Schön, dass wir zusammenarbeiten!

Die vertraglichen Formalitäten unserer Zusammenarbeit haben wir in dieser Unterlage für Sie zusammengestellt:

1. Die Allgemeinen Geschäftsbedingungen (S. 2-9)
   Das kennen Sie sicher. Die AGB ist die Basis unserer Zusammenarbeit.

2. Die AV, Auftragsverarbeitungsvereinbarung (S. 11-17)
   Diese Vereinbarung brauchen wir aufgrund der Datenschutz-Grundverordnung (DSGVO). Die Darfichrein GmbH verarbeitet die Kontaktdaten Ihrer Kunden, Gäste und Besucher in Ihrem Auftrag. Daraus ergeben sich einige Rechte und Pflichten. Diese sind in der Vereinbarung festgelegt.

3. Anhang zur AV: Technische und Organisatorische Maßnahmen (S. 18-22)
   Da die Darfichrein GmbH Daten in Ihrem Auftrag verarbeitet, ist durch die DSGVO festgelegt, dass Darfichrein Ihnen auch die ergriffenen Maßnahmen anzeigt, um die Daten zu schützen und zu sichern.

Darfichrein GmbH
Türkenstr. 7
80333 München
hi@darfichrein.de
Handelsregisternummer HRB 257975
Gesetzlich vertreten durch den Geschäftsführer Dominik Wörner und Isabella Hren

Allgemeine Geschäftsbedingungen (AGB) für die Nutzung der Plattform „darfichrein.de“

Stand 19.06.2020

Die Darfichrein GmbH (Hansastraße 12-16, 80686 München) („Anbieter“) betreibt den Cloud-Service „darfichrein.de“ („Plattform“), über den ein Unternehmer seinen Kunden eine einfache, kontaktlose Registrierung von Kontaktdaten über die Smartphones der Kunden anbieten und diese Daten verschlüsselt speichern kann, um rechtlichen Dokumentationspflichten nachzukommen. Daten der Kunden werden mit einem öffentlichen Schlüssel des Unternehmers verschlüsselt. Die Daten der Kunden sollen dabei nur bei Bedarf abgerufen und mit dem privaten Schlüssel des Unternehmers entschlüsselt werden, und werden nach Ende der jeweiligen Aufbewahrungszeiträume automatisch gelöscht.

1 Vertragsschluss, Vertragsgegenstand

1.1 Die Nutzung der Plattform wird nur öffentlichen Stellen (insb. Bund, Länder, Kommunen und deren Behörden und Einrichtungen) sowie Unternehmen im Sinne des § 14 BGB (d. h. natürliche oder juristische Personen oder rechtsfähige Personengesellschaften, die bei Abschluss des Vertrages in Ausübung ihrer gewerblichen oder selbstständigen beruflichen Tätigkeit handeln) angeboten; beide werden in diesen Bedingungen zur Vereinfachung als „Unternehmer“ bezeichnet.

1.2 Indem der Unternehmer auf der Anbieter-Website (http://www.darfichrein.de) ein Leistungspaket auswählt und die Registrierungsmaske ausfüllt und absendet, macht er ein Angebot zum Abschluss des Vertrages. Bis zum Absenden der Registrierungsmaske kann der Unternehmer Eingabefehler dadurch korrigieren, dass er das entsprechende Feld der Registrierungsmaske erneut anklickt und den Fehler korrigiert. Der Vertrag kommt zustande, indem der Anbieter das Angebot des Unternehmers ausdrücklich annimmt oder den Zugang zur Plattform tatsächlich freischaltet.

1.3 Der Anbieter stellt dem Unternehmer die auf www.darfichrein.de näher bezeichneten Funktionalitäten der Plattform als Cloud-Service bereit. Die zum Zeitpunkt des Vertragsschlusses aktuellen Funktionsbeschreibungen auf der Website werden im Folgenden auch als „Leistungsbeschreibung“ bezeichnet. Über die in den jeweiligen Leistungsbeschreibungen ausdrücklich genannten Leistungen hinaus erbringt der Anbieter keine Schulungs-, Installations-, Konfigurations-, Anpassungs-, Programmier-, oder sonstige Leistungen. Der Anbieter leistet keine Rechtsberatung. Es liegt in der Verantwortung des Unternehmers, sich über die für seinen Betrieb geltenden Dokumentationsanforderungen zu unterrichten und diese umzusetzen. Die Plattform ist lediglich ein Werkzeug, das der Unternehmer hierfür nutzen kann.

1.4 Diese AGB sind für ihren Anwendungsbereich abschließend. Etwaige Geschäftsbedingungen des Unternehmers werden auch dann nicht

Vertragsbestandteil, wenn der Anbieter ihrer Anwendung nicht ausdrücklich widerspricht.

2 Pflichten des Anbieters; Verfügbarkeit

2.1 Der Anbieter hostet die Plattform und stellt dem Unternehmer Zugangsdaten und einen öffentlichen sowie einen privaten Schlüssel zur Verfügung. Das Hosting der Plattform beinhaltet auch eine Bereitstellung von Speicherplatz in einem dem Nutzungszweck angemessenen Umfang.

2.2 Übergabepunkt der Leistungen ist der Router des vom Anbieter verwendeten Rechenzentrums. Die geschuldete Verfügbarkeit der Plattform beträgt 99% im Monatsmittel während der Geschäftszeiten des Unternehmers, d.h. die Software kann bis zu 7,44 Stunden pro Monat nicht verfügbar sein, und Ausfallzeiten außerhalb der Geschäftszeit des Unternehmers werden für diese Berechnung nicht berücksichtigt. Geplante Wartungszeiten im angemessenen Umfang gelten nicht als Zeiten fehlender Verfügbarkeit. Der Anbieter bemüht sich, solche Wartungsarbeiten in Zeiten mit statistisch geringer Auslastung der Plattform vorzunehmen.

2.3 Bei Unterschreitung der vorgenannten Verfügbarkeit kann der Unternehmer die Vergütung für den jeweiligen Monat wie folgt mindern:

a) Verfügbarkeit zwischen 99% und 95,1% Minderung um 20%
b) Verfügbarkeit zwischen 95% und 90,1%: Minderung um 50%
c) Verfügbarkeit 90% oder weniger: Minderung um 100%.

Steht dem Unternehmer in zwei aufeinanderfolgenden Monaten ein Minderungsrecht um 50% oder mehr zu, kann er den Vertrag zusätzlich fristlos kündigen. Dieses Kündigungsrecht kann jeweils nur innerhalb von einem Monat nach Vorliegen der Voraussetzungen ausgeübt werden. Außer im Fall von Vorsatz und grober Fahrlässigkeit (insoweit bleibt Ziffer 8 unberührt) sind die vorstehenden Rechtsfolgen einer Unterschreitung der Verfügbarkeit abschließend.

2.4 Der Anbieter stellt Benutzungshinweise zu der Plattform in deutscher Sprache in elektronischer Form (z.B. als Tutorial-Video, FAQ) zur Verfügung. Eine gedruckte Dokumentation wird nicht geschuldet. Der Unternehmer darf die Benutzungshinweise nur zu internen Zwecken vervielfältigen. Alle sonstigen Rechte an den Benutzungshinweisen, insbesondere die Bearbeitungsrechte, bleiben vorbehalten.

2.5 Der Anbieter verarbeitet personenbezogene Daten, die der Unternehmer bzw. dessen Kunden in die Plattform hochladen, im Auftrag des Unternehmers. Der Unternehmer ist der Verantwortliche im Sinne des Datenschutzrechts. Er hat in diesem Zusammenhang auch die in seinem Account zur Verfügung gestellten Dokumente (Auftragsverarbeitungsvereinbarung, Infoblatt und Verzeichnis der Verarbeitungstätigkeiten) herunterzuladen, zu seinen Akten zu nehmen und sich als Verantwortlicher einzutragen. Im Hinblick auf die Datenverarbeitung im Auftrag des Unternehmers schließen die Parteien die Auftragsverarbeitungsvereinbarung (AV), als

Bestandteil des Vertrags (siehe unten). Bei Widersprüchen gehen die Bestimmungen der AV dieser AGB vor.

2.6 Der Anbieter ist berechtigt, aber nicht verpflichtet, den Funktionsumfang der Plattform zu erweitern und weiterzuentwickeln. Es bleibt dem Anbieter vorbehalten, Erweiterungen und Weiterentwicklungen nur gegen Zahlung eines zusätzlichen Entgeltes (und nach Maßgabe einer dann abzuschließenden Ergänzung dieses Vertrages) anzubieten. Stellt der Anbieter nach Vertragsschluss erweiterte oder zusätzliche Funktionen kostenlos zur Verfügung, gelten diese bereitgestellten Funktionen als freiwillige Leistung des Anbieters.

2.7 Der Anbieter kann den Funktionsumfang der Plattform jederzeit in für den Unternehmer zumutbarem Maße ändern. Eine Änderung ist insbesondere dann zumutbar, wenn sie aus wichtigem Grund erforderlich wird und die in der Leistungsbeschreibung definierten Leistungsmerkmale im Wesentlichen sowie die Hauptleistungspflichten des Anbieters vollständig erhalten bleiben. Ein wichtiger Grund liegt insbesondere dann vor, wenn Störungen der Leistungserbringung durch Subunternehmer vorliegen oder die Änderung aus sicherheitstechnischen Gründen oder wegen Änderungen von Gesetzgebung und/oder Rechtsprechung geboten ist. Betreffen die Änderungen nicht ausschließlich zeitkritische Sicherheitsupdates, Erweiterungen der Funktion oder nicht nur unwesentliche Bestandteile der zu erbringenden Leistungen (wie beispielsweise geringfügige Designänderungen), wird der Anbieter den Unternehmer über die Änderung mindestens vier Wochen vor deren Inkrafttreten per E-Mail hinweisen.

2.8 Der Anbieter ist berechtigt, den Account des Unternehmers vorübergehend zu sperren, wenn

a) Anhaltspunkte bestehen, dass Zugangsdaten bzw. private Schlüssel missbraucht wurden bzw. werden oder die Zugangsdaten bzw. privaten Schlüssel einem unbefugten Dritten überlassen wurden bzw. werden oder einer Person zugewiesenen Zugangsdaten durch mehr als eine natürliche Person verwendet werden;
b) Anhaltspunkte bestehen, dass sich unbefugte Dritte anderweitig Zugang zu dem Account des Unternehmers verschafft haben;
c) die Sperrung aus technischen Gründen erforderlich ist;
d) der Anbieter aufgrund gesetzlicher, gerichtlicher oder behördlicher Vorgaben zur Sperrung verpflichtet ist;
e) der Unternehmer mehr als zwei Wochen mit der Zahlung eines vereinbarten Entgelts in Verzug ist;
f) der Unternehmer falsche Zahlungsdaten hinterlegt bzw. hinterlegte Zahlungsdaten nicht aktualisiert hat und eine regelmäßige Erfüllung der Leistungspflichten des Unternehmers nicht gewährleistet ist;
g) eine Gefahr der erheblichen Beschädigung oder Beeinträchtigung der vom Anbieter bereitgestellten Leistungen besteht.

Der Anbieter soll die Sperrung spätestens einen Werktag vor Inkrafttreten in Textform ankündigen, soweit die Ankündigung unter Abwägung der beiderseitigen Interessen zumutbar und mit dem Zweck der Sperrung vereinbar ist. Der Anbieter wird die Sperrung unverzüglich aufheben, wenn der Grund der Sperrung wegfällt. Soweit der Zweck der Sperrung es erlaubt, insb. in den Fällen der Buchstaben e) und f), verbleibt dem Unternehmer die Möglichkeit, bei Bedarf Daten der Kunden abzurufen und zu entschlüsseln.

2.9 Der Anbieter ist berechtigt, zur Erfüllung des Vertrages nach eigenem Ermessen Subunternehmer einzuschalten. Die Bestimmungen der Auftragsverarbeitungsvereinbarung bleiben unberührt.

3 Verantwortlichkeit und Pflichten des Kunden; Freistellung

3.1 Der Unternehmer hat selbstständig dafür zu sorgen, die Leistung entgegennehmen zu können. Insbesondere ist die Bereitstellung der dazu erforderlichen Hard- und Software durch den Anbieter nicht Vertragsbestandteil. Die Bedienung und Konfiguration der Plattform obliegt allein dem Unternehmer.

3.2 Der Unternehmer ist selbst dafür verantwortlich, seine Kunden über die Notwendigkeit und die Abläufe bei der Registrierung sowie die damit verbundene Datenverarbeitung (siehe auch Ziffer 2.5) zu informieren. Es obliegt dem Unternehmer, sich über die für seinen Betrieb jeweils geltenden Regelungen laufend zu informieren. Diese Regelungen können sich z.B. je nach Branche, Betriebsgröße, Bundesland und Kommune unterscheiden. Soweit der Anbieter auf seiner Website oder durch Verlinkung (bspw. auf die Übersichten von Branchenverbänden wie DEHOGA) Informationen zu solchen Registrierungspflichten bereithält, erfolgt dies ohne Gewähr.

3.3 Zur Klarstellung: Die Erfüllung von Dokumentationspflichten über die Plattform ist nur möglich, soweit die Plattform technisch erreichbar ist und der jeweilige Kunde über ein Smartphone mit QR-Lesefunktion und Internetverbindung verfügt. Es obliegt dem Unternehmer, Vorkehrung für eine alternative Dokumentation zu treffen und vorzuhalten, und diese bei Nichterreichbarkeit der Plattform bzw. bei Kunden ohne Smartphone auch einzusetzen.

3.4 Der Unternehmer zahlt an den Anbieter das vereinbarte Entgelt. Höhe und sonstige Zahlungsmodalitäten ergeben sich aus Ziffer 5 und der jeweiligen Leistungsbeschreibung.

3.5 Der Unternehmer behandelt seine Zugangsdaten und seinen privaten Schlüssel vertraulich und gibt diese nicht an Dritte weiter. Er informiert den Anbieter unverzüglich, wenn er den Verdacht hat, dass Dritte unbefugt Zugriff auf diese Daten haben oder hatten, und ändert in diesen Fällen unverzüglich die betroffenen Passwörter. Der Unternehmer ist dafür verantwortlich, seinen privaten Schlüssel sicher zu verwahren. Bei Verlust des Schlüssels ist ein Zugriff auf den Klartext der

gespeicherten Kunden-Registrierungen nicht mehr möglich, auch und insbesondere nicht für den Anbieter.

3.6 Der Unternehmer räumt dem Anbieter an sämtlichen Inhalten, die er im Rahmen der Nutzung der Plattform auf die Server des Anbieters überträgt, ein einfaches, räumlich und zeitlich unbeschränktes Nutzungsrecht ein, die Inhalte insoweit zu nutzen, wie dies zur Erfüllung des Vertrages mit dem Unternehmer erforderlich ist, insbesondere die Inhalte zu vervielfältigen und sie entsprechend der Einstellungen des Unternehmers sonstigen Dritten (z.B. Besuchern der Plattform) zugänglich zu machen. Der Anbieter ist berechtigt, an seine Erfüllungsgehilfen Unterlizenzen zu erteilen, soweit dies für die Vertragserfüllung erforderlich ist. Im Übrigen ist das Nutzungsrecht nicht übertragbar. Der Anbieter ist berechtigt, über die Dauer des Vertrages hinaus Inhalte des Unternehmers vorzuhalten, soweit dies technisch oder rechtlich erforderlich ist. Insbesondere ist der Anbieter befugt, Sicherungskopien der vom Unternehmer bereitgestellten Inhalte aufzubewahren und solche Informationen vorübergehen oder dauerhaft zu speichern, die für Buchhaltungs-, Dokumentations- und Abrechnungszwecke benötigt werden.

3.7 Der Unternehmer stellt den Anbieter von allen Ansprüchen, Schäden und Kosten (einschließlich Rechtsverteidigungskosten wie insbesondere marktüblicher Rechtsanwaltshonorare) frei, die dadurch entstehen, dass Dritte wegen eines tatsächlichen oder behaupteten Verstoßes des Unternehmers gegen seine vorstehende Pflichten Ansprüche gegen den Anbieter geltend machen.

4 Nutzungsrechte an der Software

4.1 Mit Vertragsbeginn räumt der Anbieter dem Unternehmer das zeitlich auf die Vertragslaufzeit beschränkte, nicht ausschließliche, weltweite, nicht übertragbare, nicht unterlizensierbare Recht ein, die der Plattform zugrunde liegende Software vertragsgemäß als SaaS-Leistung zu nutzen. Zur Klarstellung: Die Software wird ausschließlich bei dem Anbieter betrieben und der Unternehmer ist nicht berechtigt, diese herunterzuladen oder zu installieren oder anderweitig zu vervielfältigen, verbreiten oder nutzen; auch am Quellcode erhält der Unternehmer keine Rechte. Der Unternehmer ist nicht berechtigt, die Software seinerseits zur Erbringungen solcher Leistungen an Dritte zu nutzen, die den Leistungen des Anbieters nach diesem Vertrag ganz oder teilweise entsprechen.

4.2 Von der Rechteeinräumung ausgenommen sind Bestandteile der Software, die für den Unternehmer erkennbar Rechten Dritter (also anderer als der Anbieter und seiner Lizenzgeber) und insbesondere Open Source Lizenzen unterliegen. Als erkennbar gelten insbesondere solche Bestandteile, die vom Anbieter innerhalb der Software oder in überlassenen Textdateien als Inhalte Dritter oder als Open Source-Inhalt offengelegt bzw. gekennzeichnet werden. Solche Bestandteile unterliegen ausschließlich den jeweils für sie geltenden Lizenzen.

5 Vergütung; Kostenloser Starttzeitraum

5.1 Der Unternehmer zahlt für die Nutzung der der Plattform an den Anbieter die sich aus der Leistungsbeschreibung ergebende Vergütung. Soweit die Leistungsbeschreibung einen kostenlosen Startzeitraum vorsieht, erfolgt die Leistungserbringung durch den Anbieter insoweit unentgeltlich.

5.2 Soweit nicht in der Leistungsbeschreibung abweichend vereinbart, erfolgt die Rechnungsstellung jeweils monatlich im Voraus.

5.3 Soweit die Leistungsbeschreibung eine vergünstigte Vergütung für bestimmte Gruppen von Unternehmern (z.B. Mitglieder einer Branche, eines Verbandes, o.ä.) vorsieht, behält sich der Anbieter die Anforderung entsprechender Nachweise und/oder anderweitige Überprüfung (z.B. durch Rückfrage bei dem jeweiligen Verband) vor. Sollten die Voraussetzungen für die Vergünstigung nicht nachgewiesen werden oder wegfallen, behält sich der Anbieter vor, die volle Vergütung auch rückwirkend für solche Zeiträume zu erheben, in denen die Voraussetzungen für die Vergünstigung nicht nachgewiesen sind.

5.3 Alle Beträge sind Nettobeträge und verstehen sich zzgl. Umsatzsteuer in jeweils gesetzlicher Höhe, soweit anfallend. Die in Rechnung gestellten Beträge sind mit Zugang der Rechnung fällig und werden von dem hinterlegten Zahlungsmittel (soweit vorhanden) abgebucht. Die zur Verfügung stehenden Zahlungsmittel ergeben sich aus der Leistungsbeschreibung.

5.4 Im Falle des Verzugs stehen dem Anbieter die gesetzlichen Rechte zu. Ziffer 2.8 bleibt unberührt.

6 Laufzeit; Kündigung

6.1 Der Vertrag wird auf unbestimmte Zeit geschlossen und kann von jeder Partei mit einer Frist von zwei Wochen vom Monatsende ordentlich gekündigt werden.

6.2 Das gesetzliche Recht zur außerordentlichen fristlosen Kündigung aus wichtigem Grund bleibt unberührt.

6.3 Jede Kündigung bedarf der Textform.

6.4 Vor Wirksamwerden der Kündigung auf der Plattform erfasste Kunde-Registrierungen bleiben auch nach der Kündigung noch bis zu ihrer turnusmäßigen Löschung abrufbar.

7 Gewährleistung

7.1 Soweit der Unternehmer in Ansehung eines Teils der Leistung gesetzliche Gewährleistungsansprüche dem Grunde nach zustehen (d.h. insbesondere soweit es sich nicht um einen Dienst im Sinne der § 611 ff. BGB handelt und soweit die Leistung nicht unentgeltlich erbracht wird), wird der Anbieter zunächst nach seiner Wahl und auf seine Kosten durch Behebung von Mängeln oder Neuerbringung der Leistung innerhalb einer vom Unternehmer zu setzenden angemessenen Frist nacherfüllen. Die Frist muss mindestens drei Nacherfüllungsversuche ermöglichen.

7.2 Ein Fehler liegt dann vor, wenn die Plattform die in der Leistungsbeschreibung abschließend angegebenen Funktionen nicht erfüllt bzw. wenn diese Funktionen fehlerhafte Ergebnisse liefern, so dass die Nutzung der Plattform unmöglich oder erheblich eingeschränkt ist.

7.3 Bei der Meldung auftretender Fehler hat der Unternehmer diese detailliert zu beschreiben und alle dem Unternehmer vorliegenden Informationen beizufügen, die erforderlich oder nützlich sind, damit der Anbieter den Fehler analysieren, reproduzieren und beheben kann.

7.4 Als Nachbesserung gilt auch die Bereitstellung von Nutzungsanweisungen, mit denen der Unternehmer aufgetretene Fehler zumutbar umgehen kann, um die Plattform vertragsgemäß zu nutzen.

7.5 Schlägt die Nacherfüllung endgültig fehl, kann der Unternehmer nach Maßgabe dieser Ziffer 7.5 den Vertrag kündigen, die Vergütung mindern oder nach Maßgabe der Ziffer 8 Schadenersatz verlangen. Sonstige Ansprüche, insbesondere ein etwaiges Selbstvornahmerecht, sind ausgeschlossen. Das Recht zur Minderung ist für jeden Monat in dem der Fehler fortbesteht auf die Höhe der den mangelhaften Leistungsteil betreffenden monatlichen Vergütung beschränkt. Erreicht die Minderung nach dieser Ziffer in zwei aufeinander folgenden Monaten den genannten Höchstbetrag, kann der Unternehmer den Vertrag ohne Einhaltung einer Frist kündigen.

8 Haftung

8.1 Soweit der Anbieter eine Leistung unentgeltlich erbringt, haftet er nach Maßgabe der gesetzlichen Vorschriften nur für Vorsatz und grobe Fahrlässigkeit.

8.2 Soweit der Anbieter eine Leistung entgeltlich erbringt, haftet er abschließend wie folgt.

8.2.1 Die gesetzliche Haftung des Anbieters für Vorsatz und grobe Fahrlässigkeit sowie bei Schäden aus der Verletzung des Lebens, des Körpers oder der Gesundheit ist unbeschränkt.

8.2.2 In Fällen einfacher Fahrlässigkeit außer in den Fällen der Ziffer 8.1 haftet der Anbieter nur bei Verletzung einer wesentlichen Vertragspflicht. Eine wesentliche Vertragspflicht im Sinne dieser Ziffer ist eine Pflicht, deren Erfüllung die Durchführung des Vertrages erst ermöglicht und auf deren Erfüllung sich der Unternehmer deswegen regelmäßig verlassen darf.

8.2.3 Der Anbieter haftet im Fall von Ziffer 8.2.2 weder für mangelnden wirtschaftlichen Erfolg, noch für entgangenen Gewinn oder für mittelbare Schäden.

8.2.4 Die Haftung gemäß der vorstehenden Ziffer 8.2.2 ist pro Kalenderjahr beschränkt auf den Betrag der in diesem Kalenderjahr vom Unternehmer an den Anbieter gezahlten Vergütung.

8.3 Die Haftungsbeschränkungen gelten zugunsten der gesetzlichen Vertreter, Mitarbeiter, Beauftragten und Erfüllungsgehilfen des Anbieters und dessen Subunternehmer entsprechend.

8.4 Eine etwaige Haftung des Anbieters für gegebene Garantien (die ausdrücklich als solche bezeichnet sein müssen um Garantien im Rechtssinne zu sein) und für Ansprüche auf Grund des Produkthaftungsgesetzes bleibt unberührt.

8.5 Eine weitergehende Haftung des Anbieters ist ausgeschlossen. Insbesondere ausgeschlossen ist die verschuldensunabhängige Haftung für anfängliche Mängel der Plattform gem. § 536a Abs. 1, 1. Alt. BGB.

9 AGB-Änderungen

Diese AGB können durch entsprechende Vereinbarung wie nachfolgend beschrieben geändert werden, wenn die Änderung wegen einer Änderung des geltenden Rechts (einschließlich der Rechtsprechung) oder aus ähnlich zwingenden Gründen nötig ist und die Hauptleistungspflichten der Parteien dadurch nicht zum Nachteil des Unternehmers verändert werden: Der Anbieter übermittelt die geänderten Bedingungen vor dem geplanten Inkrafttreten in Textform und weist auf die Neuregelungen sowie das Datum des geplanten Inkrafttretens gesondert hin. Zugleich wird der Anbieter dem Unternehmer eine angemessene, mindestens vier Wochen lange Frist für die Erklärung einräumen, ob er die geänderten AGB für die weitere Inanspruchnahme der Leistungen akzeptiert. Erfolgt innerhalb dieser Frist, welche ab Erhalt der Nachricht in Textform zu laufen beginnt, keine Erklärung, so gelten die geänderten Bedingungen als vereinbart. Der Anbieter wird den Unternehmer in der Änderungsmitteilung gesondert auf diese Rechtsfolge, d.h. das Widerspruchsrecht, die Widerspruchsfrist und die Bedeutung des Schweigens hinweisen.

10 Schlussbestimmungen

10.1 Dieser Vertrag unterliegt deutschem Recht unter Ausschluss des UN-Kaufrechts. Ausschließlicher Gerichtsstand ist München.

10.2 Der Unternehmer kann gegen Forderungen des Anbieters nur dann aufrechnen oder ein Zurückbehaltungsrecht geltend machen, wenn die Gegenforderung unbestritten oder rechtskräftig zuerkannt ist oder in einem synallagmatischen Verhältnis zu dem jeweils betroffenen Anspruch steht.

10.3 Abweichungen von diesen Geschäftsbedingungen im Einzelfall bedürfen der Schriftform. Dies gilt auch für einen Verzicht auf das Schriftformerfordernis. Zur Klarstellung: Die Möglichkeit zur Änderung der Geschäftsbedingungen nach Ziffer 10 oder durch elektronische Zustimmung des Unternehmers (z.B. Zustimmung zu neuer

Version der Geschäftsbedingungen innerhalb des Accounts) bleibt unberührt. Mündliche Nebenabreden bestehen nicht.

Stand: 28 März 2021

Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 Abs. 3 Datenschutz-Grundverordnung (DSGVO)

Zwischen dem Verantwortlichen

- nachfolgend Auftraggeber genannt –

und

dem Auftragsverarbeiter (Anbieter)

Darfichrein GmbH

Türkenstr, 7

80333 München

- nachfolgend Auftragnehmer genannt –

Präambel

Diese Vereinbarung konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz in Bezug auf Auftragsverarbeitung, die sich aus der Leistungsbeschreibung auf www.darfichrein.de und der AGB (im Folgenden „Vertrag“ genannt) ergibt. Sie findet Anwendung auf alle Tätigkeiten, die mit dem Vertrag in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer beauftragte Dritte personenbezogene Daten („Daten“) des Auftraggebers verarbeiten („Auftragsverarbeitung“).

1. Gegenstand, Dauer und Spezifizierung der Auftragsverarbeitung

1.1 Aus dem Vertrag ergeben sich Gegenstand, Dauer, Umfang, Art und Zweck der Auftragsverarbeitung. sowie die Art der Daten und die Kategorien betroffener Personen. Dies gilt auch, sofern die jeweiligen vertraglichen Vereinbarungen nicht ausdrücklich Bezug nehmen auf diese Vereinbarung zur Auftragsverarbeitung. Soweit sich die Art der Daten und die Kategorie der betroffenen Personen nicht aus dem Vertrag ergeben, ist der Auftragnehmer berechtigt, diese dem Auftraggeber auf Antrag in elektronischer Form zugänglich zu machen:

https://static.darfichrein.de/Spezifizierung_Datenverarbeitung.pdf

Die Verarbeitung kann dabei insbesondere folgende Arten der Verarbeitung umfassen: das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, das Verschlüsseln, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, die Verbreitung oder eine andere Form der Bereitstellung, der Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung von Daten.

Die Laufzeit dieser Vereinbarung richtet sich grundsätzlich nach der Laufzeit des zugrundeliegenden Vertrages und gilt solange eine Vertragsbeziehung zwischen dem Auftraggeber und dem Auftragnehmer besteht. Eine Kündigung dieser Vereinbarung kann nur aus einem wichtigen datenschutzrechtlichen Grund erfolgen. Keiner Kündigung dieser Vereinbarung bedarf es im Falle der Beendigung der Vertragsbeziehung zwischen Auftraggeber und Auftragnehmer.

1.2 Die dieser Vereinbarung zugrundeliegenden Leistungen werden ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Jede Verlagerung der Leistungen oder von Teilarbeiten dazu in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

2. Rechte und Pflichten des Auftragnehmers

2.1 Der Auftragnehmer verarbeitet Daten von betroffenen Personen ausschließlich im Rahmen der getroffenen Vereinbarungen und der dokumentierten Weisungen des Auftraggebers sowie entsprechend den datenschutzrechtlichen Regelungen, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragnehmer unterliegt, verpflichtet ist. In einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 Satz 2 lit. a DSGVO).

Die Weisungen werden anfänglich durch den Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in einem elektronischen Format (Textform) an die vom Auftragnehmer bezeichnete Stelle durch einzelne Weisungen geändert, ergänzt oder ersetzt werden. Weisungen, die im Vertrag nicht vorgesehen sind, werden als Antrag auf Leistungsänderung behandelt.

2.2 Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstößt. Der Auftragnehmer darf die Umsetzung der Weisung solange aussetzen, bis die Parteien eine einvernehmliche Lösung gefunden haben.

2.3 Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird insbesondere technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers treffen, die den Anforderungen des Art. 32 DSGVO genügen. Diese technischen und organisatorischen Maßnahmen sind in der Anlage TOM beschrieben. Der Auftragnehmer wird diese technischen und organisatorischen Maßnahmen so treffen, dass die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sichergestellt sind. Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei jedoch sichergestellt sein muss, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird. Der Auftragnehmer verwendet die zur Verarbeitung überlassenen Daten für keine anderen und insbesondere nicht für eigene Zwecke. Duplikate

der Daten werden, ohne dass sie im Auftrag oder in diesem Vertrag geregelt sind, nicht erstellt.

2.4 Der Auftragnehmer unterstützt den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen in angemessener Weise bei der Erfüllung von Anfragen und Ansprüchen betroffener Personen gem. Kapitel III der DSGVO (Art. 28 Abs. 3 lit. e DSGVO) und unterstützt den Auftraggeber bei der Einhaltung der in den Art. 32 bis 36 DSGVO genannten Pflichten, wie etwa bei erforderlichen Datenschutz-Folgenabschätzungen (Art. 28 Abs. 3 Satz 2 lit. f DSGVO).

2.5 Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeitern und anderen für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb der Weisung zu verarbeiten. Ferner gewährleistet der Auftragnehmer, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheit unterliegen. Die Vertraulichkeits-/Verschwiegenheits-pflicht besteht auch nach Beendigung dieser Vereinbarung fort.

2.6 Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm im Rahmen des Auftragsverhältnisses Verletzungen des Schutzes personenbezogener Daten des Auftraggebers bekannt werden. Der Auftragnehmer trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Personen.

2.7 Der Auftragnehmer nennt dem Auftraggeber Ansprechpartner für im Rahmen dieser Vereinbarung anfallende Weisungen sowie einen etwaigen Beauftragten für den Datenschutz. Ein Wechsel oder eine längerfristige Verhinderung der Ansprechpartner ist dem Auftragnehmer unverzüglich anzuzeigen.

2.8 Der Auftragnehmer berichtigt, löscht oder sperrt die vertragsgegenständlichen Daten, wenn der Auftraggeber dies anweist und dies vom Weisungsrahmen umfasst ist, es sei denn, die Weisung widerspricht etwaigen gesetzlichen oder vertraglichen Aufbewahrungspflichten. Ist eine datenschutzkonforme Löschung, Sperrung oder eine entsprechende Einschränkung der Datenverarbeitung nicht möglich, übernimmt der Auftragnehmer die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien auf Grund einer Einzelbeauftragung durch den Auftraggeber oder gibt diese Datenträger an den Auftraggeber zurück. In besonderen, vom Auftraggeber zu bestimmenden Fällen, erfolgt eine Aufbewahrung bzw. Übergabe mit entsprechenden Schutzmaßnahmen. Für vorgenannte Leistungen kann der Auftragnehmer eine angemessene Vergütung verlangen.

2.9 Nach Auftragsende sind Daten, Datenträger sowie sonstige Materialien auf Verlangen des Auftraggebers entweder zurückzugeben oder zu löschen, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung besteht. Entstehen zusätzliche Kosten durch abweichende Vorgaben bei der Rückgabe oder Löschung der Daten, so trägt diese der Auftraggeber. **Grundsätzlich werden die personenbezogenen Daten der Gäste den gesetzlichen Vorgaben entsprechend nach Ablauf von 4 Wochen automatisch gelöscht.**

2.10 Im Falle einer Inanspruchnahme des Auftraggebers durch eine Person hinsichtlich etwaiger Schadensersatzansprüche nach Art. 82 DSGVO verpflichtet sich der Auftragnehmer, den Auftraggeber bei der Abwehr der Ansprüche im Rahmen seiner Möglichkeiten zu unterstützen.

3. Rechte und Pflichten des Auftraggebers

3.1 Der Auftraggeber ist im Rahmen dieser Vereinbarung für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Beurteilung der Rechtmäßigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DSGVO, für die Datenweitergabe an den Auftragnehmer sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DSGVO allein verantwortlich („Verantwortlicher“ im Sinne des Art. 4 Nr. 7 DSGVO).

3.2 Der Auftraggeber hat den Auftragnehmer unverzüglich zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

3.3 Im Falle einer Inanspruchnahme des Auftragnehmers durch eine Person hinsichtlich etwaiger Schadensersatzansprüche nach Art. 82 DSGVO verpflichtet sich der Auftraggeber, den Auftragnehmer bei der Abwehr der Ansprüche im Rahmen seiner Möglichkeiten zu unterstützen.

3.4 Der Auftraggeber ist verpflichtet, alle im Rahmen der Vertragsbeziehung erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieser Vereinbarung bestehen.

4. Anfragen betroffener Personen

Wendet sich eine betroffene Person mit Forderungen zur Beantwortung einer Auskunft, zur Berichtigung oder Löschung gemäß Art. 15 ff. DSGVO an den Auftragnehmer, wird der Auftragnehmer die betroffene Person an den Auftraggeber verweisen, sofern eine Zuordnung an den Auftraggeber auf Basis der Angaben der betroffenen Person möglich ist. Gemäß Ziffer 2.4 dieser Vereinbarung unterstützt der Auftragnehmer den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen. Der Auftragnehmer haftet nicht, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird. Der Auftragnehmer ist berechtigt, für vorgenannte Leistungen eine angemessene Vergütung vom Auftraggeber zu verlangen.

5. Kontrollrechte des Auftraggebers und Nachweismöglichkeiten des Auftragnehmers

5.1 Der Auftragnehmer bietet hinreichende Garantien dafür, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen der DSGVO erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet. 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 Auftragnehmer geeignete

technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

Der Auftragnehmer kann dem Auftraggeber die Einhaltung der in dieser Vereinbarung niedergelegten Pflichten mit geeigneten Mitteln nachweisen. Diese Nachweise können Ergebnisse eines Selbstaudits, Zertifikate zu Datenschutz und/oder Informationssicherheit (z.B. ISO 27001), Zertifikate gemäß Art. 42 DSGVO oder aktuelle Testate und/oder Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren), genehmigte Verhaltensregeln (Art. 40 DSGVO) oder verbindliche interne Datenschutzvorschriften (Art. 47 DSGVO) sein.

5.2 Sofern einschlägig verpflichtet sich der Auftragnehmer, den Auftraggeber über den Ausschluss von genehmigten Verhaltensregeln nach Art. 41 Abs. 4 DSGVO und den Widerruf einer Zertifizierung nach Art. 42 Abs. 7 DSGVO unverzüglich zu informieren.

5.3 Der Auftraggeber ist berechtigt, sich vor Beginn der Verarbeitung und sodann regelmäßig in angemessener Weise von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen sowie der in dieser Vereinbarung festgelegten Verpflichtungen zu überzeugen.

5.4 Sollten im Einzelfall Inspektionen durch den Auftraggeber oder einen von ihm beauftragten Prüfer erforderlich sein, werden diese nach vorheriger Anmeldung unter Berücksichtigung einer angemessenen Vorlauffrist zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs durchgeführt. Der Auftragnehmer hat die Inspektion von der Unterzeichnung einer Verschwiegenheitserklärung abhängig zu machen. Der Auftraggeber stellt sicher, dass der Prüfer in keinem Wettbewerbsverhältnis zu dem Auftragnehmer steht.

5.5 Sollte eine Datenschutzaufsichtsbehörde oder eine sonstige hoheitliche Aufsichtsbehörde eine Inspektion vornehmen, gilt grundsätzlich Ziffer 5.4 entsprechend. Die Unterzeichnung einer Verschwiegenheitsverpflichtung ist nicht erforderlich, wenn diese Aufsichtsbehörde einer berufsrechtlichen oder gesetzlichen Verschwiegenheit unterliegt.

6. Subunternehmer (weitere Auftragsverarbeiter)

6.1 Ein Subunternehmerverhältnis liegt vor, wenn der Auftragnehmer weitere Auftragnehmer mit der ganzen oder einer Teilleistung der im Vertrag vereinbarten Leistung beauftragt.

Der Auftraggeber erteilt dem Auftragnehmer die allgemeine Genehmigung, weitere Subunternehmer im Sinne des Art. 28 DSGVO einzusetzen.

Der Auftragnehmer trägt Sorge dafür, dass er die Subunternehmer unter besonderer Berücksichtigung der Eignung der von diesen getroffenen technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DSGVO sorgfältig auswählt.

Der Auftragnehmer teilt dem Auftraggeber die bereits bei Abschluss dieses Vertrags bestehenden Subunternehmer mit. Der Auftragnehmer setzt die Anstalt der Kommunale Datenverarbeitung in Bayern (AKDB) als zentralen Subunternehmer ein. Die Kontaktdaten der Endanwender (Gäste, Besucher, usw.) werden verschlüsselt, direkt und ohne Umwege an das Rechenzentrum der AKDB übermittelt und dort gespeichert.

Für die Auslieferung der statischen Daten setzt der Auftragnehmer die Hetzner Online GmbH (Industriestr. 25, 91710 Gunzenhausen, Deutschland) als Subunternehmer ein. Im Rechenzentrum der Hetzner Online Gmbh läuft das Frontend der Darfichrein-Anwendung. Das heißt, dass über die Hetzner Online GmbH die Oberflächen der Anwendung ausgeliefert werden. Dabei werden Nutzungsdaten der Besucher:innen und Gäste (wie z.B. IP-Adressen) verarbeitet. Die Infrastruktur, der Betrieb und Kundensupport der Rechenzentren der Hetzner Online GmbH verfügt über die hochwertige Zertifizierung ISO/IEC 27001:2013.
Der Auftragnehmer informiert den Auftraggeber, wenn er eine Änderung bei dem Einsatz von Subunternehmern beabsichtigt.

6.2 Nimmt der Auftragsverarbeiter die Dienste eines weiteren Auftragsverarbeiters in Anspruch, so werden diesem im Wege eines Vertrags oder eines anderen Rechtsinstruments dieselben Datenschutzpflichten auferlegt, die in dem Vertrag oder anderen Rechtsinstrument zwischen dem Verantwortlichen und dem Auftragsverarbeiter festgelegt sind, wobei insbesondere hinreichende Garantien dafür geboten werden müssen, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den datenschutzrechtlichen Anforderungen erfolgt.

6.3 Der Auftragnehmer haftet gegenüber dem Auftraggeber dafür, dass die von ihm eingesetzten Subunternehmer den Datenschutzpflichten nachkommen, die ihm durch den Auftragnehmer vertraglich auferlegt wurden.

6.4 Eine Beauftragung von Subunternehmern in Drittstaaten darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

6.5 Nicht als Subunternehmerverhältnis im Sinne dieser Regelung sind solche Leistungen zu verstehen, die der Auftragnehmer bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Hierzu zählen z.B. Telekommunikationsleistungen, Wartung und Benutzerservice (wenn kein Zugriff auf personenbezogene Daten des Auftraggebers erfolgt), Reinigungskräfte, Prüfer oder die Entsorgung von Datenträgern. Die Einbindung von Entsorgungsunternehmen ist jedoch anzeigepflichtig, wenn der Kern der Beauftragung die Entsorgung von Dokumenten/Datenträgern, welche Daten des Auftraggebers enthalten, beinhaltet. Der Auftragnehmer wird auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen treffen und sich Kontrollmaßnahmen vorbehalten, um den Schutz und die Sicherheit der Daten des Auftraggebers zu gewährleisten.

7. Haftung und Schadensersatz

Die Vertragsparteien haften entsprechend den einschlägigen gesetzlichen Bestimmungen bzw. gegenüber betroffenen Personen gemäß Art. 82 DSGVO.

8. Schlussbestimmungen

8.1 Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen und Beteiligten unverzüglich darüber informieren, dass die

Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als „Verantwortlichem“ im Sinne der Datenschutz-Grundverordnung liegen.

8.3 Änderungen und Ergänzungen dieser Vereinbarung und aller seiner Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – erfolgen in Schriftform oder auch in einem elektronischen Format (Textform) mit dem ausdrücklichen Hinweis darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Vereinbarung handelt. Vorgenannte Änderungen und Ergänzungen gelten als von der jeweils anderen Partei als genehmigt, wenn nicht binnen sechs Wochen ab Zugang der Änderungs- oder Ergänzungsmitteilung schriftlich widersprochen wird.

8.4 Sollten einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise unwirksam oder undurchführbar sein oder werden, so ist die Wirksamkeit der übrigen Regelungen hiervon nicht betroffen. In diesem Falle werden die Parteien einvernehmlich eine neue Regelung oder Ergänzung der bestehenden Regelung vereinbaren, die die unwirksame oder undurchführbare Regelung in einer Art und Weise ersetzt bzw. ergänzt, die der ursprünglich von den Parteien bei Abfassung dieser Anlage beabsichtigten Regelung am nächsten kommt, hätten sie denn die Unwirksamkeit oder Undurchführbarkeit bedacht. Dies gilt auch für Regelungslücken.

Ort, Datum
München, 28.03.2020

Auftragnehmer
Darfichrein GmbH
Dominik Wörner

Technische und organisatorische Maßnahmen (TOM) gemäß Art. 32 Abs. 1 DSGVO

Die Darfichrein GmbH entwickelt und vermarktet die Anwendung „darfichrein.de“. Die Wirksamkeit der TOM der Darfichrein GmbH wird regelmäßig überprüft. Die Darfichrein GmbH setzt die Anstalt für Kommunale Datenverarbeitung in Bayern (AKDB) als Subunternehmen ein. Konkret betreibt die AKDB das Backend (Datenebene) der Anwendung in ihrem Rechenzentrum.

Technische und organisatorische Maßnahmen der Darfichrein GmbH

1 Vertraulichkeit

1.1 Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen zu verwehren, mit denen personenbezogene Daten verarbeitet oder genutzt werden:

Hier sind die TOMs des Subunternehmers AKDB einschlägig.

1.2 Zugangskontrolle

Maßnahmen, die geeignet sind, zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können:

- ⇨ Login mit Benutzername und Passwort
- ⇨ Detaillierte Passwortregelung
- ⇨ Erzwungene Passwortkomplexität

Unser Subunternehmer AKDB ergreift in diesem Bereich weitere TOM.

1.3 Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können:

- ⇨ Regelmäßige Aktualisierung der Sicherheitskonzepte
- ⇨ Vergabe differenzierter Berechtigungsstufen innerhalb der Verfahren
- ⇨ Protokollierung von Veränderungen oder Löschungen der Daten
- ⇨ Datenträgervernichtung gemäß DIN 66399

1.4 Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

- ⇨ Festlegung von Datenbankrechten
- ⇨ Steuerung über Berechtigungskonzept

Unser Subunternehmer AKDB ergreift in diesem Bereich weitere TOM.

1.5 Verschlüsselung

Maßnahmen, die gewährleisten, dass personenbezogene Daten nicht im Klartext persistiert werden.

- ⇨ Besuchsdaten werden mit dem kryptografischen Verfahren RSA (4096 Bit Schlüssellänge) verschlüsselt. Der Schlüssel ist hierbei der öffentliche Schlüssel des besuchten Unternehmens.
- ⇨ Der private Schlüssel ist nur dem besuchten Unternehmen bekannt und wird weder vom Auftragnehmer (Darfichrein GmbH) noch vom Subunternehmer persistiert.

2 Integrität

2.1 Weitergabekontrolle

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 welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

- ⇨ Datenübermittlung über gesicherte Datenverbindungen

2.2. Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

- ⇨ Technische Protokollierung der Eingabe, Änderung und Löschung von Daten
- ⇨ Keine Modifizierbarkeit der Protokolle
- ⇨ Kontrolle der Protokolle

3 Verfügbarkeit und Belastbarkeit

3.1 Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Hier sind die TOM des Subunternehmers AKDB einschlägig.

Technische und organisatorische Maßnahmen der AKDB

Die regelmäßige Überprüfung der Wirksamkeit der Technischen und Organisatorischen Maßnahmen des Subunternehmers AKDB erfolgt mindestens jährlich im Rahmen der vorhandenen ISO 27001-Zertifizierung auf Basis von BSI IT-Grundschutz.

1 Vertraulichkeit

1.1 Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen zu verwehren, mit denen personenbezogene Daten verarbeitet oder genutzt werden:

- ⇨ Mehrstufigen Zutrittsschutz
  - Besucherkontrolle am Empfang am Standort des Primärrechenzentrums
  - Gesonderte Zutrittsberechtigung zu allen sicherheitsrelevanten Räumen mittels Chipkarte und zusätzlicher Codeeingabe am Zugangsterminal
- ⇨ Regelmäßige Überprüfung der Zutrittsberechtigungen
- ⇨ Kontrollierte Schlüsselvergabe
- ⇨ Videoüberwachung des Gebäudes einschließlich des Zugangs sowie in den Storage- und CPU-Räumen im Primärrechenzentrum
- ⇨ Außenhautsicherung des Primärrechenzentrumgebäudes an kritischen Stellen durch einbruchhemmende Spezialfenster und Türen
- ⇨ Außenhautsicherung des Primärrechenzentrumgebäudes kombiniert mit Einbruchmeldeanlage mit Alarmweiterleitung zur Polizei
- ⇨ Besucher in Begleitung durch Mitarbeiter

1.2 Zugangskontrolle

Maßnahmen, die geeignet sind, zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können:

- ⇨ Login mit Benutzername und Passwort
- ⇨ Detaillierte Passwortregelung
- ⇨ Erzwungene Passwortkomplexität
- ⇨ Regelmäßigen technisch vorgegebenen Passwortwechsel
- ⇨ Sperrung der Benutzerkennung nach mehrmaliger Fehleingabe
- ⇨ Detaillierte Security-Policies für die Produktionsumgebung und deren regelmäßige Überprüfung
- ⇨ Einsatz von Firewall-Systemen mit eigener Security-Policy
- ⇨ Zusätzlicher Einsatz von Intrusion-Prevention-Systemen
- ⇨ Anti-Viren-Software
- ⇨ Mobile Device Management
- ⇨ Verschlüsselung von Notebooks

1.3 Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können:

- ⇨ Regelmäßige Aktualisierung der Sicherheitskonzepte
- ⇨ Vergabe differenzierter Berechtigungsstufen innerhalb der Verfahren
- ⇨ Protokollierung von Veränderungen oder Löschungen der Daten
- ⇨ Datenträgervernichtung gemäß DIN 66399

1.4 Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

- ⇨ Trennung von Produktiv- und Testumgebung
- ⇨ Mandantenfähigkeit relevanter Anwendungen
- ⇨ Festlegung von Datenbankrechten
- ⇨ Steuerung über Berechtigungskonzept

2 Integrität

2.1 Weitergabekontrolle

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 welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

- ⇨ Datenübermittlung über gesicherte Datenverbindungen
- ⇨ Verschlüsselung der Daten beim Transport auf Datenträgern

2.2. Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

- ⇨ Technische Protokollierung der Eingabe, Änderung und Löschung von Daten
- ⇨ Keine Modifizierbarkeit der Protokolle
- ⇨ Kontrolle der Protokolle

3 Verfügbarkeit und Belastbarkeit

3.1 Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

- ⇨ Hohe Hardwarequalität der Systeme mit abgeschlossenen Wartungsverträgen mit kurzen Reaktionszeiten seitens der Hardwarehersteller
- ⇨ Redundante Server-Systeme
- ⇨ Speicherung der Daten auf eigenen Storage-Systemen mit Raid-Technik und Spareplatten, zu großen Teilen in Clustertechnik ausgeführt
- ⇨ Aufbewahrung von längerfristigen Sicherungsbeständen im Tresor
- ⇨ Regelmäßig aktualisierten Virenschutz
- ⇨ Redundante Firewall-Systeme
- ⇨ Redundante Internetanschlüsse
- ⇨ Redundanter Behördennetzanschluss (BYBN)
- ⇨ Mobile Arbeitsplätze mit gesichertem Zugang für Mitarbeiter in den Bereichen Operating, Produktionsdurchführung und Systemadministration zum Zugang auch außerhalb der üblichen Arbeitszeiten
- ⇨ Gebäudetechnische Maßnahmen (Feuer- Rauchmeldeanlagen, Feuerlöscher, Klimatisierung, USV)
- ⇨ Regelmäßiges Patchen der Systeme (Funktions- und Sicherheitspatches)
- ⇨ Regelmäßige Backup- und Recovery-Maßnahmen
- ⇨ Regelmäßige Tests zur Datenwiederherstellung