VERTRAGSANLAGE ZUR AUFTRAGSVERARBEITUNG GEMÄSS ART. 28 DSGVO (DATENSCHUTZ – UND DATENSICHERHEITSBESTIMMUNGEN)

zwischen Auftraggeber
- Verantwortlicher - nachstehend Auftraggeber genannt

und dem Auftragnehmer
- Auftragsverarbeiter - nachstehend Auftragnehmer genannt

Ostertag DeTeWe GmbH
Schiessstraße 61
40549 Düsseldorf

Die nachfolgenden Datenschutz- und Datensicherheitsbestimmungen (DuD-B) finden Anwendung auf alle Leistungen oder Tätigkeiten, bei denen der Auftragnehmer, von ihm eingesetzte Personen oder durch den Auftragnehmer mit Einwilligung des Auftraggebers beauftragte Nachunternehmer personenbezogene Daten im Auftrag erheben, verarbeiten oder nutzen, Art. 28. Abs. 1 Satz 1 DSGVO. Die DuD-B finden weiterhin Anwendung bei Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen, wenn dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann, Art. 28 Abs. 2-4 DSGVO. Diese Regelungen gelten entsprechend auch für alle sonstigen im Auftrag verarbeiteten Daten, insbesondere – unabhängig von der Rechtsform - Kundendaten oder eigene Daten des Auftraggebers oder seiner Mitarbeiter, und zwar auch dann, wenn sich die folgenden Bestimmungen ausdrücklich auf personenbezogene Daten beziehen.

I. Allgemeine Bestimmungen

(1) Der Auftraggeber ist als „Verantwortliche Stelle" i. S. d. Art. 4 Nr. 7 EU-Datenschutzgrundverordnung (DSGVO) für die Einhaltung der DSGVO und anderer Vorschriften über den Datenschutz, für die Rechtmäßigkeit der Datenerhebung, -verarbeitung und -nutzung, insbesondere der Datenweitergabe an den Auftragnehmer, sowie für die Wahrnehmung der Rechte der Betroffenen Art. 4 Nr. 1 DSGVO verantwortlich, Art. 28 Abs. 1 Satz 1 DSGVO. Der Auftragnehmer hat den Auftraggeber hierbei in geeigneter Weise zu unterstützen, Art. 28 Abs.3 lit. e DSGVO. Darüber hinaus verpflichtet sich der Auftragnehmer zur Einhaltung sämtlicher einschlägiger datenschutzrechtlicher Vorschriften.

(2) Bei der Erhebung, Verarbeitung und Nutzung personenbezogener Daten wird der Auftragnehmer für den Auftraggeber tätig und ist insoweit verpflichtet, die Daten ausschließlich zur Erbringung der vertraglich vereinbarten Leistungen und für Zwecke des Auftraggebers zu erheben, zu verarbeiten oder zu nutzen und dabei gemäß Art. 28 Abs.3 lit. a DSGVO den dokumentierten Weisungen des Auftraggebers zu folgen. Eine Verarbeitung oder Nutzung für sonstige, insbesondere eigene Zwecke ist dem Auftragnehmer nicht erlaubt.
Darüber hinaus sind im Einzelnen der Gegenstand und die Dauer des Auftrags, der Umfang, die Art und der Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, die sich der Auftraggeber gegenüber dem Auftragnehmer vorbehält, im Hauptvertrag festgelegt.

(3) Soweit der Auftragnehmer seine Leistung in den Räumlichkeiten oder unter Zugriff auf die Systeme des Auftraggebers erbringt, unterliegt er den Kontrolleinrichtungen des Auftraggebers (insbesondere Zutritts-, Zugangs- und Zugriffskontrolle).

(4) Bei der E-Mail-Kommunikation werden die Parteien die Vertraulichkeit beachten, indem sie vertrauliche Informationen gegen unberechtigte Kenntnisnahme oder Manipulationen schützen. Hierzu können die Parteien entsprechende technische Maßnahmen, z. B. Verschlüsselungs- und Signaturverfahren, abstimmen.

(5) Sofern der Auftraggeber den Regelungen des kirchlichen Datenschutzes unterliegt, wird insoweit festgehalten, dass neben den Regelungen der DSGVO und des BDSG auch die kirchlichen Datenschutzbestimmungen für die Vertragsparteien gültig sind und sich der Auftragnehmer ggf.

auch der Kontrolle kirchlicher Datenschutzbehörden unterwirft.

(6) Sofern der Auftraggeber den Regelungen eines Landeskrankenhausgesetzes unterliegt, wird insoweit festgehalten, dass neben den Regelungen der DSGVO und des BDSG auch die Bestimmungen dieses Landeskrankenhausgesetzes für die Vertragsparteien gültig sind und sich der Auftragnehmer ggf. auch der Kontrolle der jeweils zuständigen Aufsichtsbehörde unterwirft.

II. Gegenstand und Dauer des Auftrags

(1) Gegenstand des Auftrags zum Datenumgang ist die Durchführung folgender Aufgaben durch den Auftragnehmer: Gemäß den Leistungsvereinbarungen / Einzelbeauftragungen / der Serviceverträge aller Niederlassungen des Auftraggebers die beim Auftraggeber unter

Kunden-Nr.: _____
und
Vertrags-Nr.: _____

geführt werden (im Folgenden Leistungsvereinbarung).

(2) Definition der Aufgaben (sofern installiert):

- Inbetriebnahme, Konfiguration und Betrieb von Kommunikationsanlagen und dazugehöriger Applikationen.
- Wartungs- und Serviceleistungen remote und/oder onsite.

(3) Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung.

III. Konkretisierung des Auftragsinhalts

(1) Umfang, Art und Zweck der Erhebung, Verarbeitung und / oder Nutzung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind:

- Betrieb von Kommunikationsanlagen und dazugehöriger Applikationen (lokal, hybrid oder in der Cloud).
- Remote Serviceleistungen, Serviceleistungen vor Ort, MACD (Move, Add, Change, Delete)
- Reparatur- und Austauschleistungen

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.

(2) Art der Daten
Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien (Aufzählung / Beschreibung der Datenkategorien):

- ☒ Name, Titel, akademischer Grad
- ☒ Kontaktdaten (z. B. Telefon, E-Mail)
- ☒ Personalstammdaten (z.B. Personalnummer)
- ☒ Kommunikationsdaten (Verkehrs-, Standort,- und Nutzungsdaten
- ☒ Vertragsabrechnungs- und Zahlungsdaten
- ☒ Auskunftsangaben (von Dritten, z. B. Auskunfteien, oder aus öffentlichen Verzeichnissen)
- ☒ Patientendaten
- ☒ Gästedaten

(3) Kategorien betroffener Personen
Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- ☒ Mitarbeiter
- ☒ Mitarbeiter von Fremdfirmen
- ☒ Kunden
- ☒ Interessenten
- ☒ Lieferanten
- ☒ Mieter / Pächter
- ☒ Vermieter / Verpächter
- ☒ Patienten
- ☒ Gäste

IV. 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/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(2) Der Auftragnehmer hat die Sicherheit gem. Art. 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 Anlange „Technische und organisatorische Maßnahmen"].

(3) 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.

V. Pflichten des Auftragnehmers

(1) Zum Schutz personenbezogener Daten vor Missbrauch und Verlust wird der Auftragnehmer die technischen und organisatorischen Vorkehrungen treffen, die in der angefügten Anlage „Technische und organisatorische Maßnahmen" zwischen den Parteien festgelegt wurden. Die Vereinbarung ist Bestandteil dieser Anlage. Die vereinbarten Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Beabsichtigte wesentliche Änderungen (z. B. wesentliche Änderung von Verschlüsselungsverfahren oder Anmeldeprozeduren) sind zu dokumentieren und zu veröffentlichen. Hierzu stellt der Auftragnehmer die jeweils aktuelle Version über seine Webseite zur Verfügung

(2) Der Auftragnehmer bestätigt und stellt sicher, dass die für die Durchführung des Auftrags eingesetzten Personen abgeleitet aus Art. 28 Abs. 3 lit. b) DSGVO (Vertraulichkeit) schriftlich verpflichtet und in die Schutzbestimmungen der DSGVO sowie weiterer maßgeblicher Bestimmungen zum Datenschutz (z. B. § 3 TDDDG sowie §§ 203, 206 StGB) eingewiesen worden sind. Auf Verlangen des Auftraggebers wird der Auftragnehmer die Verpflichtung und Einweisung nachweisen.

(3) Der Auftragnehmer darf Zugriffsberechtigungen nur an Personen vergeben, die mit der Durchführung des Auftrags befasst sind. Die Berechtigungen sind in dem für die Erfüllung der jeweiligen Aufgaben erforderlichen Umfang zu vergeben. Auf Verlangen wird der Auftragnehmer dem Auftraggeber die zugriffsberechtigten Personen und deren Berechtigungen benennen.

(4) Die Verarbeitung von Daten, die Gegenstand dieses Vertrags sind, in Privatwohnungen bzw. mobiles Arbeiten (Tele- bzw. Heimarbeit von Beschäftigten des Auftragnehmers) ist seitens des Auftraggebers gestattet. Die Einhaltung der Schutzmaßnahmen dieses Vertrags sowie der Maßgaben des Art. 32 DSGVO ist seitens des Auftragnehmers sicherzustellen.

(5) Der Auftragnehmer hat den Auftraggeber unverzüglich darauf aufmerksam zu machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen die DSGVO oder eine andere Vorschrift über den Datenschutz verstößt, Art. 28 Abs. 3 lit. h) DSGVO.

(6) Der Auftragnehmer gewährleistet die ordnungsgemäße Durchführung der mit dem Auftraggeber in der Anlage „Anlage – Technische und organisatorische Maßnahmen" vereinbarten, nach Art. 32 DSGVO zu treffenden technischen und organisatorischen Maßnahmen. Die Einhaltung der technischen und organisatorischen Maßnahmen wird der Auftragnehmer regelmäßig durch geeignete Nachweise z. B. von der Revision, seinem betrieblichen Datenschutzbeauftragten oder einer anerkannten Wirtschaftsprüfungsgesellschaft belegen. Die Aktualität der Nachweise darf im Regelfall 3 Jahre nicht überschreiten. Die Nachweise sind dem Auftraggeber unaufgefordert vorzulegen. Unabhängig davon räumt der Auftragnehmer dem Auftraggeber und dessen Bevollmächtigten bezüglich der getroffenen Datenschutz- und Datensicherungsvorkehrungen ein Besichtigungs-, Einsichtnahme-, Auskunfts- und Kontrollrecht, grundsätzlich nach vorheriger Abstimmung mit dem Auftragnehmer und während dessen gewöhnlichen Geschäftszeiten, ein. Der Auftragnehmer ist verpflichtet, im Falle von Auskünften und Einsichtnahmen die erforderliche Unterstützung bereitzustellen. Im Übrigen wird der Auftragnehmer sämtlichen Personen, die Prüfungen oder sonstige Maßnahmen gemäß DSGVO vornehmen, den Zugang zu allen seinen Räumlichkeiten gestatten, sofern dies nach datenschutzrechtlichen Bestimmungen erforderlich ist, und seinen weiteren Pflichten gemäß Art. 58 DSGVO nachkommen.

(7) Der Auftragnehmer hat nur auf Weisung des Auftraggebers die personenbezogenen Daten des Verantwortlichen zu verarbeiten, Art. 28 Abs.

3 lit. a) DSGVO. Näheres bestimmt sich nach den Regelungen des Hauptvertrages.

(8) Der Auftragnehmer ist nicht befugt, ohne schriftliche Einwilligung des Auftraggebers Hard- oder Software an die Systeme des Auftraggebers anzuschließen oder darauf zu installieren.
(9) Dem Auftragnehmer ist es nicht gestattet, personenbezogene Daten in Systeme Dritter einzuspielen. Dies gilt auch für Testzwecke.

(10) Während der Entwicklung von Software werden grundsätzlich keine personenbezogenen Daten, sondern lediglich anonymisierte Original- oder fiktive Testdaten verwendet.

(11) Der Auftragnehmer wird personenbezogene Daten nach Abschluss der Arbeiten - nach den Vorgaben des Auftraggebers - vollständig datenschutzgerecht löschen (einschließlich der verfahrens- oder sicherheitstechnisch notwendigen Kopien) oder an den Auftraggeber zurückgeben. Das gleiche gilt auch für Test- und Ausschussmaterial, das bis zur Löschung oder Rückgabe unter datenschutzgerechtem Verschluss zu halten ist. Gesetzliche Aufbewahrungspflichten insbesondere nach AO und HGB bleiben hiervon unberührt. Vertragsbezogene Daten (z. B. Ansprechpartner des Auftraggebers), die zur Sicherung von Beweisinteressen des Auftragnehmers erforderlich sind, dürfen in gesperrter Form bis zum Ablauf der regelmäßigen Verjährungsfrist aufbewahrt werden. Die Löschung ist auf Anforderung schriftlich zu bestätigen.

(12) Der Auftragnehmer ist verpflichtet, den Auftraggeber unaufgefordert und unverzüglich zu informieren, wenn personenbezogene Daten unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind („Datenschutzverletzung") und Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen bestehen oder drohen (Selbstanzeigepflicht). Der Auftragnehmer nimmt zur Kenntnis, dass eine nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig erfolgte Mitteilung mit einem Bußgeld von grundsätzlich bis zu 20 Millionen Euro oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs sanktioniert werden kann, Art. 83 DSGVO. Der Auftragnehmer hat dem Auftraggeber die aus einer Datenschutzverletzung entstehenden Schäden, insbesondere die Kosten für die Benachrichtigung der Betroffenen oder ein etwaiges Bußgeld bei Verletzung der Selbstanzeigepflicht gemäß Art. 33 DSGVO zu ersetzen, sofern dem ein schuldhaftes Verhalten des Auftragnehmers zugrunde liegt.

(13) Der Auftragnehmer hat den Auftraggeber bei Unregelmäßigkeiten des Datenverarbeitungsablaufes, bei begründetem Verdacht der Verletzung von Vorschriften und vertraglichen Vereinbarungen zum Schutz personenbezogener Daten, sowie bei Beanstandungen durch die Datenschutzaufsichtsbehörde, die interne Revision oder in sonstigen Datenschutzprüfungsberichten, sofern ihm dies nicht aufgrund einer behördlichen Vorgabe im Rahmen eines Ermittlungsverfahrens untersagt ist, zu informieren und die Abhilfemaßnahmen aufzuzeigen.

(14) Der Auftragnehmer ist für die Durchführung des Auftrages verpflichtet, nach Maßgabe des Art. 37 Abs. 1 Satz 1 DSGVO einen Beauftragten für den Datenschutz schriftlich zu bestellen, der die Aufgaben nach Art. 39 DSGVO erfüllt. Der Auftragnehmer wird dem Auftraggeber den Namen des Beauftragten für den Datenschutz benennen. Bei einem Wechsel des Beauftragten für den Datenschutz wird der Auftragnehmer den Auftraggeber unverzüglich hiervon in Kenntnis setzen.

(15) Dem Auftragnehmer ist bekannt, dass ein Verstoß gegen datenschutzrechtliche Vorschriften eine Ordnungswidrigkeit nach Art. 83 DSGVO darstellen kann.

VI. Rechte von Betroffenen

(1) Der Auftragnehmer unterstützt den Auftraggeber in seinem Verantwortungsbereich und soweit möglich mittels geeigneter technisch-organisatorischer Maßnahmen bei der Beantwortung und Umsetzung von Anträgen betroffener Personen hinsichtlich ihrer Datenschutzrechte. Er darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers beauskunften, portieren, 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, Daten Portabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

VII. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

(1) Der Auftragnehmer hat, zusätzlich zu der Einhaltung der Regelungen dieses Vertrags, eigene gesetzliche Pflichten gemäß der DSGVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO. 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. 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.

b) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

c) Die unverzügliche Information des Auftraggebers 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.

d) 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.

e) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DSGVO [Einzelheiten in Anlange „Technische und organisatorische Maßnahmen"].

f) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Kap. IX dieses Vertrages.

g) Der Auftragnehmer meldet Verletzungen des Schutzes personenbezogener Daten unverzüglich an den Auftraggeber in der Weise, dass der Auftraggeber seinen gesetzlichen Pflichten, insbesondere nach Art. 33, 34 DSGVO nachkommen kann. Er fertigt über den gesamten Vorgang eine Dokumentation an, die er dem Auftraggeber für weitere Maßnahmen zur Verfügung stellt.

h) Der Auftragnehmer unterstützt den Auftraggeber in seinem Verantwortungsbereich und soweit möglich im Rahmen bestehender Informationspflichten gegenüber Aufsichtsbehörden und Betroffenen und stellt ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zu Verfügung.

i) Soweit der Auftraggeber zur Durchführung einer Datenschutz-Folgenabschätzung (DSFA) verpflichtet ist, unterstützt ihn der Auftragnehmer unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen. Gleiches gilt für eine etwaig bestehende Pflicht zur Konsultation der zuständigen Datenschutz-Aufsichtsbehörde.

(2) Dieser Vertrag entbindet den Auftragnehmer nicht von der Einhaltung anderer Vorgaben der DSGVO.

VIII. Nachunternehmer

(1) Als Unterauftragsverhältnisse durch Nachunternehmer 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 in Anspruch nimmt, z.B. Telekommunikationsleistungen, Post-/Transportdienstleistungen, Reinigungsleistungen oder Bewachungsdienstleistungen. Wartungs- und Prüfleistungen stellen dann ein Unterauftragsverhältnis dar, wenn sie für IT-Systeme erbracht werden, die im Zusammenhang mit einer Leistung des Auftragnehmers nach diesem Vertrag erbracht werden. 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 zu treffen sowie Kontrollmaßnahmen zu ergreifen.

(2) Der Auftraggeber stimmt der Beauftragung der unter Anlage 1 benannten Nachunternehmer zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO.

(3) Der Einsatz eines weiteren Nachunternehmers oder der Wechsel eines bestehenden Nachunternehmers ist zulässig, soweit:

- der Auftragnehmer eine solche Auslagerung auf Nachunternehmer dem Auftraggeber 14 Tage 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.

(4) Die vertraglichen Vereinbarungen zwischen dem Auftragnehmer und dem Nachunternehmer sind so zu gestalten, dass sie den Regelungen der vorliegenden Vereinbarung entsprechen. Zu diesem Zweck müssen insbesondere die mit dem Nachunternehmer zu vereinbarenden technischen und organisatorischen Maßnahmen ein gleichwertiges Schutzniveau aufweisen.

(5) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Nachunternehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

(6) Erbringt der Nachunternehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.

(7) Eine weitere Auslagerung durch den Nachunternehmer bedarf der ausdrücklichen Zustimmung des Haupt Auftraggebers (mind. Textform) sowie auch der ausdrücklichen Zustimmung des Haupt Auftragnehmers.

(8) Sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Nachunternehmer aufzuerlegen.

(9) Auf Anforderung des Auftraggebers wird der Auftragnehmer Auskunft über den wesentlichen Vertragsinhalt mit dem Nachunternehmer und die Umsetzung der datenschutzrelevanten Verpflichtungen geben, erforderlichenfalls durch Einsicht in die relevanten Vertragsunterlagen.

(10) Der Auftragnehmer bleibt für die Erfüllung der auf den Nachunternehmer übertragenen Tätigkeiten im gleichen Umfang verantwortlich, als würden diese durch den Auftragnehmer selbst ausgeführt.

IX. Kontrollrechte des Auftraggebers

(1) 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 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 aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z. B. Wirtschaftsprüfer, IT-Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren).

(4) Der Auftraggeber hat das Recht, kostenfrei Kontrollen durchzuführen, solange diese sich in einem Umfang von max. einem Tag pro Jahr oder Auskünfte nach Bescheinigungen zur Angemessenheit der TOM beschränken. Der Auftraggeber wird Kontrollen nur im erforderlichen Umfang durchführen und die Betriebsabläufe des Auftragnehmers dabei nicht unverhältnismäßig stören. Für die Ermöglichung von Kontrollen durch den Auftraggeber, die darüber hinaus gehen, kann der Auftragnehmer einen Vergütungsanspruch geltend machen, es sei denn die Kontrolle ist aufgrund des Verdachts eines Verstoßes ge-

gen anwendbares Datenschutzrecht oder diese DuD-B erforderlich.

X. Weisungsbefugnis des Auftraggebers
(1) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).

(2) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

XI. Zuständige Personenkreise
Personen des Auftraggebers und Auftragnehmers mit den dazugehörigen Kontaktdaten bzw. Kommunikationskanälen

(1) Zuständiger Personenkreis und Weisungsempfänger des Auftragnehmers:
a) Datenschutzbeauftragter des Auftragnehmers:
Volker Wassermann (externer DSB), bridge4IT GmbH
Telefon: 0211 / 95980 - 197
E-Mail: datenschutzbeauftragter@ostertag-detewe.de
b) Datenschutzkoordinator des Auftragnehmers:
Markus Greuter, Ansprechpartner und Weisungsempfänger
Telefon: 0211 / 95980 -196,
E-Mail: datenschutz@ostertagdetewe.de
c) Service Desk Ostertag DeTeWe, Weisungsempfänger
Telefon: 0800 3868 100,
E-Mail: info@ostertagdetewe.de

(2) Beim Auftraggeber:
Sofern sensitive Daten vom Auftragnehmer für den Auftraggeber verarbeitet werden, benennt der Auftraggeber folgende weisungsberechtigte Personen:

_____
_____
_____
_____
_____

Datenschutzbeauftragter des Auftraggebers:
_____
_____
_____

XII. Löschung und Rückgabe von personenbezogenen Daten
(1) 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 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 oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

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

XIII. Haftung
(1) Auftraggeber und Auftragnehmer haften gegenüber betroffener Personen entsprechend der in Art. 82 DSGVO getroffenen Regelung.

(2) Sofern vorstehend nicht anders geregelt, entspricht die Haftung im Rahmen dieses Vertrages der des Hauptvertrages.

XIV. Unterschriften

Auftraggeber	**Ostertag DeTeWe GmbH (Auftragsverarbeiter)**
Ort, Datum	Ort, Datum
Name in Druckbuchstaben	Name in Druckbuchstaben
Unterschrift / Stempel	Unterschrift / Stempel

Anlagen:
Anlage 1 - Nachunternehmer
Anlage 2 - TOM (Technische und organisatorische Maßnahmen)

ANLAGE 1 – NACHUNTERNEHMER ZUR AUFTRAGSVERARBEITUNG GEMÄSS ART. 28 DSGVO (DATENSCHUTZ – UND DATENSICHERHEITSBESTIMMUNGEN)

Der Auftragnehmer nimmt für die Verarbeitung von Daten im Auftrag des Auftraggebers Leistungen von Dritten in Anspruch, die in seinem Auftrag Daten verarbeiten („Unterauftragnehmer").

Dabei handelt es sich um nachfolgende(s) Unternehmen:

- ☒ AudioCodes Germany GmbH, Hanauer Landstrasse 148a, 60314 Frankfurt, 3rd Level Support
- ☒ ASC Technologies AG, Seibelstraße 2, 63768 Hösbach, 3rd Level Support
- ☒ Ascom Deutschland GmbH, Kruppstraße 105, 60388 Frankfurt, 3rd Level Support
- ☒ Avaya GmbH & Co. KG, Theodor-Heuss-Allee 112, 60486 Frankfurt, 3rd Level Support
- ☒ Bewatec Kommunikationstechnik GmbH, Orkotten 65, 48291 Telgte, 3rd Level Support
- ☒ C4B Com For Business AG, Untere Point 8, 82110 Germering, 3rd Level Support
- ☒ CASERIS GmbH, Am Birkenfeld 1-3, 52222 Stolberg, 3rd Level Support
- ☒ Crown Software GmbH, Ludwig-Erhard-Allee 20, 76131 Karlsruhe, 3rd Level Support
- ☒ Estos GmbH, Petersbrunner Str. 3A, 82319 Starnberg, 3rd Level Support
- ☒ F24 AG, Ridlerstraße 57, 80339 München, 3rd Level Support
- ☒ Ferrari electronic AG, Ruhlsdorfer Str. 138, 14513 Teltow, 3rd Level Support
- ☒ Fortinet Deutschland GmbH, Feldbergstr. 35, 60323 Frankfurt, 3rd Level Support
- ☒ Luware Deutschland GmbH, Schlossstrasse 70, 70176 Stuttgart, 3rd Level Support
- ☒ Netopsie Technologies GmbH, Lister Damm 2, 30163 Hannover, Wartung, 3rd Level Support
- ☒ Mitel Deutschland GmbH, Zeughofstraße 1, 10997 Berlin, 3rd Level Support
- ☒ Siemens AG, Werner-von-Siemens-Straße 1, 80333 München, 3rd Level Support
- ☒ Temeno GmbH, Breite Str. 10, 40670 Meerbusch, 3rd Level Support
- ☒ tetronik GmbH, Silberbachstraße 10, 65232 Taunusstein, 3rd Level Support
- ☒ Unify Software and Solutions GmbH & Co. KG, Otto-Hahn-Ring 6, 81739 München, 3rd Level Support

- ☒ newbetech solutions GmbH, An der Gümpgesbrücke 15, 41564 Kaarst, Service
- ☒ tel-da-kom GmbH & Co. KG, Nienburger Str. 24, 31515 Wunstorf, Service
- ☒ KoMota GmbH, Gustav-Kirchhoff-Straße 17, 67098 Bad Dürkheim, Service
- ☒ Telnetserve Bader & Scholz GbR, Landsberger Allee 203, 13055 Berlin, Service
- ☒ ARKTIS GmbH, Schwedenstr. 9, 13359 Berlin, Service
- ☒ ASPRRO-Tec GmbH, Augsburger Str. 10, 99091 Erfurt, Service
- ☒ Elektrotechnik Thoms, Ristedter Hauptstraße 26, 28857 Syke, Service
- ☒ purpleview GmbH, Kampstraße 6, 44137 Dortmund, Service
- ☒ Elektro Haeussler LTD, Aachener Straße 83-85, 52146 Würselen, Service
- ☒ Winfried Recknagel, Eichenstr. 19 /1, 75217 Birkenfeld, Service
- ☒ SKKOM Kommunikations- & Netzwerktechnik, Marktstraße 13, 21423 Winsen, Service

- ☒ 1&1 Versatel GmbH, Wanheimer Straße 90, 40468 Düsseldorf, Carrier
- ☒ Ecotel Communication AG, Prinzenallee 11, 40549 Düsseldorf, Carrier
- ☒ CNT AG, Ludwig-Erhard-Allee 20, 76131 Karlsruhe, Carrier
- ☒ Colt Technology Services GmbH, Gervinusstr. 18-22, 60322 Frankfurt, Carrier
- ☒ Plusnet GmbH, Mathias-Brüggen-Str. 55, 50829 Köln, Carrier
- ☒ QSC EMEA GmbH, Am Ilvesbach 6, 74889 Sinsheim, Carrier
- ☒ Telekom Deutschland GmbH, Landgrabenweg 151, 53227 Bonn, Carrier

ANLAGE 2 - TOM

TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN ZUR AUFTRAGS-VERARBEITUNG (SICHERHEIT DER VERARBEITUNG NACH ART. 32 DSGVO) DER OSTERTAG DETEWE GMBH

Verantwortlicher

Ostertag DeTeWe GmbH
Schiessstraße 61
40549 Düsseldorf
Telefon: 0211 / 95980-0
E-Mail: info@ostertagdetewe.de

vertreten durch den Geschäftsführer Manuel Ferre Hernandez.

- nachstehend Auftragnehmer genannt -

Datenschutz-Organisation

Datenschutzkoordinator:	Markus Greuter
Adresse:	Ostertag DeTeWe GmbH Datenschutz Schiessstraße 61 40549 Düsseldorf
Telefon:	0211 / 95980 - 196
E-Mail:	datenschutz@ostertagdetewe.de
Datenschutzbeauftragter:	Volker Wassermann (externer DSB) bridge4IT GmbH
Adresse:	Ostertag DeTeWe GmbH Datenschutzbeauftragter Schiessstraße 61 40549 Düsseldorf
Telefon:	0211 / 95980 - 197
E-Mail:	datenschutzbeauftragter@ostertagdetewe.de

Einleitung

Technische und organisatorische Maßnahmen (kurz auch TOM genannt) sind durch die DSGVO vorgeschriebene Maßnahmen, die die Sicherheit der Verarbeitung personenbezogener Daten gewährleisten sollen. Die Implementierung angemessener technischer und organisatorischer Maßnahmen stellt eine gesetzliche Anforderung dar und ist laut der DSGVO dokumentationspflichtig.

Technische und organisatorische Maßnahmen der Ostertag DeTeWe GmbH

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Auftraggeber und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

1. Pseudonymisierung und Verschlüsselung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)

- **Pseudonymisierung**
  Zur Auswertung von Verbindungsdaten oder Verbrauchinformationen zu statistischen Zwecken werden personenbezogene Daten pseudonymisiert, bevor diese im Report bereitgestellt werden.

- **Verschlüsselung**
  Die Übermittlung personenbezogener Daten findet elektronisch mittels VPN, TLS oder HTTPS statt. Die entsprechende Technologie und Protokolle werden auf den jeweils aktuellen Stand gehalten und verwendet. Mobile und auch andere Datenträger werden gemäß den Sicherheitsanforderungen in Bezug auf die darauf verarbeiteten personenbezogenen Daten verschlüsselt. Siehe auch Kapitel 2 – Zugriffskontrolle.

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

- **Zutrittskontrolle**
  Der Zutritt zu den Infrastrukturen des Auftraggebers obliegt ihm. Nach Vereinbarung zwischen Auftraggeber und Auftragnehmer können Namenslisten berechtigter Mitarbeiter des Auftragnehmers erstellt werden.
  An den Bürogebäuden des Auftragnehmers finden derzeit unterschiedliche Zugangskontrollen Anwendung (mind. Schließsysteme, elektronische Zutrittssysteme, Alarmanlagen, ggfls. Pförtner oder Empfangspersonal).
  Die Bürogebäude des Auftragnehmers sind in unterschiedlichen Bereichen unterteilt und in einem Zonenplan je Standort dokumentiert. Die entsprechenden Vorgaben hierzu sind in einem Zonenkonzept definiert.
  Der Zutritt ist für Mitarbeiter der entsprechenden Bereiche des Auftragsnehmer durch entsprechende Zugangskontrollen gesichert. Besuchern ist nach Anmeldung am Empfang der Zutritt möglich, wird aber durch einen Mitarbeiter des Auftragnehmers begleitet.
  Für die Rechenzentren, die von dem Auftragnehmer genutzt werden, gilt zudem: Ein Zutritt ist nur nach vorheriger Anmeldung (24h) unter Nennung des vollständigen Namens, der Angabe der Personalausweis- oder Passnummer und der beabsichtigten Aufenthaltsdauer beim Rechenzentrum möglich. Im Rechenzentrum überprüft das Empfangspersonal die Anmeldung und die Berechtigungen. Es gibt ein Zonenmodell mit unterschiedlichen Sicherheitsbereichen und entsprechenden Zugangskontrollsystemen.

- **Zugangskontrolle**
  Die Zugangskontrolle zu DV-Systemen stellt sich wie folgt dar:

  a) PCs, Server etc. des Auftraggebers unterliegen seinem Einflussbereich
  b) Service-Notebooks / PCs des Auftragnehmers sind boot- und passwortgeschützt, zudem sind die Festplatten mit Bitlocker verschlüsselt.

c) Zugänge auf zentrale DV-Systeme des Auftragnehmers bedürfen eines gültigen Domain Accounts, gemeinsam genutzte Accounts sind nicht zugelassen. Die Passwörter der Domain Accounts haben eine Gültigkeit von 90 Tagen. Bei Fehlanmeldungen findet eine Pausenschaltung statt. Zusätzlich sind die Zugänge durch eine 2-Faktor-Authenifizierung geschützt. Für alle Passwörter, die in Systemen des Auftragnehmers eingesetzt werden, gilt eine Passwortrichtlinie.
d) Remotezugang zu zentralen DV-Systemen des Auftragnehmers erfolgen ausschließlich über gesicherte VPN-Tunnels. Auch hier findet die Validierung der User via ADS statt, es gelten die gleichen Kennwortvorgaben.
e) Nur vom Informationseigentümer autorisierte, berechtigte Mitarbeiter bzw. externe Dienstleister erhalten Zugang zu den DV-Systemen.
f) Verlässt ein Mitarbeiter Ostertag DeTeWe GmbH, wird gemäß interner Verfahrensanwendung ein Deaktivieren/Löschen des Zuganges sichergestellt.
g) Externe Dienstleister sind angehalten Ostertag DeTeWe GmbH umgehend über personelle Veränderungen im Zusammenhang mit dem zu leistenden Service zu informieren. Die für ext. Dienstleister freigeschalteten Zugänge werden zusätzlich in einem Quartalsrhythmus kontrolliert (rezertifiziert).

• Zugriffskontrolle
Berechtigungen innerhalb der DV-Systeme des Auftragnehmers werden über Rollendefinitionen und Rollenzuweisungen geregelt.

Typische Rollen: Anlegen von Daten, Ändern von Daten, Löschen von Daten, Lesen

Die Zugriffskontrolle ist mittels Berechtigung von Zugriffen auf Applikationen, bzw. Einzelsysteme geregelt.

Beschreibung der Zugriffsberechtigungen:

Zugriffsberechtigung	Beschreibung System	Typische Rolle
Voll (Admin)	Sämtliche im Einsatz befindlichen Systeme, Applikationen und Netzwerkkomponenten.	Field-Service, Sysop, 2nd-4th Level Support
Lesend (User)	Sämtliche im Einsatz befindlichen Systeme, Applikationen und Netzwerkkomponenten.	Kunden-Service/ Betriebsorganisation

Zugriffe auf ITK-Lösungen beim Auftraggeber vor Ort durch Remote Services (Teleservice):
Zur Nutzung des Remote Services ist eine gesonderte Servicesoftware notwendig. Die Kontrolle erfolgt über einen User Account (Kundennummer und Anlagennummer) dem bestimmte Rechte und ein Passwort zugeordnet sind. Protokolliert werden Logins (User, Datum, Uhrzeit, IP-Adresse).
Der Auftraggeber kann entscheiden, ob der Zugang generell gesperrt bzw. ständig aktiv ist oder nur im Bedarfsfall durch ihn aktiviert wird.

Secure Remote Services SRS (produktunabhängig und IP-basierend):
Der Zugriff findet hier ausschließlich über VPN statt. Der Betrieb dieses zentralen DV Systems beim Auftragnehmer findet innerhalb eines vollständig getrennten und eigenständigen Netzwerkes statt.
Die Administration von Anlagenzugriffen und Usern innerhalb dieses Netzes wird ausschließlich durch den zentralen IT-Support des Auftragnehmers nach vorgegebenen Prozessen durchgeführt (z.B.: Freigabe von Usern für welche DV-Systeme).
Die Anbindung der DV-Systeme beim Auftraggeber an das SRS System ist mit zusätzlichen Kosten verbunden.

• Eingabekontrolle
Durchgeführte Arbeiten werden grundsätzlich Incident basierend im Service Management System dokumentiert. Die Protokollierung der durchgeführten Datenänderungen im ITK-System findet systemintern in sogenannten History/Logfiles statt. Eine Protokollierung innerhalb der DV-Systeme

findet statt, wobei mindestens User, Datum, und Uhrzeit dokumentiert werden. In Abhängigkeit der zu administrierenden ITK Lösungen können zusätzliche Protokollierungen konfiguriert werden.

- **Trennungskontrolle**

Die Mitarbeiter der Ostertag DeTeWe sind angewiesen, Daten nur im Rahmen der von ihnen aus- zuführenden Aufgaben (z.B. Dienstleistungserbringung) und zur Wahrung der damit verbundenen Zweckbindung zu erheben, zu verarbeiten und zu nutzen. Auf technischer Ebene werden dazu die Möglichkeiten der Mandantenfähigkeit, die Funktionstrennung sowie die Trennung von Test- und Produktionssystemen eingesetzt.
Daten werden ausschließlich der eindeutigen Kundennummer, im Service Management System zusätzlich der eindeutigen Location ID (Standort-Nr.) und den damit verknüpften CI's (Komponenten) zugeordnet.

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

Zur Sicherstellung der Integrität im Rahmen des E-Mail-Verkehrs werden E-Mailsignaturen zertifikatsbasierend (SMIME) eingesetzt.
Zur Analyse von Störungen können einzelne Daten, in der Regel keine personenbezogenen Daten, an den Hersteller weitergegeben werden. Die Übermittlung findet ausschließlich elektronisch mittels VPN oder HTTPS in das Service Managementsystem des Herstellers statt.
Die Übermittlung personenbezogener Daten findet elektronisch mittels VPN, TLS oder HTTPS statt. Die entsprechende Technologie und Protokolle werden auf den jeweils aktuellen Stand gehalten und verwendet. Mobile und auch andere Datenträger werden gemäß den Sicherheitsanforderungen in Bezug auf die darauf verarbeiteten personenbezogenen Daten verschlüsselt. Siehe auch Kapitel 2 – Zugriffskontrolle
Durchgeführte Arbeiten werden grundsätzlich Incident basierend im Service Management System dokumentiert. In Abhängigkeit der zu administrierenden ITK-Lösungen und der Anforderungen des Auftraggebers können zusätzliche Protokollierungen konfiguriert sein.

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

- **Verfügbarkeitskontrolle**

Zentrale DV-Systeme des Auftragnehmers sind mit RAID-Funktionalität, redundanten Netzteilen und unterbrechungsfreien Stromversorgungen (USV) ausgestattet. Zusätzlich wird das Rechenzentrum des Auftragnehmers mittels Notdiesel abgesichert.
Unternehmensweit werden Server, Desktops, Notebooks etc. des Auftragnehmers mittels eines Virenscanners ständig überwacht und zentral durch die IT des Auftragnehmers gemanagt.

- **Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO)**

Backups finden automatisiert statt, wobei partielle und Full Backups (wöchentlich) Anwendung finden. Die Backups werden auf redundanten Storage-Systemen erstellt. In Bezug auf Hardwareausfälle hält der Auftragnehmer für seine zentralen DV-Systeme Ersatzteile vor.

- **ITK-Lösungen beim Auftraggeber vor Ort:**

RAID-Funktionalität, USV-Versorgung sowie Speicherorte hängen grundsätzlich von den Anforderungen des Auftraggebers ab. In Abhängigkeit der vereinbarten Auftragskompetenz und Verantwortung obliegt dem Auftraggeber oder dem Auftragnehmer die Verfügbarkeitskontrolle.
Ist der Auftragnehmer verantwortlich, so werden automatisierte Backups eingerichtet. Die Speicherung der Daten findet derzeit in Absprache mit dem Auftraggeber statt. In Bezug auf Hardwareausfälle hält der Auftragnehmer gemäß den Vereinbarungen mit dem Verantwortlichen (SLA's) entsprechende Ersatzteile vor. Darüber hinaus werden bei den für die Leistungserbringung eingesetzten Herstellern Back-to-Back Agreements zur Hardwareversorgung und Softwareentstörung abgeschlossen.

5. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO)

- **Datenschutz-Management**
  Der Auftragsverarbeiter betreibt ein Datenschutzmanagementsystem in Anlehnung an die High-Level-Structure gemäß der ISO-Standards (kontinuierlicher Verbesserungsprozess).

- **Incident-Response-Management**
  Zum Umgang und der Behandlung von Datenschutzvorfällen hat die Ostertag DeTeWe GmbH ein Vorfallmeldesystem eingerichtet. Entsprechende Richtlinien wurden formuliert und umgesetzt.

- **Leistungsüberwachung**
  Ostertag DeTeWe hat Key Performance Indikatoren (KPI's) definiert auf deren Grundlage regelmäßig Leistungsüberwachungen stattfinden. Die Ergebnisse werden an das Management kommuniziert und mit diesem ausgewertet.

- **Auftragskontrolle**
  Es findet keine Auftragsverarbeitung ohne entsprechende Weisung des Auftraggebers statt. Hierzu werden eindeutige Verträge gestaltet und ein formalisiertes Auftragsmanagement betrieben.

- **Vertraulichkeitsverpflichtung der Mitarbeiter**
  Die Mitarbeiter der Ostertag DeTeWe GmbH sind alle durch den Arbeitsvertrag zur Vertraulichkeit verpflichtet. Durch Mitarbeiterschulungen zum Datenschutz und zur Informationssicherheit erfolgt regelmäßig eine Sensibilisierung (Art. 28 Abs.3 lit. b DSGVO).

6. Beurteilung des angemessenen Schutzniveaus (Art. 32 Abs. 2 DSGVO)

Ostertag DeTeWe pflegt eine Übersicht über die Verarbeitungstätigkeiten auch unter Berücksichtigung der im Rahmen der Dienstleistung erbrachten Services und damit verbunden Verarbeitungstätigkeiten. Infolgedessen werden auch evtl. Verfahren mit einer Datenschutzfolgenabschätzung bewertet.

Sonstiges

Die technischen und organisatorischen Maßnahmen werden kontinuierlich überprüft und ggf. verändert bzw. erweitert. Die aktuelle Version steht unter www.ostertagdetewe.de/dsgvo zum Download bereit.