Vertrag zur Auftragsverarbeitung nach Art. 28 DSGVO

zwischen

(nachfolgend Auftraggeber genannt)

und

Time iX
Poststraße 6
95138 Bad Steben

(nachfolgend Auftragnehmer genannt)

Inhalt:

1. Vorbemerkung

(1) Der Auftraggeber steht nach außen, also gegenüber Dritten und den Betroffenen für die Rechtmäßigkeit der auftragsgemäßen Erhebung und Verwendung der Auftraggeber-Daten ein. Er ist nach außen auch für die Wahrung der Rechte der Betroffenen verantwortlich

(2) Im Rahmen der Tätigkeiten und/oder Leistungen, welcher der Auftragnehmer für den Auftraggeber erbringt kann nicht ausgeschlossen werden, dass er unter anderem auch Zugriff auf personenbezogene Daten erhält. Ist dies der Fall, verarbeitet der Auftragnehmer personenbezogene Daten des Auftraggebers in dessen Auftrag.

(3) Der Auftraggeber hat den Auftragnehmer im Rahmen der Sorgfaltspflichten des Art. 28 Abs.1 DSGVO als Dienstleister ausgewählt. Voraussetzung für die Zulässigkeit einer Datenverarbeitung im Auftrag ist, dass der Auftraggeber dem Auftragnehmer den Auftrag schriftlich erteilt. Dieser Vertrag enthält nach dem Willen der beiden Parteien und insbesondere des Auftraggebers den schriftlichen Auftrag zur Auftragsverarbeitung i. S. d. Art. 28 DSGVO und regelt die Rechte und Pflichten der Parteien im Zusammenhang mit der Datenverarbeitung.

(4) Sofern in diesem Vertrag der Begriff „Datenverarbeitung“ oder „Verarbeitung“ (von Daten) benutzt wird, wird damit allgemein die Verwendung von personenbezogenen Daten verstanden. Sofern in diesem Vertrag der Begriff „Auftraggeber-Daten“ benutzt wird, werden damit personenbezogene Daten im Sinne des DSGVO bezeichnet. Eine Verwendung personenbezogener Daten umfasst insbesondere die Erhebung, Speicherung, Übermittlung, Sperrung, Löschung, Anonymisierung, Pseudonymisierung, Verschlüsselung oder sonstige Nutzung von Daten.

2. Gegenstand, Dauer und Zweck des Vertrags

2.1 Gegenstand des Auftrags

nähere Beschreibung des Auftragsgegenstandes bzw. der Tätigkeiten und/oder Leistungen:

- Softwareupdates im Rahmen der „Allgemeine Bedingungen der Softwarepflege und Hotline“, (in der Folge „Hauptvertrag“)
- Wartungs- und Servicearbeiten auf den IT-Systemen des Auftraggebers für die im aktuellen Wartungsvertrag gelisteten Softwareprodukte.
- Wartungs- und Servicearbeiten im IT-Infrastrukturbereich im Rahmen des „IT-Wartungsvertrages“
- Serviceleistungen nach Anforderung
- Datenbankauslagerung zur Nutzung der Webservices

Die Grundlage für die Verarbeitung von Daten im Auftrag bildet unter anderem auch der Hauptvertrag. Innerhalb dieses Hauptvertrags erfolgt die Regelung zu Art und Umfang der Leistungserbringung zum Softwareupdate.

„***Vertragsbezeichnung“***: „Allgemeine Bedingungen der Softwarepflege und Hotline“ incl. Wartungsschein und IT Wartungsvertrag sofern abgeschlossen

Vertragsnummer: -- ohne --

Vertragsdatum: -- in der beim Auftraggeber vorliegenden gültigen Fassung --

(in der Folge „***Hauptvertrag***“ genannt)

Sofern kein oben genannter Software-Pflegevertrag abgeschlossen ist gelten die Bestimmungen dieses Vertrages.

Bei der Verarbeitung von Daten, ist der Auftragnehmer an die Weisungen des Auftraggebers gebunden.

Dieser Vertrag konkretisiert die datenschutzrechtlichen Rechte und Pflichten der Parteien im Zusammenhang mit dem Umgang von personenbezogenen Daten des Auftraggebers (in der Folge „**Auftraggeber-Daten**“ genannt).

2.2 Die Dauer dieses Auftrages

(Zutreffendes bitte entsprechend markieren)

☐ Die Dauer dieses Auftrages (Laufzeit) entspricht der Laufzeit des Hauptvertrags

☒ Der Auftrag ist unbefristet erteilt und kann vom Auftraggeber und Auftragnehmer mit einer Frist von 3 Monaten zum Jahresende gekündigt werden.

Die Möglichkeit zur fristlosen Kündigung bleibt davon unberührt.

Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen die anzuwendenden Datenschutzvorschriften oder gegen Pflichten aus diesem Vertrag vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht

ausführen kann oder will oder der Auftragnehmer den Zutritt des Auftraggebers oder der zuständigen Aufsichtsbehörde vertragswidrig verweigert.

2.3 Art, Umfang und Zweck der Auftragsverarbeitung

(1) Der Auftragnehmer erhebt, verarbeitet und nutzt die Daten des Auftraggebers ausschließlich im Auftrag und nach Weisung des Auftraggebers i. S. d. Art. 28 DSGVO (Auftragsverarbeitung). Der Auftraggeber bleibt im datenschutzrechtlichen Sinn verantwortliche Stelle („Herr der Daten“).

(2) 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 Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Artt. 44 ff. DSGVO erfüllt sind. Die Feststellung und Dokumentation der Angemessenheit des Schutzniveaus erfolgt in Anlage1

(3) Der Auftragnehmer darf die Auftraggeber-Daten ausschließlich in der Art, in dem Umfang und zu den Zwecken erheben und verwenden, die abschließend in Anlage 1 (*„Art Umfang und Zweck, der Datenverarbeitung“ – „Zweck der Datenverarbeitung*“) zu diesem Vertrag festgelegt sind. Die Erhebung und Verwendung der Auftraggeber-Daten durch den Auftragnehmer betrifft ausschließlich die in Anlage 1 (*„Art Umfang und Zweck, der Datenverarbeitung*“) zu diesem Vertrag abschließend festgelegten Datenarten und den dort bestimmten Kreis der Betroffenen. Jede davon abweichende oder darüberhinausgehende Erhebung oder Verwendung von Auftraggeber-Daten ist dem Auftragnehmer untersagt, insbesondere eine Verwendung der Auftraggeber-Daten zu eigenen Zwecken.

(4) Sofern der Auftragnehmer Auftraggeber-Daten außerhalb seiner Hauptniederlassung verarbeitet (z. B.: „Telearbeit“), bedarf es der schriftlichen Zustimmung des Auftraggebers. Die Art der Daten-verarbeitung sowie die Orte, an welchen diese Art der Datenverarbeitung erfolgt wird abschließend in Anlage 1 (*„Art Umfang und Zweck, der Datenverarbeitung*“ -- „Telearbeit“) aufgeführt.

(4) Datenverarbeitung in Homeoffices und/oder mittels mobiler Arbeitsgeräte („Telearbeit“) ist nur in Ausnahmefällen gestattet und bedarf der schriftlichen Zustimmung des Auftraggebers. Art und Umfang der Datenverarbeitung in Homeoffices und/oder mit mobilen Arbeitsgeräten ist in Anlage 1 „Telearbeit“ detailliert zu beschreiben.
(5) Der Auftragnehmer kann bei Bedarf den Auftraggeber bei den in Artt. 34-36 DSGVO genannten Pflichten unterstützen.
(6) Die Regeln zur Haftung und zum Recht auf Schadenersatz gemäß Artt. 82 DSGVO bleiben von ggf. vereinbarten vertraglichen Regeln zur Haftung unberührt.

3. Technisch-organisatorische Maßnahmen

(1) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

Insgesamt handelt es sich bei den zu treffenden Maßnahmen um nicht auftragsspezifische Maßnahmen hinsichtlich

- der Organisationskontrolle,
- Zutrittskontrolle,
- Zugangskontrolle,
- Zugriffskontrolle,

- Weitergabekontrolle,
- Auftragskontrolle,
- Verfügbarkeitskontrolle
- Trennungsgebots

(2) Die vom Auftragnehmer getroffenen Maßnahmen sind in Anlage 3 („**t**echnische und **o**rganisatorische **M**aßnahmen – **TOM**“) zu dokumentieren.

(3) Ebenso sind besondere Maßnahmen zum Schutze der Daten, mit Hinblick auf

- die Art des Datenaustauschs
- der Bereitstellung von Daten, Art / Umstände
- der Verarbeitung / der Datenhaltung sowie
- die Art / Umstände beim Datenversand,

in Anlage 3 zu dokumentieren, – soweit sie sich dies nicht bereits aus dem zugrundeliegenden Hauptvertrag ergibt.

(4) Der Auftragnehmer hat die Sicherheit gem. Artt. 28 Abs. 3 lit. c, 32 DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO 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 DSGVO zu berücksichtigen [Einzelheiten in Anlage 1].

(5) 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. Wesentliche Änderungen sind zu dokumentieren.

4. Berichtigung, Sperrung und Löschung von Daten

(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) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

(1) Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Artt. 28 bis 33 DSGVO

5.1 Pflicht zur Bestellung eines Datenschutzbeauftragten

(1) Der Auftragnehmer hat, soweit gesetzlich vorgeschrieben, eine(n) Datenschutzbeauftragte(n) bestellt. Diese(r), kann seine Tätigkeit gemäß Artt. 38 und 39 DSGVO) ausüben. Dessen Kontaktdaten werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme in Anlage 2 („Art Umfang und Zweck, der Datenverarbeitung“ – „Datenschutzbeauftragter“) mitgeteilt.

5.2 Pflicht zur Wahrung der Vertraulichkeit

(1) Der Auftragnehmer setzt, Gemäß Artt. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO, 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. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind. Auftraggeber und Auftragnehmer sind verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Betriebs-, Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Vertragspartners vertraulich zu behandeln.

5.3 Umsetzung und Nachweisbarkeit zur Einhaltung der TOM gem. Art. 32 DSGVO

(1) Der Auftragnehmer hat die Pflicht zur Umsetzung und Einhaltung aller für diesen Auftrag notwendigen technischen und organisatorischen Maßnahmen entsprechend Art. 32 DSGVO.

(2) Zudem hat der Auftragnehmer die Pflicht zur Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber. Hierzu kann der Auftragnehmer auch aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, interner/externer Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) oder eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz, ISO 27001, vds 3474 oder ähnliche) vorlegen.

5.4 Die Durchführung der Auftragskontrolle

(1) Der Auftraggeber hat die Pflicht zur Durchführung der Auftragskontrolle. Dies erfolgt mittels regelmäßiger Prüfungen durch den Auftraggeber, im Hinblick auf die Vertragsausführung bzw. -erfüllung, insbesondere auf Einhaltung und ggf. notwendige Anpassung von Regelungen und Maßnahmen zur Durchführung des Auftrags. Der Auftragnehmer ist verpflichtet diese Kontrollen in angemessener Weise zu unterstützen.

(2) Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

5.5 Zweckbindung

(1) Der Auftragnehmer hat die Pflicht, die Daten für keine anderen als in diesem Vertrag vereinbarten Zwecke zu verwenden und ist insbesondere nicht berechtigt, sie an Dritte weiterzugeben. Kopien und Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(2) Der Auftragnehmer darf Auftraggeber-Daten ohne vorherige schriftliche Zustimmung durch den Auftraggeber nicht an Dritte oder andere Empfänger aushändigen. Hiervon ausgenommen sind Datenweitergaben an Unterauftragnehmer, deren Beauftragung der Auftraggeber gemäß Ziffer 6 zugestimmt hat

5.6 Selbstkontrolle

(1) Der Auftragnehmer hat die Pflicht zur regelmäßigen Selbstkontrolle seiner internen Prozesse, so dass die Verarbeitung der Auftraggeber-Daten in Übereinstimmung mit diesem Vertrag und den Weisungen des

Auftraggebers erfolgt und die technisch-organisatorischen Maßnahmen gemäß Ziffer 3 dieses Vertrags eingehalten werden.

Der Auftragnehmer ist verpflichtet, die Selbstkontrollen schriftlich in Form von Prüfprotokollen zu dokumentieren und dem Auftraggeber die Prüfprotokolle auf Verlangen unverzüglich vorzulegen.

5.7 Mitwirkungspflicht

(1) Ist der Auftraggeber gegenüber einer staatlichen Stelle, einem Betroffenen oder einer anderen Person verpflichtet, Auskünfte über die Auftraggeber-Daten oder deren Erhebung oder Verwendung zu erteilen, so ist der Auftragnehmer verpflichtet, den Auftraggeber bei der Erteilung solcher Auskünfte auf erstes Anfordern zu unterstützen, insbesondere durch unverzügliches Zurverfügungstellen sämtlicher Informationen und Dokumente über die vertragsgegenständliche Verarbeitung von Auftraggeber-Daten.

5.8 Benennung der zum Empfang von Weisungen berechtigten Personen /-gruppen

(1) Der Auftragnehmer kann dem Auftraggeber die Person(en) benennen, die zum Empfang von Weisungen des Auftraggebers berechtigt sind.

Zum Empfang von Weisungen berechtigte Person(en) / Personengruppen des Auftragnehmers ist (sind):

☒ Die Liste der zum Empfang berechtigten Personen / Personengruppen befindet sich in Anlage 1

(2) In dringenden Fällen darf der Auftraggeber aber auch jedem anderen Beschäftigten des Auftragnehmers entsprechende Weisungen erteilen, sofern weder der Empfangsberechtigte noch sein Stellvertreter für den Auftraggeber erreichbar waren.

(3) Ein Wechsel in dem Personenkreis der Empfangsberechtigten oder bei dauerhafter Verhinderung hat der Auftragnehmer dem Auftraggeber dies möglichst frühzeitig, schriftlich und unter Benennung eines Vertreters mitzuteilen. Bis zum Zugang einer solchen Mitteilung beim Auftraggeber gelten die benannten Personen weiter als empfangsberechtigt für Weisungen des Auftraggebers.

(4) Der Auftragnehmer ist verpflichtet, die Weisungen des Auftraggebers unverzüglich auszuführen. Der Auftraggeber ist berechtigt, dem Auftragnehmer hierfür im Einzelfall eine jeweils angemessene Frist zu setzen, die der Auftragnehmer einzuhalten hat.

(5) Ist der Auftragnehmer der begründeten Ansicht, dass eine Weisung des Auftraggebers gegen diesen Vertrag oder das geltende Datenschutzrecht verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen.

(6) Der Auftragnehmer muss den Auftraggeber bei Ausnahmen von der Weisungspflicht bei Datenverarbeitungen aufgrund von Rechtsvorschriften unterrichten, wenn nicht die Rechtsvorschrift eine solche Mitteilung verbietet.

6. Unterauftragsverhältnisse

(1) 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, Wartung und Benutzerservice 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.

(2) Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.

Die Unterauftragsverhältnisse werden in Anlage 2 („Liste der Unterauftragsverhältnisse“) gelistet.

7. Kontrollrechte des Auftraggebers

1) Der Auftraggeber hat das Recht, im Einvernehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DSGVO 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.

(3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch

- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO;
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO;
- 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).

(4) Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

8. Mitteilung bei Verstößen des Auftragnehmers

(1) Wenn eine Person gegen Vorschriften zum Schutz personenbezogener Daten, gegen Festlegungen nach diesem Vertrag oder gegen eine vom Auftraggeber erteilte Weisung verstoßen hat, wenn Anhaltspunkte dafür bestehen, dass ein Dritter – egal aus welchem Grund – unrechtmäßig Kenntnis von Auftraggeber-Daten erlangt haben könnte, oder wenn in sonstiger Weise eine Gefährdung für die Integrität oder Vertraulichkeit der Auftraggeber-Daten eingetreten ist („Datensicherheitsvorfall“)

(2) Es ist bekannt, dass nach Art. 33 DSGVO Informationspflichten im Falle des Abhandenkommens oder der unrechtmäßigen Übermittlung oder Kenntniserlangung von personenbezogenen Daten bestehen können. Deshalb sind solche Vorfälle ohne Ansehen der Verursachung innerhalb von 24 Stunden nach Kenntnisnahme dem Auftraggeber mitzuteilen. Dies gilt auch bei schwerwiegenden Störungen des Betriebsablaufs, bei Verdacht auf sonstige Verletzungen gegen Vorschriften zum Schutz personenbezogener Daten oder anderen Unregelmäßigkeiten beim Umgang mit personenbezogenen Daten des Auftraggebers. Der Auftragnehmer hat im Einvernehmen mit dem Auftraggeber angemessene Maßnahmen zur Sicherung der Daten sowie zur Minderung möglicher nachteiliger Folgen für Betroffene zu ergreifen. Soweit den Auftraggeber Pflichten nach Art. 33 DSGVO treffen, hat der Auftragnehmer ihn hierbei zu unterstützen.

9. Weisungsbefugnis des Auftraggebers

(1) Der Umgang mit den Daten erfolgt ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisung des Auftraggebers (vgl. Art. 28 DSGVO). Der Auftraggeber behält sich im Rahmen der in dieser Vereinbarung getroffenen Auftragsbeschreibung ein umfassendes Weisungsrecht über Art, Umfang und Verfahren der Datenverarbeitung vor, dass er durch Einzelweisungen konkretisieren kann.

(2) Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam abzustimmen und zu dokumentieren. Auskünfte an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger schriftlicher Zustimmung durch den Auftraggeber erteilen.

(3) Mündliche Weisungen wird der Auftraggeber unverzüglich schriftlich oder per E-Mail (in Textform) bestätigen.

(4) Weisungen sollen im Regelfall von dem Weisungsberechtigten des Auftraggebers oder dessen Stellvertreter erteilt werden.

Zur Erteilung von Weisungen berechtigte Personen / Personengruppen sind:

☒ Die Liste der zur Erteilung von Weisungen befugten Personen des Auftraggebers befindet sich in Anlage 1

(5) Der Auftragnehmer hat den Auftraggeber unverzüglich entsprechend Art. 28 DSGVO zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen datenschutzrechtliche Vorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird.

10. Löschung und Rückgabe von Daten

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, Daten welche sich innerhalb von Archivierungs-/Langzeitarchivierungssystem und in Datensicherungssystemen befinden und zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(2) 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.

(3) Ist eine Aushändigung der Daten, systembedingt nicht oder nur mit unangemessenem Aufwand verbunden kann an die Stelle der Aushändigung auch eine sichere, datenschutzkonforme Löschung / Vernichtung treten.

(4) Das Protokoll der Löschung / Vernichtung ist auf Anforderung vorzulegen.

(5) 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

11. Schlussbestimmungen

(1) Sollte das Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu informieren. Der Auftragnehmer wird die Gläubiger über die Tatsache, dass es sich um Daten handelt, die im Auftrag verarbeitet werden, unverzüglich informieren.

(2) Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

(3) Änderungen, Ergänzungen und die Aufhebung dieses Vertrags bedürfen der Schriftform. Gleiches gilt für eine Änderung oder Aufhebung des Schriftformerfordernisses.

(4) Sollten einzelne Bestimmungen dieses Vertrags unwirksam sein oder werden oder eine Lücke enthalten, so bleiben die übrigen Bestimmungen hiervon unberührt. Die Parteien verpflichten sich, anstelle der unwirksamen Regelung eine solche gesetzlich zulässige Regelung zu treffen, die dem Zweck der unwirksamen Regelung am nächsten kommt und den Anforderungen des Art. 28 DSGVO am besten gerecht wird.

(5) Im Fall von Widersprüchen zwischen diesem Vertrag und sonstigen Vereinbarungen zwischen den Parteien, insbesondere dem Hauptvertrag, gehen die Regelungen dieses Vertrags vor.

Ort, Datum	Ort, Datum
Auftraggeber (rechtsverbindliche Unterschrift)	Auftragnehmer (rechtsverbindliche Unterschrift)
Firmenstempel	Firmenstempel

Anlage 1 Art, Umfang und Zweck, der Datenverarbeitung

(Hinweis: Diese Anlage ist vom Auftraggeber auszufüllen)

A1.1 Zur Erteilung von Weisungen berechtigte Personen / Personengruppen

(in obiges Feld bitte Namen der Weisungsbefugten ergänzen)

A1.2 Zweck der Datenverarbeitung

☒ Der Zweck der Datenverarbeitung wurde im Vertrag gem. Ziff. 2.1 geregelt

A1.3 Kreis der Betroffenen

☒ Beschäftigte
☐ weitere:

(eventuell weitergehend betroffene Personengruppen bitte im obigen Feld nennen)

A1.4 Art der Daten

☒ Firmenstammdaten

☒ Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)

☒ weitere Vertragsdaten soweit diese für die weitere Vertragsabwicklung erforderlich sind (Abrechnungs- /Zahlungsdaten)

☒ Kundenhistorie

☒ Personalstammdaten

☐ Daten gemäß den Anforderungen aus den Sozialgesetzbüchern

☐ weitere:

(in obiges Feld Benennung des von der Datenverarbeitung betroffenen Datenarten)

A1.5 Telearbeit

☐ Der Auftraggeber stimmt der Datenverarbeitung der „Telearbeit“ gem. Ziff. 2.3 nicht zu:

☒ Der Auftraggeber stimmt der Datenverarbeitung der „Telearbeit“ gem. Ziff. 2.3 zu:

wenn der Auftraggeber der Telearbeit zustimmt erfolgt hier die Beschreibung der Art der Telearbeit:

Die Telearbeit darf nur über verschlüsselte, zentrale und gesicherte Verbindungen zum Unternehmensnetzwerk („VPN-Tunnel“) und mit unternehmenseigener Hardware des Auftragnehmers erfolgen.

Gemäß Softwarepflegevertrag wurden entsprechende Zugänge eingerichtet (Open VPN, S-Tunnel, TeamViewer). Eine zeitliche Einschränkung der Verbindungszeiten erfolgt nicht.

wenn der Auftraggeber der Telearbeit zustimmt erfolgt hier die Beschreibung der Standorte an welchen die Telearbeit durchgeführt werden darf:

Es sind alle fernen Standorte mit entsprechender Datenverbindung zulässig. Es erfolgt keine räumliche Einschränkung.

A1.6 Zustimmung zur Datenverarbeitung in einem Drittstaat

☐ Der Auftraggeber stimmt einer Verarbeitung von Daten in einem Drittstaat zu.

☒ Der Auftraggeber stimmt einer Verarbeitung von Daten in einem Drittstaat **nicht** zu.

A1.7 Die Feststellung/Dokumentation Angemessenheit des Schutzniveaus im Drittstaat

Falls Datenverarbeitung im Drittstaat zugestimmt, erfolgt Beurteilung der Angemessenheit des Schutzniveaus in diesem Drittstaat:

- kein Drittstaat einbezogen -

(Benennung Drittstaat)

☐ ist festgestellt durch einen Angemessenheitsbeschluss der Kommission (Art. 45 Abs. 3 DSGVO);

☐ wird hergestellt durch verbindliche interne Datenschutzvorschriften (Art. 46 Abs. 2 lit. b iVm 47 DSGVO);

☐ wird hergestellt durch Standarddatenschutzklauseln (Art. 46 Abs. 2 lit. c und d DSGVO);

☐ wird hergestellt durch genehmigte Verhaltensregeln (Art. 46 Abs. 2 lit. e iVm 40 DSGVO);

☐ wird hergestellt durch einen genehmigten Zertifizierungsmechanismus (Art. 46 Abs. 2 lit. f i.V.m. 42 DSGVO).

☐ wird hergestellt durch sonstige Maßnahmen:

Anlage 2 Datenschutzbeauftragter, Unterauftragsverhältnisse und zum Empfang von Weisungen Befugte des Auftragnehmers

A2.1 Zum Empfang von Weisungen berechtigte Personen bei dem Auftragnehmer

Support-Abteilung Email: service@time-ix.com - Telefonisch: 09288 4057591

A2.2 Unterauftragsverhältnisse:

☒ Der Auftraggeber stimmt der Beauftragung der nachfolgenden Unterauftragnehmer zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO

Firma	**Anschrift / Sitzland**	**Art der Leistung**
Strato AG	DE, Rechenzentrum Berlin/Karlsruhe	Webformular, Hosting, eMail, Datenbank (verschlüsselt, anonymisiert)
Teamviewer GmbH	DE, Göppingen	Fernwartungstool zur Erbringung von Support-Dienstleistungen

☒ Die Auslagerung auf Unterauftragnehmer oder der Wechsel des bestehenden Unterauftragnehmers sind zulässig, soweit:

- der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und
- der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und
- eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO zugrunde gelegt wird.

A2.3 Datenschutzbeauftragter

☒ Der Auftragnehmer unterliegt der Pflicht zur Bestellung eines Datenschutzbeauftragten:

Markus Roedel, Comaro Int. Business Network
Eichenweg 3
95119 Naila
Mail: info@comaro.net

Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen

☐ Der Auftragnehmer unterliegt nicht der Pflicht zur Bestellung eines Datenschutzbeauftragten:

☐ Der Auftragnehmer hat seinen Sitz außerhalb der Union:

Sollte der Auftragnehmer seinen Sitz außerhalb der Union haben kann er nach Art. 27 Abs. 1 DSGVO einen Vertreter in der Union benennen:

Anlage 3 „TOM“ des Auftragnehmers, gem. Art. 32 DSGVO

(1) 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. Wesentliche Änderungen sind zu dokumentieren

(2) Hierbei weist der Auftragnehmer gegenüber dem Auftraggeber die Umsetzung der technischen und organisatorischen Maßnahmen gemäß Art. 32 DSGVO nach. Dabei kann der Nachweis der Umsetzung solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, auch durch Vorlage eines aktuellen Testats, von Berichten oder Berichtsauszügen unabhängiger Instanzen (z. B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) oder einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z. B. nach BSI-Grundschutz) erbracht werden.

A3.1 Testat, falls vorhanden

(1) Falls beim Auftragnehmer bereits ein Testat vorliegt, kann ggf. das weitere Ausfüllen entfallen. In diesem Falle bitte in den einzelnen Abschnitten auf die entsprechende Stelle im Testat, welches dieser Anlage angehängt werden muss, verweisen.

Falls vorhanden, Nennung des aktuellen Testats:

- Keines -

(2) Liegt kein aktuelles Testat vor, verpflichtet sich der Auftragnehmer hiermit gegenüber dem Auftraggeber zur Einhaltung nachfolgender technischer und organisatorischer Maßnahmen, die zur Einhaltung der anzuwendenden Datenschutzvorschriften erforderlich sind.

A3.2 Maßnahmenkatalog

(1) Falls beim Auftragnehmer bereits ein Maßnahmenkatalog zum Schutze der Daten besteht und dieser alle Anforderungen gem. Art. 32 DSGVO erfüllt, so kann dieser Katalog als Anhang zu dieser Anlage beigefügt werden.

(2) In diesem Falle bitte in den einzelnen Abschnitten auf die entsprechende Stelle im Maßnahmenkatalog, welcher dieser Anlage angehängt werden muss, verweisen.

Falls vorhanden, Nennung des Maßnahmenkataloges:

Siehe Maßnahmenkatalog

(2) Liegt kein Maßnahmenkatalog vor, verpflichtet sich der Auftragnehmer hiermit gegenüber dem Auftraggeber zur Einhaltung nachfolgender technischer und organisatorischer Maßnahmen (siehe Ziff. A3.3), die zur Einhaltung der anzuwendenden Datenschutzvorschriften erforderlich sind.

A3.3 Beschreibung der technischen und organisatorischen Maßnahmen

A3.3.1 Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

Zutrittskontrolle

(1) Ein unbefugter Zutritt ist zu verhindern, wobei der Begriff „Zutritt“ räumlich zu verstehen ist.

(2) Technische und/oder organisatorische Maßnahmen, mit denen Unbefugten der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, verwehrt wird:

Siehe Maßnahmenkatalog

Zugangskontrolle

(3) Das Eindringen Unbefugter in die Datenverarbeitungssysteme ist zu verhindern.

(4) Maßnahmen, die das Eindringen Unbefugter in die Datenverarbeitungsanlagen verhindern:

Siehe Maßnahmenkatalog

Zugriffskontrolle

(5) Unerlaubte Tätigkeiten in Datenverarbeitungssystemen außerhalb eingeräumter Berechtigungen sind zu verhindern.

(6) Zu nennen sind Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugangsberechtigung unterliegenden Daten zugreifen können. Außerdem muss sichergestellt sein, dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

(7) Maßnahmen zur Verhinderung von Tätigkeiten innerhalb von Datenverarbeitungsanlagen, welche über die eingeräumten Berechtigungen hinausgehen:

Siehe Maßnahmenkatalog

Trennungskontrolle

(8) Daten, welche zu unterschiedlichen Zwecken erhoben wurden, sind auch getrennt zu verarbeiten.

(9) Maßnahmen zur getrennten Verarbeitung (Speicherung, Veränderung, Löschung, Übermittlung) von Daten mit unterschiedlichen Zwecken:

Siehe Maßnahmenkatalog

Pseudonymisierung

(10) Die Verarbeitung personenbezogener Daten ist in einer Weise durchzuführen, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können.

Erfolgt durch eine nummerische ID in Verbindung mit einem Zeitstempel

A3.3.2 Integrität (Art. 32 Abs. 1 lit. b DSGVO)

Weitergabekontrolle

(8) Zu nennen sind die Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und dass überprüft und festgestellt werden kann, an welchen Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

(9) Maßnahmen zur Kontrolle der Weitergabe von personenbezogenen Daten beim Transport, der Übermittlung sowie bei der Speicherung:

Siehe Maßnahmenkatalog

Eingabekontrolle

(10) Die Nachvollziehbarkeit bzw. die Dokumentation der Datenverwaltung und –pflege sind zu gewährleisten.

(11) Maßnahmen zur Möglichkeit nachträglicher Überprüfung, ob und von wem Daten eingegeben, verändert oder entfernt (gelöscht) worden sind:

Siehe Maßnahmenkatalog

A3.3.3 Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

Verfügbarkeitskontrolle

(12) Die Daten sind gegen zufällige / mutwillige Zerstörung oder Verlust zu schützen.

(13) Maßnahmen zur Datensicherung (Backupstrategie, physikalisch/logisch):

Siehe Maßnahmenkatalog

A3.3.4 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

Auftragskontrolle

(14) Der Verantwortliche und der Auftragsverarbeiter unternehmen Schritte, um sicherzustellen, dass ihnen unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedsstaaten zur Verarbeitung verpflichtet.

(15) Die weisungsgemäße Auftragsverarbeitung ist zu gewährleisten.

(16) Technische und/oder organisatorische Maßnahmen zur Abgrenzung der Kompetenzen zwischen Auftraggeber und Auftragnehmer:

Siehe Maßnahmenkatalog

☒ Eine Beurteilung des angemessenen Schutzniveaus wurde vom Auftragnehmer selbst durchgeführt und kann belastbar nachvollzogen werden.

(17) Insbesondere wurden Risiken berücksichtigt, welche mit der Verarbeitung von personenbezogenen Daten verbunden sind, wie z. B.:

- Vernichtung/Löschung,
- Verlust,
- unbeabsichtigte oder unrechtmäßige Veränderung,
- unbefugte Offenlegung oder
- unbefugten Zugang zu personenbezogenen Daten bei
- Übermittelung,
- Speicherung oder
- Verarbeitung auf andere Weise.