" und „Colocation"
  - Server-Passwörter, welche nur vom Auftraggeber nach erstmaliger Inbetriebnahme von ihm selbst geändert werden und dem Auftragnehmer nicht bekannt sind
  - Das Passwort zur Administrationsoberfläche wird vom Auftraggeber selbst vergeben - die Passwörter müssen vordefinierte Richtlinien erfüllen. Zusätzlich steht dem Auftraggeber dort eine Zwei-Faktor-Authentifizierung zur weiteren Absicherung seines Accounts zur Verfügung.
- bei Hauptauftrag „Managed Server"
  - Zugang ist passwortgeschützt, Zugriff besteht nur für Mitarbeiter von Auftragnehmer; verwendete Passwörter müssen Mindestlänge haben und werden in regelmäßigen Abständen erneuert

3. Zugriffskontrolle

- bei internen Verwaltungssysteme des Auftragnehmers
  - Durch regelmäßige Sicherheitsupdates und Backups (nach dem jeweiligen Stand der Technik) stellt der Auftragnehmer sicher, dass unberechtigte Zugriffe verhindert werden.
  - Revisionssicheres, verbindliches Berechtigungsvergabeverfahren für Mitarbeiter des Auftragnehmers
- bei Hauptauftrag „Dedicated Server", „vServer" und „Colocation"

Hetzner Online GmbH
Geschäftsführer: Martin Hetzner
Registergericht Ansbach, HRB 6089
USt-IdNr. DE812871812

Industriestr. 25 | 91710 Gunzenhausen
Tel.: +49 9831 505-0
Fax: +49 9831 505-3
info@hetzner.de | www.hetzner.de

Bankverbindung:
Deutsche Bank AG Nürnberg
IBAN: DE92 7607 0012 0750 0077 00
BIC: DEUTDEMM760

- Die Verantwortung der Zugriffskontrolle obliegt dem Auftraggeber.

- bei Hauptauftrag „Managed Server“
  - Durch regelmäßige Sicherheitsupdates und Backups (nach dem jeweiligen Stand der Technik) stellt der Auftragnehmer sicher, dass unberechtigte Zugriffe verhindert werden.
  - Revisionssicheres, verbindliches Berechtigungsvergabeverfahren für Mitarbeiter des Auftragnehmers
  - Für übertragene Daten/Software ist einzig der Auftragnehmer in Bezug auf Sicherheit und Updates zuständig.

4. Weitergabekontrolle

- Alle Mitarbeiter sind auf das Datengeheimnis nach § 5 BDSG verpflichtet.
- Datenschutzgerechte Löschung der Daten nach Auftragsbeendigung.
- Möglichkeiten zur verschlüsselten Datenübertragung werden im Umfang der Leistungsbeschreibung des Hauptauftrages zur Verfügung gestellt.

5. Eingabekontrolle

- bei internen Verwaltungssysteme des Auftragnehmers
  - Die Daten werden vom Auftraggeber selbst eingegeben bzw. erfasst.
  - Änderungen der Daten werden protokolliert.
- bei Hauptauftrag „Dedicated Server“, „vServer“ und „Colocation“
  - Die Verantwortung der Eingabekontrolle obliegt dem Auftraggeber.
- bei Hauptauftrag „Managed Server“
  - Die Daten werden vom Auftraggeber selbst eingegeben bzw. erfasst.
  - Änderungen der Daten werden protokolliert.

6. Auftragskontrolle

- Unsere Mitarbeiter werden in regelmäßigen Abständen im Datenschutzrecht unterwiesen und sie sind vertraut mit den Verfahrensanweisungen und Benutzerrichtlinien für die Datenverarbeitung im Auftrag, auch im Hinblick auf das Weisungsrecht des Auftraggebers. Die AGB enthalten detaillierte Angaben über Art und Umfang der beauftragten Verarbeitung und Nutzung personenbezogener Daten des Auftraggebers.
- Die AGB enthalten detaillierte Angaben über die Zweckbindung der

Hetzner Online GmbH
Geschäftsführer: Martin Hetzner
Registergericht Ansbach, HRB 6089
USt-IdNr. DE812871812

Industriestr. 25 | 91710 Gunzenhausen
Tel.: +49 9831 505-0
Fax: +49 9831 505-3
info@hetzner.de | www.hetzner.de

Bankverbindung:
Deutsche Bank AG Nürnberg
IBAN: DE92 7607 0012 0750 0077 00
BIC: DEUTDEMM760

personenbezogenen Daten des Auftraggebers.

- Die Hetzner Online GmbH hat einen betrieblichen Datenschutzbeauftragten bestellt und sorgt durch die Datenschutzorganisation für dessen angemessene und effektive Einbindung in die relevanten betriebliche Prozesse.

7. Verfügbarkeitskontrolle

- bei internen Verwaltungssysteme des Auftragnehmers
  - Backup- und Recovery-Konzept mit täglicher Sicherung aller relevanten Daten.
  - Sachkundiger Einsatz von Schutzprogrammen (Virenscanner, Firewalls, Verschlüsselungsprogramme, SPAM-Filter).
  - Einsatz von Festplattenspiegelung bei allen relevanten Servern.
  - Monitoring aller relevanter Server.
  - Einsatz unterbrechungsfreier Stromversorgung.
  - Dauerhaft aktiver DDoS-Schutz.
- bei Hauptauftrag „Dedicated Server", „vServer" und „Colocation"
  - Datensicherung obliegt dem Auftraggeber.
  - Einsatz unterbrechungsfreier Stromversorgung.
  - Dauerhaft aktiver DDoS-Schutz.
- bei Hauptauftrag „Managed Server"
  - Backup- und Recovery-Konzept mit täglicher Sicherung der Daten je nach gebuchten Leistungen des Hauptauftrages.
  - Einsatz von Festplattenspiegelung.
  - Einsatz unterbrechungsfreier Stromversorgung.
  - Einsatz von Softwarefirewall und Portreglementierungen.
  - Dauerhaft aktiver DDoS-Schutz.

8. Maßnahmen zur Datensicherung (physikalisch / logisch)

- bei internen Verwaltungssysteme des Auftragnehmers
  - Daten werden physikalisch oder logisch von anderen Daten getrennt gespeichert.
  - Die Datensicherung erfolgt ebenfalls auf logisch und/oder physikalisch getrennten Systemen.

Hetzner Online GmbH
Geschäftsführer: Martin Hetzner
Registergericht Ansbach, HRB 6089
USt-IdNr. DE812871812

Industriestr. 25 | 91710 Gunzenhausen
Tel.: +49 9831 505-0
Fax: +49 9831 505-3
info@hetzner.de | www.hetzner.de

Bankverbindung:
Deutsche Bank AG Nürnberg
IBAN: DE92 7607 0012 0750 0077 00
BIC: DEUTDEMM760

- bei Hauptauftrag „Dedicated Server“, „vServer“ und „Colocation“
  - Die Trennungskontrolle obliegt dem Auftraggeber.
- bei Hauptauftrag „Managed Server“
  - Daten werden physikalisch oder logisch von anderen Daten getrennt gespeichert.
  - Die Datensicherung erfolgt ebenfalls auf logisch und/oder physikalisch getrennten Systemen.

Hetzner Online GmbH
Geschäftsführer: Martin Hetzner
Registergericht Ansbach, HRB 6089
USt-IdNr. DE812871812

Industriestr. 25 | 91710 Gunzenhausen
Tel.: +49 9831 505-0
Fax: +49 9831 505-3
info@hetzner.de | www.hetzner.de

Bankverbindung:
Deutsche Bank AG Nürnberg
IBAN: DE92 7607 0012 0750 0077 00
BIC: DEUTDEMM760

ANLAGE 3

Technisch organisatorische Maßnahmen T-Systems International GMBH

Hosting des Formularservers
(nur relevant für Kunden, die das Antragsmanagement auf pdf.form-solutions.net nutzen)

Die technischen und organisatorischen Maßnahmen sind nachfolgend abgedruckt.

Ergänzende Bedingungen Auftragsverarbeitung (ErgB-AV) für Open Telekom Cloud

Vertragspartner sind die Telekom Deutschland GmbH (im Folgenden Telekom genannt), Landgrabenweg 151, 53227 Bonn, und der Kunde.

1 Allgemeines

Allgemeines

Gegenstand der Vereinbarung ist die Regelung der Rechte und Pflichten des Verantwortlichen (Kunde) und des Auftragsverarbeiters (Telekom), sofern im Rahmen der Leistungserbringung (nach AGB und mitgeltenden Dokumenten) eine Verarbeitung personenbezogener Daten durch die Telekom für den Kunden im Sinne des anwendbaren Datenschutzrechts erfolgt. Die Vereinbarung gilt entsprechend für die (Fern-)Prüfung und Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen, wenn dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann. Aus den AGB und den mitgeltenden Dokumenten, diesen „Ergänzenden Bedingungen Auftragsverarbeitung" sowie der „Anlage zu den Ergänzenden Bedingungen Auftragsverarbeitung" (Anlage) – zusammen „ErgB-AV" - ergeben sich Rechtsgrundlage, Gegenstand und Dauer sowie Art und Zweck der Verarbeitung, Art der personenbezogenen Daten sowie die Kategorien der betroffenen Personen.

Definitionen

Im Sinne dieser „ErgB-AV" bezeichnet der Ausdruck

a) „Auftragsverarbeiter" eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet; „Auftragsverarbeiter" ist die Telekom;

b) „Dritter" eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und die Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten;

c) „AGB und mitgeltenden Dokumenten" die, die Leistungserbringung regelnden Dokumente;

d) „Verantwortlicher" die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; Verantwortlicher ist die als „Kunde" bezeichnete Vertragspartei, die hier in diesen ErgB-AV allein über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet;

e) „Verarbeitung" jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung;

f) „personenbezogene Daten" alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person") beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann;

g) „weiterer Auftragsverarbeiter oder Unterauftragsverarbeiter" den Vertragspartner der Telekom, der von dieser mit der Durchführung bestimmter Verarbeitungsaktivitäten für den Verantwortlichen beauftragt wird;

h) „Sub-Unterauftragsverarbeiter" den Vereinbarungspartner des weiteren Auftragsverarbeiters oder Unterauftragsverarbeiters, der von Letzterem mit der Durchführung bestimmter Verarbeitungsaktivitäten im Regelungsbereich diesen ErgB-AV beauftragt wird.

2 Rechte und Pflichten des Kunden

2.1 **[Zulässigkeit der Datenverarbeitung]** Für die Beurteilung der Zulässigkeit der Datenverarbeitung sowie für die Wahrung der Rechte der Betroffenen ist allein der Kunde verantwortlich. Der Kunde wird in seinem Verantwortungsbereich dafür Sorge tragen, dass die gesetzlich notwendigen Voraussetzungen (z.B. durch Einholung von Einwilligungserklärungen) geschaffen werden, damit die Telekom die vereinbarten Leistungen auch insoweit rechtsverletzungsfrei erbringen kann.

2.2 **[Weisungen]** Die Telekom wird personenbezogene Daten nur auf dokumentierte Weisung des Kunden – auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation – verarbeiten, sofern sie nicht durch das Recht der Union oder der Mitgliedstaaten, dem die Telekom unterliegt, hierzu verpflichtet ist. In einem solchen Fall teilt die Telekom dem Kunden diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

Als Weisungen sind die AGB und mitgeltenden Dokumente sowie die ErgB-AV zu verstehen. Im Rahmen der produktspezifischen

Parameter bestimmt der Kunde Art und Umfang der Datenverarbeitung durch die Art der Nutzung des Produktes, durch Auswahl der dort ggf. ermöglichten Varianten z.B. hinsichtlich des Umfangs und der Art der zu verarbeitenden Daten oder des Ortes der Datenverarbeitung.
Alle zusätzlichen Weisungen werden schriftlich oder per E-Mail erteilt. Die Telekom informiert den Kunden unverzüglich, falls sie der Auffassung ist, dass eine Weisung gegen die geltenden rechtlichen Bestimmungen verstößt. Die Telekom ist berechtigt, die Durchführung einer solchen Weisung solange auszusetzen, bis diese durch den Kunden bestätigt oder geändert wird.

2.3 **[Ausgleich Mehrleistung]** Soweit in den AGB und den mitgeltenden Dokumenten Vereinbarungen zu Leistungsänderungen getroffen wurden, gehen diese den Regelungen in diesem Absatz vor. Soweit keine Vereinbarung zu Leistungsänderungen in den AGB und den mitgeltenden Dokumenten getroffen wurden, werden zusätzliche Weisungen und Maßnahmen, die eine Abweichung zu den in dieser ErgB-AV oder in den AGB und den mitgeltenden Dokumenten festgelegten Leistungen darstellen, als Antrag auf Leistungsänderung behandelt. Zusätzliche Weisungen und Maßnahmen, die über die vertraglich vereinbarten Leistungen hinausgehen, sind - soweit nicht ausdrücklich anders vereinbart - bei Mehraufwand für die Telekom gesondert zu vergüten. Die Vertragsparteien werden sich in diesem Fall über eine angemessene Vergütung gesondert verständigen. Bei begründeten Weisungen, deren Umsetzung für die Telekom nicht oder nur mit unverhältnismäßig hohem Mehraufwand möglich ist, und deshalb von der Telekom nicht umgesetzt werden, kann der Kunde den Vertrag fristlos kündigen.
Soweit nicht ausdrücklich anders vereinbart, werden Unterstützungsleistungen der Telekom nach Ziffer 2.5 und Ziffer 3.4, 3.5. 3.7, 3.8, (dort Satz 2), 3.9 und 3.10 dieser Vereinbarung gesondert vergütet.

2.4 **[Nachweis durch die Telekom]** Der Telekom steht es frei, die hinreichende Umsetzung ihrer gesetzlichen Pflichten sowie der Pflichten aus diesen ErgB-AV, insbesondere der technisch-organisatorischen Maßnahmen (Ziffer 4) und Maßnahmen, die nicht nur den konkreten Auftrag betreffen, durch die in der Anlage bezeichneten Nachweise zu belegen.

2.5 **[Überprüfungen, Inspektionen]** Der Kunde kann auf eigene Kosten die Einhaltung der Vorschriften über den Datenschutz und der in diesen ErgB-AV niedergelegten Pflichten durch die Einholung von Auskünften und Abfrage der nach Ziffer 2.4 angeführten Nachweise bei der Telekom in Hinblick auf die sie betreffende Verarbeitung kontrollieren. Der Kunde wird vorrangig prüfen, ob die in Satz 1 dieses Absatzes eingeräumte Möglichkeit der Überprüfung ausreicht. Der Kunde kann darüber hinaus in besonders zu begründenden Ausnahmefällen auf eigene Kosten die Einhaltung der Vorschriften über den Datenschutz vor Ort kontrollieren. Der Kunde kann die Kontrollen selbst durchführen oder durch einen von ihm beauftragten Dritten auf seine Kosten durchführen lassen. Vom Kunden mit der Kontrolle betraute Personen oder Dritte sind mit Beauftragung nachweislich zur Wahrung der Vertraulichkeit zu verpflichten. Die vom Kunden mit der Kontrolle betrauten Personen oder Dritte werden der Telekom in angemessener Form vorangekündigt und in die Lage versetzt, ihre Legitimation zur Durchführung der Kontrollen nachzuweisen. Dritte im Sinne dieses Absatzes dürfen keine Vertreter von Wettbewerbern der Telekom oder ihrer Konzernunternehmen sein. Der Kunde wird Kontrollen mit einer angemessenen Frist ankündigen und bei deren Durchführung auf Geschäftsbetrieb und Betriebsablauf Rücksicht nehmen. Die der Telekom entstehenden Kosten für eine vor Ort Kontrolle sind vom Kunden zu tragen.

2.6 **[Unterstützung durch den Kunden]** Der Kunde wird in Hinblick auf die ihn betreffende Verarbeitung die Telekom bei Verdacht auf Datenschutzverletzungen und/oder anderen Unregelmäßigkeiten bei der Verarbeitung der personenbezogenen Daten unverzüglich und vollständig informieren. Der Kunde wird in Hinblick auf die ihn betreffende Verarbeitung die Telekom bei der Prüfung möglicher Verstöße und bei der Abwehr von Ansprüchen Betroffener oder Dritten sowie bei der Abwehr von Sanktionen durch Aufsichtsbehörden zeitnah und umfänglich unterstützen.

3. Rechte und Pflichten der Telekom

3.1 **[Datenverarbeitung]** Die Telekom verarbeitet die personenbezogenen Daten ausschließlich im Rahmen des getroffenen Vertrags und nach Weisung des Kunden entsprechend der Regelung der Ziffer 2.2. Die Telekom verwendet die personenbezogenen Daten für keine anderen Zwecke und wird die ihr überlassenen personenbezogenen Daten nicht an unberechtigte Dritte weitergeben. Kopien und Duplikate werden ohne vorherige Einwilligung des Kunden nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung.
Die Telekom gewährleistet, dass die mit der Verarbeitung der personenbezogenen Daten des Kunden befassten Mitarbeiter und andere für die Telekom tätigen Personen diese personenbezogenen Daten nur auf Grundlage der Weisung des Kunden verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet.

3.2 **[Datenschutzbeauftragter]** Die Telekom wird einen unabhängigen, fachkundigen und zuverlässigen Datenschutzbeauftragten bestellen, sofern dies von dem anwendbaren Recht der Europäischen Union oder des Mitgliedsstaates, dem die Telekom unterliegt, gefordert wird.

3.3 **[Räumliche Beschränkungen; Vollmacht]** Die Telekom wird die vertraglichen Leistungen in Deutschland bzw. von den mit dem Kunden in den AGB und mitgeltenden Dokumente sowie der ErgB-AV vereinbarten Leistungsstandorten aus erbringen. Änderungen des Ortes der Datenverarbeitung werden die Parteien bei Bedarf unter Beachtung der in dieser Vereinbarung festgelegten Form nach Maßgabe der Ziffer 6.2 bis Ziffer 6.6 entsprechend vereinbaren.

3.4 **[Unterstützung bei Pflichten des Verantwortlichen]** Die Telekom wird – im vertraglich vereinbarten Umfang unter Berücksichtigung der Art der Verarbeitung und der ihr zur Verfügung stehenden Informationen - den Kunden bei der Einhaltung seiner ihm nach den geltenden rechtlichen Bestimmungen obliegenden Pflichten unterstützen.

3.5 **[Unterstützung bei Überprüfung und Auskunftsbegehren]** Ist der Kunde gegenüber einer staatlichen Stelle oder einer

betroffenen Person (Betroffener) verpflichtet, Auskünfte über die Verarbeitung von personenbezogenen Daten zu geben, so wird die Telekom den Kunden darin unterstützen, diese Auskünfte zu erteilen, sofern diese Auskünfte die vertragliche Datenverarbeitung betreffen und soweit der Kunde dem Auskunftsbegehren nicht selbst oder bereits durch entsprechende Auswahl bestimmter Produktparameter nachkommen kann.

Abhängig von der Art der Verarbeitung wird die Telekom den Kunden bei dessen Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der Betroffenenrechte nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen unterstützen. Soweit sich ein Betroffener zwecks Geltendmachung eines Betroffenenrechts unmittelbar an die Telekom wendet, leitet die Telekom die Anfragen des Betroffenen zeitnah an den Kunden weiter.

Die Telekom wird den Kunden – soweit rechtlich zulässig - über an sie als Auftragsverarbeiter gerichtete Mitteilungen der Aufsichtsbehörden (z. B. Anfragen, Benachrichtigung über Maßnahmen oder Auflagen) in Verbindung mit der Verarbeitung von personenbezogenen Daten nach diesen ErgB-AV informieren. Soweit rechtlich zulässig wird die Telekom Auskünfte an Dritte, auch an Aufsichtsbehörden, nur nach schriftlicher Zustimmung durch und in Abstimmung mit dem Kunden erteilen.

3.6 **[Meldung von Zwischenfällen]** Die Telekom informiert den Kunden ohne schuldhaftes Zögern über Fälle von schwerwiegenden Betriebsstörungen, bei Verdacht auf Datenschutzverletzungen und/oder anderen Unregelmäßigkeiten bei der Verarbeitung der personenbezogenen Daten.

3.7 **[Nachweis und Dokumentation]** Die Vertragsparteien unterstützen sich gegenseitig beim Nachweis und der Dokumentation der ihnen obliegenden Rechenschaftspflicht im Hinblick auf die Grundsätze ordnungsgemäßer Datenverarbeitung.

3.8 **[Verzeichnis von im Auftrag durchgeführten Tätigkeiten der Verarbeitung]** Die Telekom führt nach Maßgabe der einschlägigen geltenden rechtlichen Bestimmungen, denen sie unterliegt, ein Verzeichnis zu allen Kategorien von im Auftrag des Kunden durchgeführten Tätigkeiten der Verarbeitung personenbezogener Daten. Die Telekom unterstützt den Kunden auf Anfrage und stellt dem Kunden die für die Führung seines Verzeichnisses von Verarbeitungstätigkeiten notwendigen Angaben zur Verfügung, soweit diese Angaben im vertraglich umschriebenen Verantwortungs- und Leistungsbereich der Telekom als Auftragsverarbeiter liegen und der Kunde keinen anderen Zugang zu diesen Informationen hat.

3.9 **[Datenschutz-Folgenabschätzung]** Falls der Kunde eine Datenschutzfolgenabschätzung durchführt und/oder eine Konsultation der Aufsichtsbehörde nach einer Datenschutzfolgenabschätzung beabsichtigt, werden sich die Vertragsparteien bei Bedarf und auf Anfrage des Kunden über Inhalt und Umfang etwaiger Unterstützungsleistungen der Telekom abstimmen.

3.10 **[Abschluss der vertraglichen Arbeiten, Rückgabe oder Löschung]** Nicht mehr benötigte personenbezogene Daten, mit Ausnahme der aufgrund gesetzlicher Verpflichtung der Telekom weiter vorzuhaltenden personenbezogenen Daten, werden, soweit nicht in den AGB und den mitgeltenden Dokumenten bereits geregelt und soweit nicht anders vereinbart, an den Kunden zurückgegeben oder auf Kosten des Kunden vernichtet bzw. gelöscht. Gleiches gilt für Test- und Ausschussmaterial. Soweit nicht bereits durch entsprechende Auswahl bestimmter Produktparameter durch den Kunden möglich, kann der Kunde während des Bestehens des Vertragsverhältnisses oder mit Vertragsende schriftlich die personenbezogenen Daten, die nicht gemäß Satz 1 vernichtet bzw. gelöscht sind, auf seine Kosten und in einem vorher abgestimmten Format heraus verlangen und der Telekom einen Zeitpunkt (längstens bis Vertragsende) für die Herausgabe nennen. Das Herausgabeverlangen muss der Telekom einen Monat vor dem vom Kunden benannten Zeitpunkt bzw. ein Monat vor Vertragsende zugegangen sein.

4. Technische und organisatorische Sicherheitsmaßnahmen

4.1 **[Technisch organisatorische Maßnahmen]** Der Kunde und die Telekom werden geeignete technische und organisatorische Maßnahmen treffen, um ein, dem Risiko angemessenes Schutzniveau zu gewährleisten.

Die derzeit als geeignet angesehenen Maßnahmen der Telekom sind in der Anlage beschrieben. Der Kunde hat die technischen und organisatorischen Maßnahmen vor dem Hintergrund seiner konkreten Datenverarbeitung in Hinblick auf ein angemessenes Schutzniveau bewertet und als angemessen akzeptiert. Etwaige Weiterentwicklungen erfolgen nach Maßgabe von Ziffer 4. 2.

4.2 **[Weiterentwicklung]** Die technischen und organisatorischen Maßnahmen können im Laufe des Vertragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden. Dabei darf das Schutzniveau das vereinbarte Schutzniveau nicht unterschreiten. Die Sicherheit der Verarbeitung und die Angemessenheit des Schutzniveaus wird der Kunde regelmäßig prüfen und der Telekom unverzüglich mitteilen, sollten die technischen und organisatorischen Maßnahmen seinen Anforderungen nicht mehr genügen. Der Kunde wird der Telekom hierzu alle erforderlichen Informationen zur Verfügung stellen. Die Telekom ihrerseits kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in ihrem Verantwortungsbereich im Einklang mit den Anforderungen der EU DSGVO erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird. Zusätzliche technische und organisatorische Maßnahmen, die über die vertraglich vereinbarten Maßnahmen hinausgehen, sind - soweit nicht ausdrücklich anders vereinbart - bei Mehraufwand für die Telekom gesondert zu vergüten. Die Vertragsparteien werden sich in diesem Fall über eine angemessene Vergütung gesondert verständigen. Bei Maßnahmen, deren Umsetzung für die Telekom nicht oder nur mit unverhältnismäßig hohem Mehraufwand möglich ist, kann die Telekom den Vertrag kündigen.

4.3 **[Überprüfung und Nachweis]** Für die Überprüfungs- und Nachweismöglichkeiten gelten Ziffer 2.4 und 2.5.

5. Vertraulichkeit

5.1 **[Vertraulichkeit]** Die Telekom wird im Zusammenhang mit der hier vereinbarten Verarbeitung personenbezogener Daten die Vertraulichkeit wahren. Sie wird die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichten, soweit diese nicht bereits einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

Vereinbarungen in den AGB und den mitgeltenden Dokumenten zur Wahrung der Vertraulichkeit und zum Schutz von nicht personenbezogenen Daten bleiben unberührt. Soweit in den AGB und den mitgeltenden Dokumenten hierzu keine Vereinbarung getroffen wurden, verpflichten sich beide Parteien, alle nicht allgemein offenkundigen Informationen aus dem Bereich der anderen Partei, die ihnen durch die Geschäftsbeziehung bekannt werden, geheim zu halten und nicht für eigene Zwecke außerhalb dieses Vertrages oder Zwecke Dritter zu verwenden.

5.2 **[Pflichten beteiligter Personen]** Die Telekom wird Personen, die Zugang zu personenbezogenen Daten haben, mit den für sie maßgeblichen Datenschutzvorgaben und Weisungen dieser Vereinbarung im Voraus vertraut machen.

6. Unterauftragsverarbeiter

6.1 **[Befugnis]** Die Telekom darf zur Erfüllung der in diesem Vertrag beschriebenen Aufgaben weitere Auftragsverarbeiter (Unterauftragsverarbeiter und Sub-Unterauftragsverarbeiter) einsetzen.

Nicht als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Aufträge zu verstehen, die die Telekom bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung erteilt und die keine Auftragsverarbeitungsleistung personenbezogener Daten für den Kunden beinhalten.

6.2 **[Gesonderte Genehmigung]** Für die in der Anlage aufgeführten Unterauftragsverarbeiter sowie Sub-Unterauftragsverarbeiter und die dort genannten Aufgabenbereiche gilt die Genehmigung des Kunden als erteilt.

6.3 **[Allgemeine schriftliche Genehmigung]** Der Kunde erteilt hiermit der Telekom die allgemeine Genehmigung für den künftigen Einsatz weiterer Auftragsverarbeiter (Unterauftrags- und Sub-Unterauftragsverarbeiter).

6.4 **[Information bei Änderungen]** Die Telekom informiert den Kunden über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung weiterer oder die Ersetzung bestehender Unterauftragsverarbeiter und/oder Sub-Unterauftragsverarbeiter, wodurch der Kunde die Möglichkeit erhält, gegen derartige Änderungen binnen 14 Tagen nach Zugang der Information beim Kunden Einspruch zu erheben. Der Kunde wird die Genehmigung derartiger Änderungen nicht ohne wichtigen Grund verweigern. Sofern der Kunde von seinem Einspruchsrecht Gebrauch macht und die Telekom den Unterauftragsverarbeiter und/oder Sub-Unterauftragsverarbeiter trotzdem einsetzt, kann der Kunde den Vertrag fristlos kündigen.

6.5 **[Auswahl]** Die Telekom wird Unterauftragsverarbeiter auswählen, die hinreichende Garantien dafür bieten, dass die vereinbarten geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen der einschlägigen geltenden rechtlichen Bestimmungen erfolgt. Die Telekom wird mit Unterauftragsverarbeitern vertragliche Vereinbarungen treffen, die den vertraglichen Regelungen dieser ErgB-AV inhaltlich entsprechen. Die Telekom wird mit dem Unterauftragsverarbeiter die technischen und organisatorischen Maßnahmen festlegen und sich die Einhaltung der vereinbarten technischen und organisatorischen Maßnahmen von diesem regelmäßig bestätigen lassen.

6.6 **[Sub-Unterauftragsverarbeiter]** Die Beauftragung von Sub-Unterauftragsverarbeitern ist nach Maßgabe der Ziffer 6.1 bis Ziffer 6.5 entsprechend zulässig.

7. Vertragsdauer; Kündigung

Diese Vereinbarung gilt für die Dauer der tatsächlichen Leistungserbringung durch die Telekom. Dies gilt unabhängig von der Laufzeit etwaiger anderer Verträge (insbesondere der AGB und den mitgeltenden Dokumenten), die die Parteien ebenfalls bzgl. der Erbringung der vereinbarten Leistungen abgeschlossen haben.

8. Haftung und Freistellung

8.1 **[Verantwortungsbereich des Kunden]** Der Kunde gewährleistet in seinem Verantwortungsbereich die Umsetzung der sich aus den einschlägigen geltenden rechtlichen Bestimmungen ergebenden Pflichten bei der Verarbeitung personenbezogener Daten.

8.2 **[Haftung]** Die Haftungsregelung aus den AGB und den mitgeltenden Dokumenten gilt für diese ErgB-AV, soweit nicht eine Haftungsbeschränkung nach Maßgabe der jeweils einschlägigen geltenden rechtlichen Bestimmungen zugunsten der Telekom greift.

9. Sonstiges

9.1 **[Gültigkeit des Vertrags]** Von der Ungültigkeit einer Bestimmung dieser ErgB-AV bleibt die Gültigkeit der übrigen Bestimmungen unberührt. Sollte sich eine Bestimmung als unwirksam erweisen, werden die Parteien diese durch eine neue ersetzen, die dem von den Parteien Gewollten am nächsten kommt.

9.2 **[Änderungen des Vertrags]** Sämtliche Änderungen dieser ErgB-AV sowie Nebenabreden bedürfen der Textform (einschließlich der elektronischen Form). Dies gilt auch für das Abbedingen dieser Schriftformklausel selbst.

9.3 **[Geschäftsbedingungen]** Es besteht zwischen den Parteien Einigkeit darüber, dass die „Allgemeinen Geschäftsbedingungen" des Kunden auf diese ErgB-AV keine Anwendung finden.

9.4 **[Gerichtsstand]** Der alleinige Gerichtsstand für alle Streitigkeiten aus und im Zusammenhang mit diesen ErgB-AV ist Bonn. Dieser gilt vorbehaltlich eines etwaigen ausschließlich gesetzlichen Gerichtsstandes.

9.5 **[Rechtsgrundlage]** Dieser ErgB-AV liegen die Bestimmungen der EU-Datenschutzgrundverordnung (EU

DSGVO) zugrunde. Gegebenenfalls ergänzende landesspezifische Regelungen sind in der Anlage aufgeführt.

9.6 **[Vorrangregelung]** Bei Widersprüchen zwischen den Bestimmungen dieser ErgB-AV und Bestimmungen sonstiger Vereinbarungen, insbesondere der AGB und den mitgeltenden Dokumenten, sind die Bestimmungen dieser ErgB-AV maßgebend. Im Übrigen bleiben die Bestimmungen der AGB und den mitgeltenden Dokumenten unberührt und gelten für diese ErgB-AV entsprechend.

Anlage zu Ergänzende Bedingungen Auftragsdatenverarbeitung personenbezogener Daten für Open Telekom Cloud

1. Einzelheiten der Datenverarbeitung

a) Angaben zu „Kategorien von Verarbeitungen":

☒ IaaS (Infrastructure as a Service)

b) Kategorien betroffener Personen:

☒ Kunden

☒ alle Personen deren Daten der Kunden in der Open Telekom Cloud speichert

c) Betroffene personenbezogene Daten:

☒ Name

☒ Kontaktdaten (z. B. Telefon, E-Mail

☒ Personenbeziehbare oder personenbezogene Protokolldaten (Benutzernamen, IP-Adresse)

☒ Alle anderen personenbezogenen Daten, die in Art 4 Nr. 1 der DSGVO definiert sind, die vom Kunden im Zuge der Nutzung des Produktes übermittelt oder gespeichert wird.

d) Besondere Kategorien von personenbezogenen Daten: (z.B. Art. 9 DSGVO (müssen hier detailliert angegeben werden)
keine

2. Zugriff auf personenbezogene Daten

Der Kunde stellt der Telekom die personenbezogenen Daten bereit, ermöglicht ihm Zugriff auf die personenbezogenen Daten oder erlaubt ihm, die personenbezogenen Daten zu erheben und zwar wie nachfolgend beschrieben:

☒ Übermittlung durch den Verantwortlichen (Kunde) über gesicherte und verschlüsselte Verbindung:

Internet, IP VPN

3. Leistungen; Vertragszweck:

Die Art der Leistung sowie der Verarbeitungszweck sind in den Produkt-AGB und der Leistungsbeschreibung abschließend geregelt.

4. Verarbeitungsort:

Die Verarbeitung der Daten findet in Deutschland und Ungarn statt.

5. Technische und organisatorische Sicherheitsmaßnahmen

Für die beauftragte Erhebung und / oder Verarbeitung von personenbezogenen Daten werden folgende Maßnahmen vereinbart:

a) Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

- Zutrittskontrolle
  Kein unbefugter Zutritt zu Datenverarbeitungsanlagen, z.B.: Magnet- oder Chipkarten, Schlüssel, elektrische Türöffner, Werkschutz bzw. Pförtner, Alarmanlagen, Videoanlagen;
- Zugangskontrolle
  Keine unbefugte Systembenutzung, z.B.: (sichere) Kennwörter, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern;
- Zugriffskontrolle
  Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B.: Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen;
- Trennungskontrolle
  Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, z.B. Mandantenfähigkeit, Sandboxing;
- Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)
  Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen;

b) Integrität (Art. 32 Abs. 1 lit. b DSGVO)

- Weitergabekontrolle
  Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z.B.: Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur;
- Eingabekontrolle
  Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben,

verändert oder entfernt worden sind, z.B.: Protokollierung, Dokumentenmanagement;

c) Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)
- Verfügbarkeitskontrolle
  Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backup-Strategie (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfallpläne;
- Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO);

d) Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)
- Datenschutz-Management;
- Incident-Response-Management;
- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO);
- Auftragskontrolle
  Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DSGVO ohne entsprechende Weisung des Auftraggebers, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.

6. Nachweis durch die Telekom

Der Telekom steht es frei, die hinreichende Umsetzung der Pflichten aus diesen ErgB AV, insbesondere der technisch-organisatorischen Maßnahmen (Ziffer 6) und Maßnahmen, die nicht nur den konkreten Auftrag betreffen, durch einen der folgenden Nachweise zu belegen:

☒ Die Zertifizierung nach einem genehmigten Zertifizierungsverfahren; siehe unter cloud.telekom.de

7. Genehmigte Unterauftragsverarbeiter

Angaben zu Unterauftragsverarbeitern / Leistungen / Verarbeitungsorte

Gesonderte Genehmigung:
Telekom beabsichtigt, die folgenden Unterauftragsverarbeiter für die folgenden Leistungen / an den folgenden Verarbeitungsorten einzusetzen:

Die Telekom beabsichtigt Unterauftragnehmer zu beauftragen. Welche dies konkret sind, ist abrufbar bzw. über GDPR@telekom.de zu erfragen

ANLAGE 4

Technisch organisatorische Maßnahmen 1&1 Internet AG

Mailserver-Provider für das Antragsmanagement. Automatisiertes Versenden von E-Mails in Verbindung mit dem Formularserver z.B. Eingangsbenachrichtigungen.

Die technischen und organisatorischen Maßnahmen sind nachfolgend abgedruckt.

Technische und organisatorische Maßnahmen nach Art. 32 DSGVO

Informationen zum Dokument	
Version	1.0
Datum	07.02.2019
Dokumentenklassifikation	Öffentlich
Genehmigungsstatus	Genehmigt
Ursprungsversion freigegeben durch	Datenschutzbeauftragter 1&1
Aktuelle Version freigegeben durch	Konzerndatenschutzbeauftragter United Internet AG
Freigegeben am	07.02.2019

Hinweis

Dieses Dokument enthält Informationen, welche Geschäftspartnern, Kunden sowie weiteren externen Stellen, die ein gesetzliches oder sonstig begründetes Einsichtsrecht haben, zur Verfügung gestellt werden.

Aus Gründen der Lesbarkeit wurde im Text die männliche Form gewählt, nichtsdestoweniger beziehen sich die Angaben auf Angehörige aller Geschlechter.

Präambel

Der Verantwortliche hat geeignete Maßnahmen zur Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit sowie Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung implementiert.

Der allgemeine Teil beschreibt technische und organisatorische Maßnahmen die unabhängig von den jeweiligen Dienstleistungen und Services, Standorten und Kunden gelten. In den Anhängen sind Maßnahmen beschrieben, die über die im allgemeinen Teil dokumentierten Maßnahmen hinaus gelten.

1. Vertraulichkeit

Vertraulichkeit ist die Eigenschaft, dass personenbezogene Daten unberechtigten Personen, Einheiten oder Prozessen nicht verfügbar gemacht oder enthüllt werden.

Zutrittskontrolle

- Empfangs- und Sicherheitsdienst
- Individuelle, dokumentierte und rollenabhängige Zutrittsberechtigungen (Karten, Transponder und Schlüssel)
- Mitarbeiter- und Besucherausweise
- Besucher dürfen sich grundsätzlich nur in Begleitung eines Mitarbeiter im Gebäude aufhalten
- Alarm- und Einbruchmeldeanlage
- Büroräume sind außerhalb der Arbeitszeit verschlossen

Zugangskontrolle

- Formale Benutzer- und Berechtigungsverfahren
- Login nur mit Benutzername, Passwort und wo erforderlich 2-Faktor-Authentifizierung
- Systemisch forcierte Passwortrichtlinien
- VPN bei Remotezugriff und durch vom Verantwortlichen verwaltete Geräte
- Mobile Device Management
- Mobile Datenträger sind verschlüsselt
- Automatische Sperre von Desktops nach wenigen Minuten Inaktivität
- Clean Desk-Policy

Zugriffskontrolle

- Führen von Assetregistern und Ableitung von Maßnahmen anhand der Datenklassifikation
- Nutzung kryptografischer Verfahren (z.B. Verschlüsselung)
- Umsetzung von Berechtigungskonzepten nach dem Need-to-Know-Prinzip
- Trennung von Anwendungs- und Administrationszugängen
- Protokollierung von Zugriffsversuchen
- Einrichtung von Administratorarbeitsplätzen
- Minimale Anzahl an Administratoren
- Nutzung von Dokumentenvernichtung

Pseudonymisierung

- Sofern möglich oder erforderlich werden personenbezogene Daten pseudonymisiert verarbeitet (Trennung der Zuordnungsdaten und Aufbewahrung in getrenntem System)

Trennungskontrolle

- Trennung von Entwicklungs-, Test- und Produktivumgebung
- Personenbezogene Daten dürfen nicht für Testzwecke verwendet werden

- Mandantenfähigkeit / logische Trennung von Daten bei relevanten Anwendungen: Separate Datenbanken, Schema-Trennung in Datenbanken, Berechtigungskonzepte und/oder strukturierte Dateiablage

2. Integrität

Die Integrität personenbezogener Daten ist dann gewahrt, wenn sie richtig, unverändert und vollständig sind.

Weitergabekontrolle

- Bereitstellung von Daten über verschlüsselte Verbindungen (z.B. SFTP)
- Weitergabe von personenbezogenen Daten im Sinne des Need-to-Know / Need-to-Do-Prinzips
- Personenbezogene Daten werde nach ihrem Schutzbedarf klassifiziert, wobei vertrauliche Daten nur über sichere Kommunikationswege übertragen werden dürfe
- Wo möglich wird E-Mailverschlüsselung eingesetzt
- Wo möglich werden personenbezogene Daten nur in pseudonymisierter oder anonymisierter Form übermittelt
- Dokumentation der Weitergabe von physischen Speichermedien
- Weitergabe von Papierdokumenten mit personenbezogenen Daten in einem verschlossenen undurchsichtigen Umschlag

Eingabekontrolle

- Technische Protokollierung der Eingabe, Änderung und Löschung von personenbezogenen Daten sowie Kontrolle der Protokolle
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch Individuelle Benutzernamen (nicht Benutzergruppen)
- Rollenbasiertes Berechtigungskonzept (Lese-, Schreib-, und Löschrechte)
- Protokollierung von administrativen Änderungen

3. Verfügbarkeit und Belastbarkeit

Die Verfügbarkeit von personenbezogenen Daten ist vorhanden, wenn diese von den Anwendern stets wie vorgesehen genutzt werden können

- Einsatz von Hardware- und Softwarefirewalls
- Intrusion Detection Systeme
- Überspannungsschutz der Gebäudeaußenhaut gegen Blitzeinschlag
- Unterbrechungsfreie-Stromversorgung (USV)
- Notfallhandbücher für die Datenwiederherstellung, Schutz gegen versehentliche Zerstörung und Verlust
- Durchführung von Wiederherstellungstests
- Wo notwendig Nutzung redundanter Systeme (z.B. RAID)
- Regelmäßiger Test von Datensicherungen
- Externe Audits und Sicherheitstests

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Wie wird gewährleistet, dass die genannten Datensicherungsmaßnahmen regelmäßig überprüft werden?

Datenschutz-Management

- Datenschutzbeauftragte und ein Informationssicherheitsbeauftragter sind benannt

- Etablierung einer Datenschutz- und Informationssicherheitsorganisation
- Alle Mitarbeiter sind auf die Vertraulichkeit im Umgang mit personenbezogenen Daten verpflichtet und werden auf das Telekommunikationsgeheimnis hingewiesen
- Mitarbeiter sind im Umgang mit personenbezogenen Daten sensibilisiert
- Neue Mitarbeiter erhalten Informationsmaterial bezüglich dem Umgang mit personenbezogenen Daten
- Ein Verzeichnis von Verarbeitungstätigkeiten wird gepflegt und Datenschutzfolgenabschätzungen werden bei Bedarf durchgeführt
- Prozesse zur Wahrnehmung von Betroffenenrechten sind etabliert

Auftragskontrolle

- Daten die im Auftrag verarbeitet werden, werden nur nach Weisungen des Auftraggebers verarbeitet
- Auftragnehmer werden im Hinblick auf getroffene technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten sorgfältig ausgewählt
- Weisungen zum Umgang mit personenbezogenen Daten werden in Textform dokumentiert
- Sofern erforderlich werden Auftragsverarbeitungsvereinbarungen bzw. geeignete Garantien zur Übermittlung von Daten an Drittländer geschlossen

Datenschutzfreundliche Voreinstellungen

- Es wird prozessual sichergestellt, dass Systeme und Produkte datenschutzfreundlich entwickelt werden
- Es werden nur diejenigen personenbezogenen Daten erhoben, die für den jeweiligen Zweck erforderlich sind

Incident-Response-Management

- Dokumentierter Prozess zur Erkennung, Meldung und Dokumentation von Datenschutzverletzungen unter Einbindung des Datenschutzbeauftragten
- Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen unter Einbindung des Informationssicherheitsbeauftragten

Anhang 1: Besondere technische und organisatorische Maßnahmen für Rechenzentren

- Alle Rechenzentren sind nach dem ISO 27001 Standard zertifiziert
- Elektronische Zutrittskontrollsysteme überwachen und gewährleisten den Zutritt zum jeweiligen Rechenzentrum nur für autorisierte Personen
- Sicherheitsschleuse
- Videokameras sowie Einbruch- und Kontaktmelder überwachen die Außenhaut des Gebäudes
- Definierte Sicherheitszonen
- Hochredundante Netzwerkinfrastruktur
- Feuer und/oder Rauchmelder verfügt über eine direkte Aufschaltung bei der örtlichen Feuerwehr
- Kühlsystem im Rechenzentrum / Serverraum
- Serverraumüberwachung Temperatur und Feuchtigkeit
- Keine sanitären Anschlüsse im oder oberhalb von Rechenzentren
- Alarmmeldung bei unberechtigtem Zutritt zu Rechenzentren

ANLAGE 5

Technisch organisatorische Maßnahmen TeamViewer GmbH

TeamViewer ist eine Software, die bei Form-Solutions für Supportfälle, Screen-Sharing und Fernwartungszugriffe zum Einsatz kommt.

Auf Ihre Anfrage hin leisten wir Ihnen auch technischen Support auf Ihren Systemen. Im Rahmen von Fernwartungssessions mit dem Werkzeug TeamViewer realisieren wir gemeinsam mit Ihnen einen Vieraugenzugriff auf Ihre Administrationsoberfläche. Diese Sitzungen werden standardmäßig von uns aufgezeichnet und für einen Zeitraum von 6 Monaten zu Revisionszwecken vorrätig gehalten. Falls Sie nicht damit einverstanden sind, informieren Sie bitte zu Beginn der Sitzung den Form-Solutions Mitarbeiter.

Die technischen und organisatorischen Maßnahmen der Firma TeamViewer GmbH sind nachfolgend abgedruckt.

Kundendaten, Vertragsdaten (Büro)	TeamViewer Software (Rechenzentren)
Zutrittskontrolle	
• Das Betriebsgebäude bildet nach außen hin eine geschlossene Einheit. Türen und Tore der Gebäude sind mit Sicherheitsschlössern versehen. Türen und Fenster sind außerhalb der Betriebszeiten fest verschlossen. • Die Schlüssel zu den Räumlichkeiten, in denen Daten verarbeitet werden, befinden sich in der ausschließlichen Obhut der zuständigen Mitarbeiter. Dritte haben zu den Räumlichkeiten keinen Zutritt. Über ein elektronisches Schließsystem wird durch verschiedene Berechtigungsstufen gewährleistet, dass Mitarbeiter neben den allgemeinen Bereichen nur ihre eigenen Räume betreten können. Die Vergabe von Schlüsseln ist schriftlich geregelt. • Darüber hinaus erhalten alle Mitarbeiter eine Schlüsselkarte, die den Zutritt je nach individuellen Berechtigungen des jeweiligen Mitarbeiters gestattet. Zudem dient diese Schlüsselkarte als Mitarbeiterausweis (mit Bild). • Besucher des Bürogebäudes werden durch einen Sicherheitsdienst empfangen und erhalten einen Besucherausweis (ohne Bild). • Die Eingangsbereiche werden Videoüberwacht. • Das Gebäude ist 24/7 überwacht durch einen sorgfältig ausgewählten Sicherheitsdienst.	• Der Zugang zu den Rechenzentren, in denen die zentralen TeamViewer Verbindungsserver stehen, ist nur autorisierten Personen möglich; Videokameras, elektronische Zugangskontrollsysteme, Bewegungs-, Einbruchs- und Kontaktmelder sowie 24/7-Überwachung durch Sicherheitspersonal vor Ort schützen und überwachen die Gebäude nach außen hin.
Zugangskontrolle	
• Der Zugang zu den Datenverarbeitungssystemen erfolgt über eine zweistufige Zugangskennung, mindestens mit Benutzernamen und Passwort. • Für besonders sensible Bereiche ist darüber hinaus eine Zweifaktorauthentifizierung erforderlich.	
Zugriffskontrolle	
• Berechtigte Personen, die sich mit ihrer Nutzerkennung ordnungsgemäß am DV-System identifiziert haben, besitzen entsprechend ihrer Nutzerrechte differenzierte und damit abgestufte Berechtigungen in den jeweiligen Software-Systemen.	**• Während einer TeamViewer-Verbindung werden zu keinem Zeitpunkt Verbindungsinhalte an unser System übermittelt.** TeamViewer arbeitet mit vollständiger Verschlüsselung auf Basis eines RSA Public-/Private Key Exchange und AES (256 Bit) Session Encoding. Diese Technik wird in vergleichbarer Form auch bei

• Alle Mitarbeiter der TeamViewer GmbH sind gemäß § 5 BDSG auf das Datengeheimnis verpflichtet und entsprechend geschult.	https/SSL eingesetzt und gilt nach heutigem Stand der Technik als vollständig sicher. Alle Verbindungen sind vollständig Ende-zu-Ende verschlüsselt. Da der Private Key niemals den Clientrechner verlässt, ist durch dieses Verfahren technisch sichergestellt, dass zwischengeschaltete Rechner im Internet den Datenstrom nicht entziffern können. Das gilt somit auch für die TeamViewer- Routingserver. Weitere Informationen hierzu finden sich auch in unserem Sicherheitsstatement unter: http://www.TeamViewer.com/images/pdf/ TeamViewer_Sicherheitsstatement.pdf.
Weitergabekontrolle	
• Sicherung bei der elektronischen Übertragung: Durch ein 2048 Bit RSA verschlüsseltes Zertifikat wird sichergestellt, dass externe Mitarbeiter sich stets hochverschlüsselt in das interne Netzwerk verbinden. • Transport: Der physikalische Transport von Akten mit personenbezogenen Daten geschieht ausschließlich in verschlossenen Behältern.	• Sicherung bei der elektronischen Übertragung: Durch den Einsatz geeigneter Fernwartungslösungen wird sichergestellt, dass sich stets hochverschlüsselt zu den TeamViewer-Verbindungsservern verbunden wird.
Eingabekontrolle	
• Aufgrund von individuellen Nutzerkennungen sowie Protokolldaten kann überprüft und festgestellt werden, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.	
Auftragskontrolle	
• Die Verarbeitung der personenbezogenen Daten geschieht ausschließlich im Rahmen der vertraglich festgelegten Weisungen des Auftraggebers. • Mit Unternehmen, die mit der Verarbeitung personenbezogener Daten beauftragt sind, wurden entsprechende und geeignete Auftragsdatenverarbeitungsverträge geschlossen.	
• Die Rechenzentren, in denen die zentralen TeamViewer-Verbindungsserver stehen, sind nach ISO/IEC 27001 zertifiziert.	

Verfügbarkeitskontrolle	
Folgende Maßnahmen stellen sicher, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind: • Brandschutzmaßnahmen: Geeignete Kohlendioxid-Feuerlöscher für Serverräume • Unterbrechungsfreie Stromversorgung (USV) inklusive Überspannungsschutz • Serverraum-Klimaanlagen: Primäre 9400 Watt Klimaanlage. Als Backup fungiert eine zentrale Klimaanlage. • RAID: Einsatz von verschiedenen RAID-Lösungen je nach Zweckmäßigkeit • Backupkonzept: - Datensicherheitskonzept nach dem Generationenprinzip (GFS-Rotation) - Backup-Lösung mit Bandsicherung auf ein Laufwerk - Sicherheitskopien werden extern geeignet aufbewahrt • Virenschutzkonzept: - Zentrale Firewall - unternehmensweiter Einsatz von Antivirensoftware für Firmen	• Die zentralen TeamViewer Verbindungsserver befinden sich in einem hochmodernen Datacenter mit multiredundanter Carrier-Anbindung und redundanter Stromversorgung. Es wird ausschließlich Markenhardware eingesetzt. • Entsprechende RAID-Lösungen, sowie tägliche Backups zu geographisch getrennten Servern garantieren höchste Verfügbarkeit. • Firewalls mit entsprechend gehärteten Regelsätzen schützen vor Angriffen von außen. • Überwachung der Produktiv-Infrastruktur und des Netzwerkverkehrs mit Hilfe entsprechender Monitoring Software.
Trennungsgebot	
• Getrennte Ordnerstrukturen, separate Tabellen innerhalb von Datenbanken sowie komplett getrennte Datenbanken gewährleisten eine separate Speicherung und Verarbeitung personenbezogener Daten, die zu unterschiedlichen Zwecken erhoben wurden.	• Separate Tabellen innerhalb von Datenbanken sowie komplett getrennte Datenbanken gewährleisten eine separate Speicherung und Verarbeitung personenbezogener Daten, welche von den Kunden selbst erstellt und gepflegt werden (z.B.: Daten des „TeamViewer-Kontos“).
Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Daher ist es der TeamViewer GmbH gestattet alternative Maßnahmen umzusetzen, sofern diese das Sicherheitsniveau der betreffenden Maßnahmen nicht unterschreiten.	

ANLAGE 6

Technisch organisatorische Maßnahmen LogMeIn Ireland Limited

GoToMeeting® ist eine Software, die bei Form-Solutions für Web-Schulungen und Online-Meetings zum Einsatz kommt.

Die Zertifizierung nach einem genehmigten Zertifizierungsverfahren, siehe unter:
https://www.goto.com/de/company/trust/resource-center

Die technischen und organisatorischen Maßnahmen der Firma LogMeIn
sind nachfolgend abgedruckt.

TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN FÜR GOTO MEETING, GOTO WEBINAR, GOTO TRAINING UND GOTO STAGE

Operative Sicherheits- und Datenschutzkontrollen

V3.2

Datum der Veröffentlichung: Februar 2022

1 Produkte und Services

Dieses Dokument behandelt die technischen und organisatorischen Maßnahmen (TOMs) für GoTo Meeting, GoTo Webinar, GoTo Training und GoTo Stage (zusammenfassend als „UCC-Lösungen von GoTo" bezeichnet).

Bei den GoTo-Produkten der UCC-Lösungen handelt es sich um Online-Kommunikationsservices, die es Einzelpersonen und Organisationen ermöglichen, je nach Service-Angebot mit zahlreichen Funktionen zu interagieren. Dazu gehören Bildschirmfreigabe, Videokonferenzen und integriertes Audio. Die GoTo-Services der UCC-Lösungen werden mit Hilfe eines Webbrowsers oder eines Client-Programms über ein global verteiltes Netzwerk proprietärer Hardware und Software bereitgestellt.

- GoTo Meeting ermöglicht es Benutzern, Sitzungen über die GoTo Meeting-Website bzw. über Client-Software zu planen, einzuberufen und zu moderieren.
- GoTo Webinar ermöglicht es Unternehmen, über das Internet Events und Präsentationen für ein größeres lokales oder globales Publikum durchzuführen. Webinare werden über die GoTo Webinar-Website und/oder die Client-Software geplant, einberufen und moderiert.
- GoTo Training ermöglicht es Benutzern, Schulungssitzungen über die GoTo Training-Website bzw. über Client-Software zu planen, einzuberufen und zu moderieren. Es bietet spezielle Funktionen für webbasierte Schulungen wie Online-Zugang zu Tests und Schulungsmaterialien und ein gehostetes Kursverzeichnis.
- GoTo Stage ist ein Online-Portal, in dem GoTo Webinar-Organisatoren anpassbare Kanäle erstellen und ihre aufgezeichneten Webinare veröffentlichen können. Veröffentlichte Aufzeichnungen werden von uns in einer Reihe geschäftlicher Kategorien auf der GoTo Stage-Homepage vorgestellt. Organisatoren können die Veröffentlichung ihrer Aufzeichnungen über GoTo Webinar jederzeit rückgängig machen, wodurch die Videos von ihrer Kanalseite und aus der GoTo Stage-Umgebung gelöscht werden.

2 Produktarchitektur

Die Bildschirmübertragung zwischen den Teilnehmern in Sitzungen der UCC-Lösungen von GoTo erfolgt über einen Overlay Networking Stack, der logisch über dem konventionellen TCP/IP-Stack auf den Computern der einzelnen Benutzer angeordnet ist (siehe Abbildung 1).

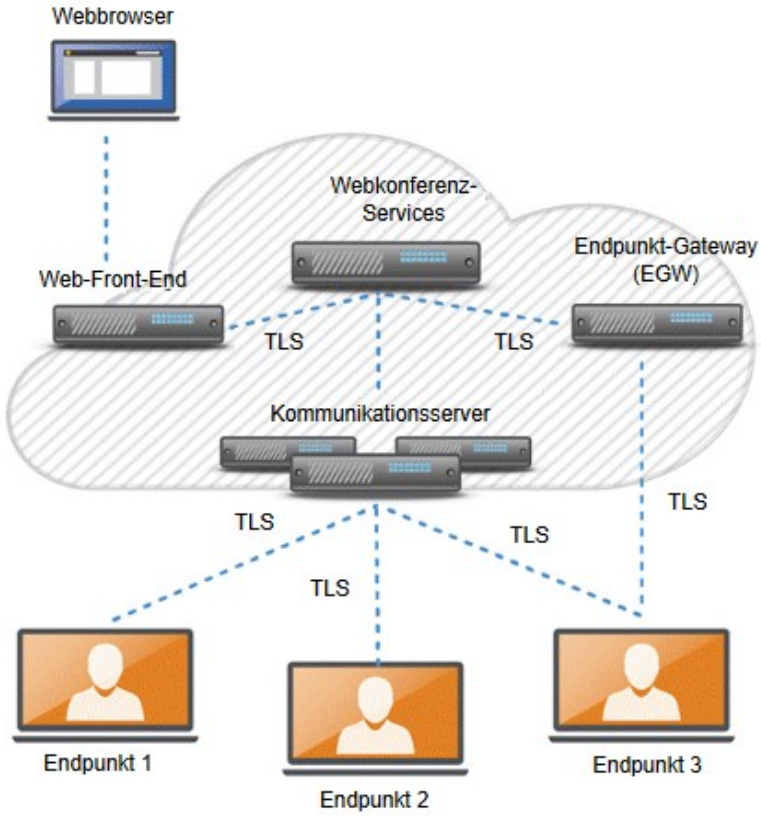

Abbildung 1 – Architektur von GoTo Meeting, GoTo Webinar, GoTo Training und GoTo Stage.

***Web-Front-End** – Portal-Webseite der GoTo-Suite, wird in Co-Location-Rechenzentren an Tier 1 und auf AWS gehostet*

***WCS** – Sitzungsplanung, Meetingchronik, GTM-Organisatoreinstellungen, wird in Co-Location-Rechenzentren an Tier 1 gehostet*

***Kommunikationsserver** – inkl. Server für Bildschirmfreigabe, Audio Bridges und Voice Gateways (als Proxy), H.323-Gateways – gehostet auf Amazon Web Services/**Multicast-Kommunikationsserver** und Video Cluster Server in Co-Location-Rechenzentren an Tier 1 gehostet*

***Endpunkt-Gateway (EGW)** – verarbeitet Organisator- und Endpunktverbindungen und Verschlüsselungsmechanismen – EGW auf Amazon Web Services gehostet*

Die Teilnehmer (Sitzungsendpunkte) verwenden ausgehende TCP/IP-Verbindungen über den Port 443, um mit den Kommunikationsservern und Gateways der Infrastruktur zu kommunizieren. Dabei können sich die Teilnehmer überall im Internet befinden. Clients kommunizieren in der Regel über das Endpunkt-Gateway mit den UCC-Lösungen von GoTo. Neue Clients kommunizieren jedoch direkt mit Hilfe von REST-Aufrufen (Representational

State Transfer) über Lastenausgleiche mit den Back-End-Services. Die Service-Infrastruktur ermöglicht es Benutzern des Telefonnetzes, sich in ein Meeting einzuwählen.

GoTo-Produkte von UCC-Lösungen verwenden ein ASP-Modell (Application Service Provider), das einen sicheren Betrieb gewährleistet und sich dabei in die bestehende Netzwerk- und Sicherheitsinfrastruktur eines Unternehmens einfügt.

Die Architektur ist für eine hohe Leistung, Zuverlässigkeit und Skalierbarkeit konzipiert und wird auf Hochleistungsservern betrieben, auf denen die entsprechenden Sicherheitspatches installiert sind. Redundante Switches und Router sind so konzipiert, dass „Single Points of Failure" ausgeschlossen werden. Geclusterte Server und Backup-Systeme stellen selbst bei hoher Auslastung oder einem Systemausfall sicher, dass die Anwendungsprozesse funktionieren. Webkonferenz-Services verteilen die Last der Client/Server-Sitzungen auf geografisch verteilte Kommunikationsserver, um die Leistung und eine angemessene Latenz sicherzustellen.

Die Service-Infrastruktur wird hauptsächlich in Co-Location-Rechenzentren an Tier 1 gehostet, wobei einige Komponenten-Services bei Cloud-Hosting-Anbietern gehostet werden. Die Audio Bridge-Services werden vollständig von Cloud-Anbietern gehostet, während einige der Webkonferenz-Services für Produkte teilweise von Cloud-Anbietern gehostet werden. Die Daten, die mit einem von einem Cloud-Anbieter gehosteten Service verbunden sind, werden auch bei diesem Anbieter gespeichert.

Der physische Zugriff auf Co-Location Hosted Servern ist eingeschränkt und wird kontinuierlich überwacht. Alle Standorte verfügen über redundante Stromversorgungen und entsprechende Einrichtungen zur Kontrolle der Umgebungsbedingungen. Die privaten Netzwerke und Back-End-Server von GoTo sind durch Firewalls, Router und VPN-basierte Zugangskontrollen gesichert. Die Sicherheit der Infrastruktur wird kontinuierlich überwacht. Interne Mitarbeiter und externe Prüfer führen regelmäßige Tests auf Schwachstellen durch.

Weitere Informationen finden Sie im Whitepaper zur UCC-Sicherheit.

3 Technische Sicherheitskontrollen für UCC-Lösungen von GoTo

GoTo nutzt technische Kontrollen nach Branchenstandard gemäß der Art und Weise und des Umfangs der Services (gemäß Definition des Begriffs in den Nutzungsbedingungen). Diese Kontrollen wurden zum Schutz der Service-Infrastruktur und der darin enthaltenen Daten entwickelt. Sie finden die Nutzungsbedingungen unter https://www.goto.com/company/legal/terms-and-conditions.

3.1 Logische Zugriffskontrolle

Es werden logische Zugriffskontrollverfahren eingesetzt, um die durch nicht autorisierten Anwendungszugriff entstehenden Bedrohungen und einen Datenverlust in Unternehmens- und Produktionsumgebungen zu verhindern oder zu minimieren. Mitarbeiter erhalten bei Bedarf minimalen Zugriff (oder „Least Privilege"-Zugriff) auf angegebene GoTo-Systeme, -Anwendungen, -Netzwerke und -Geräte. Zudem sind Benutzerrechte basierend auf der funktionalen Rolle und Umgebung voneinander getrennt.

3.2 Perimeterverteidigung und Erkennung von Eindringversuchen

GoTo setzt Standard-Tools, -Techniken und -Services für den Perimeterschutz ein, die verhindern sollen, dass nicht autorisierter Netzwerkdatenverkehr in unsere Produktinfrastruktur gelangt. Das GoTo-Netzwerk enthält nach außen gerichtete Firewalls und eine interne Netzwerksegmentierung. Cloud-Ressourcen nutzen auch Host-basierte Firewalls. Außerdem wird ein Cloud-basierter DDoS-Schutzservice (Distributed Denial of Service) eines Drittanbieters zum Schutz vor umfangreichen DDoS-Angriffen verwendet. Dieser Service wird mindestens einmal pro Jahr getestet. Wichtige Systemdateien werden vor böswilliger oder unbeabsichtigter Infizierung oder Zerstörung geschützt.

3.3 Datentrennung

GoTo nutzt eine Architektur mit mehreren Mandanten, die basierend auf dem GoTo-Konto eines Benutzers oder einer Organisation logisch auf Datenbankebene getrennt ist. Nur authentifizierten Parteien wird Zugriff auf die relevanten Konten gewährt.

3.4 Physische Sicherheit

Physische Rechenzentrumssicherheit

GoTo arbeitet mit Rechenzentren zusammen, um physische Sicherheits- und Umgebungskontrollen für Serverräume mit Produktionsservern zu bieten. Zu diesen Kontrollen gehören:

- Videoüberwachung und Aufzeichnung
- Multifaktor-Authentifizierung für hochsensible Bereiche
- Temperaturregelung von Heizung, Lüftung und Klimaanlage
- Sprinkleranlage und Rauchmelder
- Unterbrechungsfreie Stromversorgung (USV)
- Zwischenböden oder umfassendes Kabelmanagement
- Kontinuierliche Überwachung und Warnmeldungen
- Schutz vor häufigen Naturkatastrophen und vom Menschen verursachten Katastrophen entsprechend der Geografie und des Standorts des jeweiligen Rechenzentrums
- Geplante Wartung und Validierung aller wichtigen Sicherheits- und Umgebungskontrollen

GoTo beschränkt den physischen Zugang zu Produktionsrechenzentren nur auf autorisierte Einzelpersonen. Für den Zugang zu einer Hosting-Einrichtung ist die Einreichung eines Antrags über das entsprechende Ticketing-System und die Genehmigung des jeweiligen Managers sowie eine Überprüfung und Genehmigung der Technikabteilung erforderlich. Die GoTo-Verwaltung überprüft die Protokolle für den physischen Zugang zu Rechenzentren und Serverräumen mindestens auf vierteljährlicher Basis. Außerdem wird der physische Zugang zu Rechenzentren bei Kündigung von bereits autorisiertem Personal entfernt.

3.5 Daten-Backup, Notfallwiederherstellung und Verfügbarkeit

Die Architektur von GoTo wurde im Allgemeinen so konzipiert, dass die Replikation zu geografisch verteilten Standorten nahezu in Echtzeit erfolgt. Datenbanken werden mit Hilfe einer rollierenden inkrementellen Backup-Strategie gesichert. Im Falle eines Notfalls oder eines Totalausfalls einer der vielen aktiven Sites können die übrigen Standorte die Anwendungslast ausgleichen. Die Notfallwiederherstellung der Systeme wird regelmäßig getestet.

3.6 Malware-Schutz

Malware-Schutzsoftware mit Überwachungsprotokollen wird auf allen Servern der UCC-Lösungen von GoTo eingesetzt. Warnmeldungen, die auf mögliche böswillige Aktivitäten hinweisen, werden an ein entsprechendes Reaktionsteam gesendet.

3.7 Vertraulichkeit und Authentizität der Daten

GoTo verfügt über einen kryptografischen Standard, der sich nach Empfehlungen von Branchengruppen, staatlichen Veröffentlichungen und anderen für Standards relevanten Gruppen richtet. Der kryptografische Standard wird regelmäßig überprüft und ausgewählte Technologien und Cipher werden in Einklang mit dem bewerteten Risiko und der Marktakzeptanz neuer Standards aktualisiert.

3.7.1 Übertragene Daten

GoTo Meeting, GoTo Webinar und GoTo Training umfassen Sicherheitsmaßnahmen für übertragene Daten zum Schutz vor und zur Abwehr von passiven und aktiven Angriffen auf die Vertraulichkeit, Integrität und Verfügbarkeit Ihrer Daten. Bildschirm- und Videofreigabe, VoIP, Webcam-Video, Tastatur-/Maussteuerung und textbasierte Chat-Informationen („Sitzungsdaten“) weisen Kommunikationssicherheitskontrollen nach Branchenstandard auf.

Sitzungsdaten werden bei der Übertragung zwischen Endpunkten und GoTo-Kommunikationsservern nie in Klartext offengelegt.

In zwei Schichten sind Kommunikationssicherheitskontrollen auf Basis starker Verschlüsselung implementiert: (i) auf dem TCP (Transmission Control Protocol) und UDP (User Datagram Protocol) und (ii) in der MPSL (Multicast Packet Security Layer).

TCP- und UDP-Sicherheit

Die TCP-Kommunikation zwischen Endpunkten wird durch TLS-Protokolle (Transport Layer Security) nach IETF-Standard (Internet Engineering Task Force) geschützt.

GoTo empfiehlt Kunden zu ihrer eigenen Sicherheit, ihre Browser so zu konfigurieren, dass sie nach Möglichkeit standardmäßig eine starke Verschlüsselung verwenden und sicherstellen, dass die Sicherheitspatches für ihr Betriebssystem und ihre Browser aktuell sind.

Beim Herstellen einer TLS-Verbindung zur Website sowie zwischen den GoTo Meeting-, GoTo Webinar- oder GoTo Training-Komponenten authentifizieren sich die GoTo-Server mit Hilfe von Public-Key-Zertifikaten bei den Clients. Als zusätzlicher Schutz vor Infrastrukturangriffen erfolgt eine gegenseitige zertifikatbasierte Authentifizierung bei allen Server-zu-Server-Verbindungen (z.B. Kommunikations-server zu Webkonferenz-Services).

Für mit UDP gesendete Daten wird eine vorhandene TLS-Verbindung genutzt, um kryptografische Schlüssel zum Verschlüsseln und Authentifizieren von UDP-Daten sicher auszutauschen.

Sicherheit der Multicast Packet Layer

Multicast-Daten wie Tastatur-/Maussteuerung, Chat und Statusinformationen in der Sitzung sind durch Verschlüsselung bei der Übertragung und Integritätsmechanismen geschützt, die jeden mit Zugriff auf die Kommunikationsserver – egal ob Freund oder Feind – daran hindern sollen, eine Sitzung abzuhören oder Daten unerkannt zu manipulieren. Die MPSL bietet speziell für GoTo-Produkte eine zusätzliche Ebene der Kommunikationsvertraulichkeit und -integrität. Diese zusätzliche Sicherheits-schicht verwendet AES-Verschlüsselung mit 128 Bit im Abwehrmodus für weiteren Schutz vor Abhörung und Manipulation.

Zur Optimierung der Bandbreite werden Klartextdaten in der Regel vor der Verschlüsselung mit proprietären, leistungsstarken Methoden komprimiert. Der Schutz der Datenintegrität wird durch eine ICV-Prüfsumme gewährleistet, die derzeit mit dem HMAC-SHA-1-Algorithmus generiert wird.

Die Schlüsselvereinbarung erfolgt mittels eines zufällig generierten 128-Bit-Startwerts („Seed"), der vom GoTo-Service ausgewählt und über TLS an alle Endpunkte verteilt wird. Er dient als Eingabe für eine vom NIST genehmigte Schlüsselableitungs-funktion. Bei Beendigung der Sitzung wird der Seed-Wert aus dem Arbeitsspeicher des Service gelöscht.

Audiosicherheit

GoTo Meeting, GoTo Webinar und GoTo Training unterstützen integrierte Audio-konferenzen sowohl über das herkömmliche Telefonnetz als auch über VoIP (Voice over Internet Protocol). Das herkömmliche Telefonnetz gewährleistet von vornherein die Vertraulichkeit und Integrität der Sprachkommunikation. Zum Schutz der Vertraulichkeit und Integrität der VoIP-Verbindungen zwischen Endpunkten und Sprachservern kommt sowohl über UDP als auch TCP ein SRTP-basiertes Protokoll mit AES-128-HMAC-SHA1 zum Einsatz. Client und Server tauschen die Schlüssel über die hergestellte TLS-Verbindung aus.

Videosicherheit

Zum Schutz der Vertraulichkeit und Integrität von Videoverbindungen zwischen Endpunkten und Videoservern nutzt GoTo ein SRTP-basiertes Protokoll mit AES-128-HMAC-SHA1. Client und Server tauschen die Schlüssel über die hergestellte TLS-Verbindung aus.

Webcast-Sicherheit

GoTo Webinar-Webcasts nutzen Kommunikationsserver, Broadcast-Gateways, Streaming Engines und Content Delivery Networks von Drittanbietern, um die Bildschirm-, Ton- und Videoübertragung für Teilnehmer, die über einen Browser beitreten, zu ermöglichen. Die Gateways empfangen Mediendaten von den Kommunikationsservern, transcodieren sie in Standard-Codecs und leiten sie an die Streaming Engine über RTP weiter – alles in unserem sicheren internen Netzwerk. Die Streaming Engine erzeugt HTTP Live Streaming (HLS) mit mehreren Bitraten, um eine adaptive Zustellung für Clients mit nicht ganz optimalen Netzwerkverbindungen zu ermöglichen. CDNs wurden eingerichtet, um Daten aus der Streaming Engine über HTTPS sicher abrufen. Die Clients rufen Daten auch sicher von CDNs über HTTPS ab.

GoTo Stage

GoTo Stage ist ein Online-Portal, in dem GoTo Webinar-Organisatoren anpassbare Kanäle erstellen und ihre aufgezeichneten Webinare veröffentlichen können. Veröffentlichte Aufzeichnungen werden von uns in einer Reihe geschäftlicher Kategorien auf der GoTo Stage-Homepage vorgestellt. Ein auf GoTo Stage veröffentlichtes Video ist über die GoTo Stage-Homepage und über Suchmaschinen auffindbar, sofern der Organisator die Auffindbarkeit nicht mit Hilfe der Administratoreinstellungen auf seiner Kanalseite eingeschränkt. Andernfalls können alle bei GoTo Stage registrierten Personen mit einem direkten Link zum Kanal oder zur individuellen „Watch Now"-Seite des Videos die Aufzeichnung ansehen. Besucher registrieren sich mit ihrem Namen und ihrer E-Mail-Adresse bei GoTo Stage oder stellen über Konten in sozialen Netzwerken wie LinkedIn, Facebook und Gmail eine Verbindung her. Nach der Registrierung erfolgt die Wiedergabe des aufgezeichneten Webinars über eine signierte S3-URL mit einer festgelegten TTL. Organisatoren können die Veröffentlichung ihrer Aufzeichnungen über GoTo Webinar jederzeit rückgängig machen, wodurch die Videos von ihrer Kanalseite und aus der GoTo Stage-Umgebung gelöscht werden. Zum Schutz der GoTo Stage-Administrationsfunktionen werden Passwörter verwendet, und alle Verbindungen im GoTo Stage-Portal sind mittels TLS geschützt.

3.7.2 Daten im Ruhezustand

In GoTo Meeting, GoTo Webinar und GoTo Training können Organisatoren ihre Live-Sitzungen einschließlich Audio-, Video- und Bildschirminhalten aufzeichnen. Sobald ein Organisator die Aufzeichnung startet, werden die Teilnehmer dazu benachrichtigt. Dass eine Aufzeichnung läuft, wird ihnen dann auf dem Bedienpanel angezeigt. Kunden können Sitzungsaufzeichnungen auf ihrem lokalen Rechner oder in der Cloud speichern.

Cloud-Aufzeichnungen

Cloud-Aufzeichnungen werden auf AWS S3 gespeichert. Dateien werden im Ruhezustand unter Verwendung von serverseitiger Verschlüsselung mit 256-Bit-AES gespeichert

Transkripte

Wenn vom Organisator aktiviert, wird Cloud Speech-to-Text-Technologie von Google verwendet, um Sitzungsaufzeichnungen zu transkribieren. Audiodateien werden mit TLS für die Transkription übertragen, wobei die Datei mit 256-Bit-AES verschlüsselt und direkt nach der Verarbeitung von Sprache zu Text gelöscht wird. Transkripts werden von GoTo mithilfe der AWS S3-Instanz aufbewahrt und dem Organisator bei den Cloud-Aufzeichnungen zur Verfügung gestellt.

Upload von Inhalten

Einige der GoTo-Services bieten Funktionen, mit denen Organisatoren Videos für den Einsatz in Live-Sitzungen hochladen können. Auch diese Uploads werden in AWS S3 gespeichert, wenn AES-Verschlüsselung (256 Bit) im Ruhezustand und bei der Übertragung aktiviert ist.

3.8 Schwachstellen-Management

Die internen und externen Systeme und Netzwerke werden monatlich auf Schwachstellen überprüft. Es werden auch regelmäßig Schwachstellenprüfungen dynamischer und statischer

Anwendungen vorgenommen und Penetrationstestaktivitäten für bestimmte Umgebungen ausgeführt. Für die Ergebnisse dieser Überprüfungen und Tests werden in Netzwerküberwachungstools Berichte erstellt, und wo dies basierend auf der Wichtigkeit der identifizierten Schwachstellen erforderlich ist, werden Abhilfemaßnahmen ergriffen.

Schwachstellen werden auch in monatlichen und vierteljährlichen Berichten kommuniziert und verwaltet, die den Entwicklungsteams sowie dem Management zur Verfügung gestellt werden.

3.9 Protokollierung und Warnmeldungen

GoTo erfasst identifizierten anomalen oder verdächtigen Datenverkehr in entsprechenden Sicherheitsprotokollen in den jeweiligen Produktionssystemen.

4 Organisatorische Kontrollen

GoTo bietet einen umfassenden Satz an organisatorischen und administrativen Kontrollen zum Schutz des Sicherheits- und Datenschutzstatus der UCC-Lösungen von GoTo.

4.1 Sicherheitsrichtlinien und -verfahren

GoTo pflegt umfangreiche Sicherheitsrichtlinien und -verfahren, die an Geschäftszielen, Compliance-Programmen und der allgemeinen Unternehmensführung ausgerichtet sind. Diese Richtlinien und Verfahren werden regelmäßig überprüft und bei Bedarf aktualisiert, um die Einhaltung von Vorschriften stets sicherzustellen.

4.2 Einhaltung der Standards

GoTo hält geltende rechtliche, finanzielle, datenschutzrechtliche und regulatorische Anforderungen ein und wahrt Compliance mit den folgenden Zertifizierungen und externen Audit-Berichten:

- TRUSTe Enterprise Privacy & Data Governance Practices Certification, um operative Datenschutz- und Data Protection-Kontrollen zu adressieren, die sich an den wichtigsten Datenschutzgesetzen und anerkannten Datenschutzabkommen orientieren. Weitere Informationen finden Sie in unserem Blog-Beitrag.
- Service Organization Control (SOC) 2 Type 2-Bericht des American Institute of Certified Public Accountants (AICPA)
- Service Organization Control (SOC) 3 Type II-Bericht des American Institute of Certified Public Accountants (AICPA)
- Einhaltung des Payment Card Industry Data Security Standard (PCI DSS) bei den E-Commerce- und Zahlungsumgebungen von GoTo
- Interne Kontrollenbewertung wie im Rahmen der Jahresrechnungsprüfung durch das Public Company Accounting Oversight Board (PCAOB)

4.3 Security Operations und Incident-Management

Das Security Operations Center (SOC) von GoTo ist mit dem Security Operations-Team besetzt und ist für das Erkennen von und Reagieren auf Sicherheitsereignisse verantwortlich. Das SOC verwendet Sicherheitssensoren und Analysesysteme, um mögliche Probleme zu

identifizieren und hat einen Vorfallsreaktionsplan entwickelt, der die entsprechenden Reaktionen vorgibt.

Der Vorfallsreaktionsplan ist auf die wichtigen GoTo-Kommunikationsprozesse, die Incident-Management-Richtlinie für Informationssicherheit sowie standardmäßige Betriebsvorgänge ausgerichtet. Diese Richtlinien und Verfahren wurden entwickelt, um vermutete oder identifizierte Sicherheitsereignisse in den Systemen und Services von GoTo, einschließlich der UCC-Lösungen von GoTo zu verwalten, zu identifizieren und zu beheben. Laut Vorfallsreaktionsplan gibt es Techniker, die Ereignisse und Schwachstellen hinsichtlich der Sicherheit von Informationen identifizieren und alle vermuteten oder bestätigten Ereignisse gegebenenfalls an das Management eskalieren. Mitarbeiter können Sicherheitsvorfälle gemäß des auf der Intranet-Seite von GoTo dokumentierten Prozesses per E-Mail, Telefon und/oder Ticket melden. Alle identifizierten oder vermuteten Ereignisse werden über standardisierte Ereignistickets dokumentiert, eskaliert und je nach Wichtigkeit selektiert.

4.4 Anwendungssicherheit

Das Anwendungssicherheitsprogramm von GoTo basiert auf dem Microsoft Security Development Lifecycle (SDL) für einen sicheren Produktcode. Zu den Hauptelementen dieses Programms gehören manuelle Codeüberprüfungen, Bedrohungsmodellierung, statische Codeanalysen, dynamische Analysen und Systemhärtung.

4.5 Personalsicherheit

Überprüfungen der Mitarbeiter – soweit dies nach geltendem Recht zulässig und für die Position angemessen ist – werden weltweit bei neuen Mitarbeitern vor dem Datum ihrer Einstellung vorgenommen. Die Ergebnisse werden im Personalstammblatt des Mitarbeiters hinterlegt. Die Kriterien der Mitarbeiterüberprüfung variieren in Abhängigkeit der Gesetze, der Arbeitsverantwortung und dem Führungsniveau des potenziellen Mitarbeiters und unterliegen den üblichen und zulässigen Praktiken des jeweiligen Lands.

4.6 Sicherheitsbewusstsein und Schulungsprogramme

Neu eingestellte Mitarbeiter werden zur Orientierung über die Sicherheitsrichtlinien und den Verhaltenskodex und Geschäftsethik von GoTo informiert. Diese obligatorische jährliche Schulung zu Sicherheit und Datenschutz wird für die entsprechenden Mitarbeiter durch das Talentförderungsteam und mit Unterstützung des Sicherheitsteams durchgeführt.

Die Mitarbeiter und Zeitarbeiter von GoTo werden regelmäßig über die Anweisungen, Verfahren, Richtlinien und Standards zu Sicherheit und Datenschutz informiert. Dazu werden verschiedene Medien wie Einarbeitungsunterlagen für Neueingestellte, Aufklärungs-kampagnen, Webinare mit dem CISO, ein Sicherheits-Champion-Programm und der Aushang von Plakaten oder anderes Begleitmaterial genutzt, die mindestens halbjährlich ausgetauscht werden und Methoden zum Schutz von Daten, Geräten und Anlagen veranschaulichen.

5 Datenschutzpraktiken

GoTo nimmt den Schutz der Daten seiner Kunden, Abonnenten der UCC-Lösungen von GoTo und Endbenutzer sehr ernst und verpflichtet sich, entsprechende Praktiken zur Verarbeitung und Verwaltung von Daten offen und transparent preiszugeben.

5.1 DSGVO

Die Datenschutz-Grundverordnung (DSGVO) ist eine Verordnung der Europäischen Union (EU), die sich mit dem Schutz der Daten und der Privatsphäre von Einzelpersonen in der Europäischen Union befasst. Sie zielt primär darauf ab, ihren Bürgern und Bewohnern Kontrolle über ihre personenbezogenen Daten zu geben und die regulative Umgebung in der EU zu vereinfachen. Die UCC-Lösungen von GoTo sind mit den anwendbaren DSGVO-Bestimmungen kompatibel. Weitere Informationen finden Sie unter https://www.goto.com/company/trust/privacy.

5.2 CCPA

GoTo sichert hiermit zu, dass es mit dem California Consumer Privacy Act (CCPA) konform ist. Weitere Informationen finden Sie unter https://www.goto.com/company/trust/privacy.

5.3 Data Protection- und Datenschutzerklärung

GoTo freut sich, einen umfassenden, globalen Datenverarbeitungsnachtrag (DVN) in Englisch und Deutsch bereitzustellen. Es regelt die Verarbeitung personenbezogener Daten durch GoTo, um die Anforderungen von DSGVO, CCPA und mehr zu erfüllen.

Der DVN schließt folgende Datenschutz-Anforderungen in Bezug auf die DSGVO ein: (a) Details zur Datenverarbeitung, Offenlegung bzgl. Auftragsverarbeiter-Partnerunternehmen etc. gemäß Artikel 28 (b) EU-Standardvertragsklauseln (auch als EU-Modellklauseln bekannt) und (c) die technischen und organisatorischen Maßnahmen von GoTo. Im Zusammenhang mit dem Inkrafttreten des CCPA haben wir zusätzlich in unserem globalen DVN Folgendes aktualisiert: (a) Definitionen im Zusammenhang mit dem CCPA (b) Zugriffs- und Löschrechte und (c) Garantien, dass GoTo keine persönlichen Daten von Benutzern verkaufen wird.

Für Besucher unserer Webseiten veröffentlicht GoTo die Arten von Informationen, die es sammelt und verwendet, um seine Services bereitzustellen, aufrechtzuerhalten, zu verbessern und zu sichern, in seiner Datenschutzerklärung auf der öffentlichen Website. Das Unternehmen kann seine Datenschutzrichtlinie von Zeit zu Zeit aktualisieren, um Änderungen an seinen Informationspraktiken und/oder Änderungen geltender Gesetze zu berücksichtigen, weist aber auf seiner Website auf jegliche Materialänderungen hin, bevor diese wirksam werden.

5.4 Abkommen zur Datenübertragung

GoTo hat ein robustes globales Data Protection-Programm, das das geltende Recht berücksichtigt und rechtmäßige internationale Datenübertragungen im Rahmen der folgenden Abkommen unterstützt:

5.4.1 Standardvertragsklauseln

Die Standardvertragsklauseln („SCC") sind standardisierte Vertragsbestandteile, die von der Europäischen Kommission anerkannt und übernommen wurden und vorrangig dem Zweck dienen, eine EU-datenschutzkonforme Übermittlung personenbezogener Daten in Regionen außerhalb des Europäischen Wirtschaftsraums („EWR") sicherzustellen. GoTo hat ein ausgefeiltes Datenschutzprogramm eingerichtet, das die Ausführungsbestimmungen der SCC für die Übermittlung personenbezogener Daten einhält. GoTo bietet Kunden SCC (andere Bezeichnung: EU-Modellklauseln) an. Diese leisten als Bestandteil des globalen DVN von spezifische Garantien betreffend

die Übermittlung personenbezogener Daten für die zum Leistungsumfang gehörigen GoTo-Services im Rahmen des globalen DVN. Der Abschluss der SCC hilft, die freie Übermittlung der Daten von GoTo-Kunden aus dem EWR in andere Weltregionen sicherzustellen.

Ergänzende Maßnahmen

Neben den in diesen TOMs angegebenen Maßnahmen hat GoTo die folgenden FAQ erstellt, um seine ergänzenden Maßnahmen zur Unterstützung rechtmäßiger Datenübertragungen gemäß Kapitel 5 der DSGVO zu skizzieren und alle Analysen zu adressieren und anzuleiten, die vom Europäischen Gerichtshof zusammen mit den SCCs empfohlen werden.

5.4.2 Zertifizierungen zu APEC, CBPR und PRP

GoTo hat zudem die Zertifizierungen zu APEC (Asiatisch-Pazifische Wirtschaftsgemeinschaft), CBPR (Grenzüberschreitende Datenschutzregulierung) und PRP (Datenschutzanerkennung für Datenverarbeiter) erworben. Die APEC-, CBPR- und PRP-Rahmenregelungen sind die ersten Datenregelungen, die für die Übermittlung personenbezogener Daten zwischen APEC-Mitgliedsländern genehmigt wurden. Sie wurden von TrustArc, einem von der APEC anerkannten führenden Drittanbieter für die Einhaltung von Datenschutzbestimmungen, eingeholt und unabhängig validiert.

5.5 Rückgabe und Löschung von Kundeninhalt

Kunden der UCC-Lösungen von GoTo können jederzeit die Rückgabe oder Löschung ihres Inhalts anfordern. Derartige Anfragen werden innerhalb von dreißig (30) Tagen der Anfrage ausgeführt (oder früher, wo durch geltendes Recht erforderlich). Zudem werden GoTo Meeting-Meetingchronik und Cloud-Aufzeichnungen automatisch auf rollierender 1-Jahres-Basis während eines aktiven Abonnementzeitraums des Kunden gelöscht.

Nach Ende eines zahlungspflichtigen Abonnements für GoTo Meeting werden die Konten des Kunden in ein kostenloses Konto umgewandelt. Wenn ein Konto explizit gekündigt oder aufgelöst wird, wird der Inhalt innerhalb von 90 Tagen der Kündigung oder Auflösung gelöscht. Kostenlose GoTo Meeting-Konten unterliegen der rollierenden 1-Jahres-Löschung, die oben beschrieben ist. Kostenlose GoTo Meeting-Konten werden zudem nach zwei (2) Jahren Inaktivität des Benutzers (z. B. keine Anmeldungen) automatisch gelöscht.

Zur Berücksichtigung eines saisonalen Benutzerstamms werden GoTo Webinar- und GoTo Training-Konten zwei (2) Jahre nach Ablauf oder Beendigung der jeweiligen Endlaufzeit gelöscht. GoTo Stage-Benutzer können ihre veröffentlichten Webinare während eines aktiven GoTo Webinar-Abonnements jederzeit per Self-Service über die GoTo Webinar-Service-Umgebung und/oder durch Einreichen einer Supportanfrage bei GoTo entfernen oder die Veröffentlichung rückgängig machen. Auf schriftliche Anfrage bestätigt GoTo die Löschung des betreffenden Kontos und des Inhalts.

5.6 Sensible Daten

Es ist das Ziel von GoTo, den gesamten Kundeninhalt zu schützen, und regulatorische und vertragliche Beschränkungen verlangen, dass die Verwendung von GoTo Meeting, GoTo Webinar, GoTo Training und GoTo Stage für bestimmte Arten von Informationen eingeschränkt wird. Sofern der Kunde keine schriftliche Genehmigung von GoTo hat, dürfen die

folgenden Daten nicht in GoTo Meeting, GoTo Webinar, GoTo Training und GoTo Stage hochgeladen oder dort generiert werden:

- Staatlich vergebene Identifikationsnummern und Bilder von Ausweisdokumenten.
- Informationen über die Gesundheit einer Person, einschließlich, aber nicht beschränkt auf, persönliche Gesundheitsinformationen, die im US-amerikanischen Health Insurance Portability and Accountability Act (HIPAA) und damit verbundenen Gesetzen und Vorschriften festgelegt sind.
- Informationen über Finanzkonten und Zahlungsinstrumente, einschließlich – aber nicht beschränkt auf – Kreditkartendaten. Die einzige allgemeine Ausnahme von dieser Bestimmung betrifft ausdrücklich gekennzeichnete Zahlungsformulare und Seiten, die von GoTo verwendet werden, um Zahlungen für GoTo Meeting, GoTo Training, GoTo Webinar und GoTo Stage zu erheben.
- Alle Informationen, die besonders durch geltende Gesetze und Vorschriften geschützt sind, insbesondere Informationen über die Rasse, die ethnische Zugehörigkeit, religiöse oder politische Überzeugungen, organisatorische Mitgliedschaften der Person usw.

5.7 Nachverfolgung und Analysen

GoTo verbessert kontinuierlich seine Websites und Produkte mit Hilfe von Webanalysetools von Drittanbietern, um Folgendes besser zu verstehen: Nutzung der Websites, Desktop-Tools und mobilen Anwendungen durch Besucher, Benutzerpräferenzen und Probleme. Weitere Einzelheiten finden Sie in der Datenschutzrichtlinie.

6 Drittanbieter

6.1 Nutzung von Drittanbietern

Im Rahmen der internen Bewertung und der Prozesse im Zusammenhang mit Anbietern und Dritten können Anbieterbewertungen je nach Relevanz und Anwendbarkeit von mehreren Teams vorgenommen werden. Das Sicherheitsteam bewertet Anbieter von Services, die auf Informationssicherheit basieren, und nimmt auch die Bewertung der Hosting-Einrichtungen von Drittanbietern vor. Die Teams für Recht und Beschaffung können bei Bedarf nach internen Prozessen Verträge, Leistungsbeschreibungen und Servicevereinbarungen bewerten.

Angemessene Konformitätsdokumente oder -berichte können mindestens einmal jährlich eingeholt und bewertet werden, sofern dies für angemessen erachtet wird, um sicherzustellen, dass die Kontrollumgebung ordnungsgemäß funktioniert und alle erforderlichen benutzerbezogenen Kontrollen durchgeführt werden. Zudem müssen Drittanbieter, die sensible oder vertrauliche Daten hosten oder von GoTo Zugriff darauf erhalten haben, einen schriftlichen Vertrag zu unterzeichnen, in dem die relevanten Anforderungen für den Zugriff auf die Informationen sowie deren Speicherung oder Verarbeitung (sofern zutreffend) festgelegt sind.

6.2 Vertragspraktiken

Um die Geschäftskontinuität zu gewährleisten und sicherzustellen, dass geeignete Maßnahmen zum Schutz der Vertraulichkeit und Integrität von Geschäftsprozessen und

Datenverarbeitung durch Drittanbieter getroffen werden, überprüft GoTo die jeweiligen Nutzungsbedingungen von Drittanbietern und nutzt entweder von GoTo genehmigte Beschaffungsvorlagen oder verhandelt die Bedingungen dieser Drittanbieter, wenn dies als notwendig erachtet wird.

7 GoTo kontaktieren

Kunden können sich bei allgemeinen Anfragen an https://support.goto.com oder bei Fragen zum Datenschutz an privacy@goto.com wenden.

ANLAGE 7

Unterauftragsverarbeiter des Auftragnehmers

Bitte das Zutreffende ankreuzen:

☐ Es werden keine Unterauftragsverarbeiter eingesetzt.

Eingesetzte Unterauftragsverarbeiter des Auftragnehmers

Name und Adresse Unterauftragsverarbeiter 1	Durchzuführende Tätigkeit(en)
Name: Hetzner Online-AG Stuttgarter Straße 1 91710 Gunzenhausen	Bestandteil Backupstrategie des Form-Solutions Formularservers
Name und Adresse von Unterauftragsverarbeiter 2	**Durchzuführende Tätigkeit(en)**
Name: T-Systems International GMBH Heinrich Hertz Straße 1 64295 Darmstadt	Hosting des Formularservers (nur relevant für Kunden, die das Antragsmanagement auf pdf.form-solutions.net nutzen)
Name und Adresse von Unterauftragsverarbeiter 3	**Durchzuführende Tätigkeit(en)**
Name: 1&1 IONOS SE Elgendorfer Str. 57 56410 Montabaur	Mailserver-Provider

Name und Adresse von Unterauftragsverarbeiter 4	Durchzuführende Tätigkeit(en)
Name: TeamViewer GmbH Jahnstraße 30 73037 Göppingen	Von Form-Solutions eingesetzte Software für den Support und für die Fernwartung.
Name und Adresse von Unterauftragsverarbeiter 5	**Durchzuführende Tätigkeit(en)**
Name: LogMeIn Ireland Limited Bloodstone Building Block C 70 Sir John Rogerson's Quay Dublin 2, Ireland	Lieferant von GoToMeeting®; wird zum Abhalten von Web-Schulungen und Online-Trainings eingesetzt.

Die Zustimmung zum Einsatz des/der oben genannten Unterauftragsverarbeiters/ Unterauftragsverarbeiter für die genannten durchzuführenden Tätigkeiten wird erteilt, sofern die datenschutzrechtlichen Voraussetzungen entsprechend dieser Vereinbarung auch in diesem Vertragsverhältnis (Unterauftragsverarbeiter-ADV) eingehalten werden.