Nutzungsbedingungen

Nutzungsbedingungen der apotec® Kühlschranküberwachung

Gegenstand dieser Nutzungsbedingungen ist der von der WEPA APOTHEKENBEDARF GmbH & Co. KG (nachfolgend „WEPA“) bereitgestellte apotec® Kühlschranküberwachung (nachfolgend „apotec® Kühlschranküberwachung“)

1. Geltungsbereich

1.1 Die nachfolgenden Nutzungsbedingungen gelten ausschließlich für die Nutzung von apotec® Kühlschranküberwachung. Anbieter von Kühlschranküberwachung ist die WEPA APOTHEKENBEDARF GmbH & Co. KG, Am Fichtenstrauch 6-10, 56204 Hillscheid, vertreten durch den Geschäftsführer Dr. Christian Ciesielski.

1.2 apotec® Kühlschranküberwachung richtet sich ausschließlich an Nutzer, die in Ausübung ihrer gewerblichen oder selbstständigen beruflichen Tätigkeit handeln. Andere Nutzer, insbesondere Verbraucher i.S.v. § 13 BGB sind von der Nutzung von apotec® Kühlschranküberwachung ausgeschlossen.

2. Gegenstand von apotec® Kühlschranküberwachung

2.1 apotec® Kühlschranküberwachung ist ein digitaler cloudbasierter Service, der es ermöglicht, den Schaltzustand von Komponenten sowie Alarmzustände und Temperaturen von ein oder mehreren professionellen Kühl- und Gefriergräten aufzuzeichnen und visuell in einer browserbasierten Anwendung darzustellen. Im Weiteren können mit Kühlschranküberwachung Messgrößen, mittels externer Sensorik, die in verschiedenen Varianten als Zubehör zum apotec® Kühlschranküberwachung-System erworben werden kann, erfasst und dargestellt werden.

3. Nutzungsrecht

3.1 Der Nutzer wird nach Maßgabe dieser Nutzungsbedingungen ausschließlich gegenüber WEPA zur Nutzung von apotec® Kühlschranküberwachung berechtigt. Das Nutzungsrecht ist ein gerätebezogenes, einfaches, nicht ausschließliches, nicht übertragbares, zeitlich gemäß Ziffer 5.1 beschränktes Nutzungsrecht (nachfolgend „apotec® Kühlschranküberwachung Lizenz“)

4. Nutzungsvoraussetzungen und Pflichten des Nutzers

4.1 Um apotec® Kühlschranküberwachung nutzen zu können benötigt der Nutzer auf seine Kosten

· ein für apotec® Kühlschranküberwachung geeignetes Kühl- und/oder Gefriergerät,

· RS485-Stecker und RS485-Adapter zur Vernetzung des Kühl- und/oder Gefriergeräts,

· eine gültige apotec® Kühlschranküberwachung Lizenz für das jeweilige Kühl- und/oder Gefriergerät und

· ein aktives WEPA Account Konto.

4.2 Der Nutzer verpflichtet sich, nur von WEPA für apotec® Kühlschranküberwachung zugelassene Kühl- und/ oder Gefriergeräte zu registrieren und seine Kontaktdaten im Nutzerprofil von apotec® Kühlschranküberwachung stets auf dem aktuellen Stand zu halten.

4.3 apotec® Kühlschranküberwachung darf nur mit von WEPA für apotec® Kühlschranküberwachung freigegebenen Kühl- und/ oder Gefriergeräten verwendet werden, die innerhalb der europäischen Union, EFTA-Staaten oder dem Vereinigten Königreich aufgestellt sind und dort verwendet werden.

4.4 Die von WEPA für apotec® Kühlschranküberwachung freigegebenen Kühl- und/oder Gefriergeräte dürfen ausschließlich mit dem von WEPA zugelassenen Vernetzungslösungen vernetzt werden.

4.5 Der Nutzer darf apotec® Kühlschranküberwachung nicht missbräuchlich verwenden, insbesondere darf er keine technischen Beschränkungen von apotec® Kühlschranküberwachung umgehen oder gesetzwidrige Zwecke verfolgen.

5. Vertragslaufzeit

5.1 Der Vertrag beginnt mit der Aktivierung des Lizenzschlüssels in der apotec® Kühlschranküberwachung und weist je nach gewähltem Abonnement eine Vertragslaufzeit von 12 oder 36 Monaten auf. Die im Einzelfall für den Nutzer geltende Vertragsdauer ergibt sich aus der Auftragsbestätigung. Er verlängert sich jeweils um die oben aufgeführte Laufzeit, wird er nicht mit einer Kündigungsfrist von vier Wochen zu jeweiligen Vertragsende gekündigt.

5.2 Die Möglichkeit einer fristlosen Kündigung aus wichtigem Grund bleibt unberührt. Ein wichtiger Grund, der WEPA zur fristlosen Kündigung berechtigt, liegt insbesondere vor, wenn

5.2.1 der Nutzer Nutzungsrechte von WEPA dadurch verletzt, dass er apotec® Kühlschranküberwachung über das nach diesen Nutzungsbedingungen oder den ebenfalls abzuschließenden Lizenzbedingungen gestattete Maß hinaus nutzt und die Verletzung auf eine Abmahnung von WEPA hin nicht innerhalb angemessener Frist abstellt;

5.2.2 der Nutzer mit der Zahlung der geschuldeten Vergütung für zwei oder mehr Monate in Verzug ist;

5.2.3 der Nutzer in seinen wirtschaftlichen Verhältnissen wesentliche Einbußen erleidet oder zu erleiden droht, insbesondere, wenn der Kunde selbst Antrag auf Eröffnung des Insolvenzverfahrens über sein Vermögen stellt oder das Insolvenzverfahren über sein Vermögen eröffnet wird;

5.2.4 der Kooperationspartner Liebherr-Hausgeräte Vertriebs- und Service GmbH die mit WEPA vereinbarten Leistun-

gen nicht mehr gegenüber WEPA erbringt (z.B. wegen Kündigung der Vertragsbeziehung) und WEPA damit die geschuldete Leistung nicht mehr anbieten kann.

5.3 Die Kündigungserklärungen zu ihrer Wirksamkeit der Textform. Die Einhaltung dieser Form ist Voraussetzung für die Wirksamkeit der Kündigung.

5.4 WEPA wird mit Beendigung des Vertrages den Dienst in der WEPA-Cloud deaktivieren und die Zugangsberechtigung des Nutzers zu dem Dienst aufheben.

6. Nutzungsentgelt

6.1 Die vom Nutzer zu zahlende Vergütung ergibt sich aus der Auftragsbestätigung Sämtliche Preise verstehen sich in EUR zzgl. der gesetzlichen Umsatzsteuer.

6.2 Die Zahlungsmodalitäten ergeben sich aus der Auftragsbestätigung.

6.3 WEPA kann das Nutzungsentgelt gem. Ziff. 6.1 nach billigem Ermessen (§ 315 Abs. 3 BGB) der Entwicklung der Kosten anpassen, die für die Preisberechnung maßgeblich sind. Maßgeblich für die Preiskalkulation sind insbesondere die Lizenzentgelte, die WEPA für den Betrieb der apotec® Kühlschranküberwachung zu entrichten hat. WEPA wird dem Nutzer etwaige Erhöhungen der Vergütung rechtzeitig, spätestens 3 Monate vor dem Inkrafttreten in Textform mitteilen. Eine Preiserhöhung darf die bisherige Vergütung nicht um mehr als 10 % überschreiten.

Im Falle einer Preiserhöhung ist der Nutzer berechtigt, den Vertrag innerhalb von drei Monaten nach Erhalt der Ankündigung nach Satz 2 in Textform kündigen. Auf die Kündigungsmöglichkeit weist WEPA in seiner Mitteilung nach Satz 2 ausdrücklich hin. Erfolgt keine Kündigung innerhalb dieser Frist, gilt das von WEPA mitgeteilte neue Nutzungsentgelt.

7. Systemänderungen

7.1 WEPA ist im Rahmen der Produktentwicklung zu Änderungen von apotec® Kühlschranküberwachung, insbesondere zur Anpassung an rechtliche, gesetzliche, wirtschaftliche und technische Bedingungen, berechtigt.

8. Haftung

8.1 Schadensersatzansprüche des Nutzers für Schäden gleich welcher Art sind ausgeschlossen. Die Haftungsbeschränkung gilt auch zugunsten gesetzlicher Vertreter und Erfüllungsgehilfen von WEPA, sofern der Nutzer gegen diese Ansprüche geltend macht.

8.2 Von vorstehender Haftungsbeschränkung ausgenommen sind Schadensersatzansprüche, die aus einer vorsätzlichen oder grob fahrlässigen Pflichtverletzung von WEPA, eines gesetzlichen Vertreters oder Erfüllungsgehilfen resultieren. Ebenfalls ausgenommen von dieser Haftungsbeschränkung ist die zumindest leicht fahrlässige Verletzung von wesentlichen Vertragspflichten. Wesentliche Vertragspflichten sind solche, deren Erfüllung die ordnungsgemäße Durchführung des Vertrags überhaupt erst ermöglichen und auf deren Erfüllung der Nutzer vertrauen darf.

8.3 Eine gesetzlich vorgeschriebene verschuldensunabhängige Haftung, insbesondere eine Haftung nach dem Produkthaftungsgesetz, sowie eine Haftung bei schuldhafter Verletzung von Leben, Körper oder Gesundheit eines Nutzers bleibt von der vorstehenden Haftungsbeschränkung unberührt.

9. Verfügbarkeit

9.1 Es besteht kein Anspruch auf eine unterbrechungsfreie Nutzung. Es wird nicht gewährleistet, dass der Zugang oder die Nutzung von apotec® Kühlschranküberwachung nicht durch Wartungsarbeiten, Weiterentwicklungen oder anderweitig durch Störungen unterbrochen oder beeinträchtigt wird. Die WEPA bemüht sich um eine möglichst unterbrechungsfreie Nutzbarkeit von apotec® Kühlschranküberwachung und wird den Nutzer über geplante Wartungsarbeiten im Voraus informieren. Jedoch können durch technische Störungen (wie z.B. Unterbrechung der Stromversorgung, Hardware- und Softwarefehler, technische Probleme in den Datenleitungen) zeitweilige Beschränkungen oder Unterbrechungen auftreten.

10. Datenschutz

10.1 Die Parteien verpflichtet sich, die Verarbeitung personenbezogener Daten unter Beachtung der einschlägigen datenschutzrechtlichen Vorschriften durchzuführen.

10.2 Soweit WEPA im Zusammenhang mit der Leistungserbringung personenbezogene Daten von Beschäftigten des Nutzers verarbeitet, vereinbaren die Parteien für den Umgang mit diesen personenbezogenen Daten die als Anlage 1 beigefügte Vereinbarung zur Auftragsverarbeitung gem. Art. 28 DSGVO.

11. Urheberrechte, Kennzeichnungsrechte uns sonstiges geistiges Eigentum

11.1 Die in apotec® Kühlschranküberwachung abrufbaren Inhalte (Texte, Daten, Bilder, Logos, Grafiken, Dokumentationen, Ton-, Video- und sonstige Bilddarstellungen) unterliegen dem Urheberrecht sowie sonstiger Gesetze zum Schutz geistigen Eigentums. Ohne ausdrückliche vorherige Zustimmung des jeweiligen Rechteinhabers dürfen die Inhalte weder ganz noch teilweise vervielfältigt, verbreitet, in anderen Medien (zum Beispiel anderen Webseiten) gespeichert oder verändert werden.

12. Änderungen der Nutzungsbedingungen

12.1 WEPA behält sich vor, einzelne Klauseln dieser Nutzungsbedingungen mit Wirkung für die Zukunft und ohne Angabe von Gründen zu ändern, sofern dies unter Berücksichtigung der Interessen von WEPA und für den Nutzer zumutbar ist. WEPA wird den Nutzer rechtzeitig über jegliche Änderungen der Nutzungsbedingungen informieren. Falls der Nutzer der Änderung der Nutzungsbedingungen nicht innerhalb von sechs Wochen nach Inkrafttreten der geänderten Nutzungsbedingungen widerspricht, gelten die abgeänderten Nutzungsbedingungen als angenommen. Widerspricht der Nutzer den Änderungen ist WEPA für den Fall, dass ein Festhalten an der Vertragsbeziehung unter der Geltung der bisherigen Nutzungsbedingungen nicht möglich oder zumutbar ist, unter Berücksichtigung der Interessen des Nutzers berechtigt, den Nutzungsvertrag zu kündigen.

13. Schlussbestimmungen

13.1 Auf diese Nutzungsbedingung und ihre Auslegung findet ausschließlich das Recht der Bundesrepublik Deutschland Anwendung. Die Anwendung des deutschen bzw. europäischen Internationalen Privatrechts sowie des UN-Kaufrechts ist ausgeschlossen.

13.2 Ausschließlicher Gerichtsstand und Erfüllungsort für Rechtsstreitigkeiten aus oder im Zusammenhang mit diesen Nutzungsbedingungen ist der Sitz von WEPA.

13.3 Sind oder werden einzelne Bestimmungen dieser Nutzungsbedingungen unwirksam und/oder nicht durchsetzbar, so bleibt die Gültigkeit der Bestimmungen im Übrigen unberührt. Unwirksame und/oder nicht durchsetzbare Bestimmungen werden im Wege der ergänzenden Vertragsauslegung durch diejenigen wirksamen und durchsetzbaren Bestimmungen ersetzt, die unter Berücksichtigung der Interessenlage beider Parteien zur Erreichung des gewünschten wirtschaftlichen Zwecks am ehesten geeignet sind. Entsprechendes gilt für die Ausfüllung von Lücken in diesen Nutzungsbedingungen.

Stand: 04/2024

Anlage 1: Vereinbarung zur Auftragsverarbeitung nach Art. 28 DSGVO

Soweit WEPA (nachfolgend in dieser Anlage: „Auftragsverarbeiter“) im Zusammenhang mit der Leistungserbringung personenbezogene Daten von Beschäftigten des Nutzers (nachfolgend: „Verantwortlicher“) verarbeitet, gelten die im Folgenden festgelegten Vereinbarungen zur Auftragsverarbeitung.

1. Zweck und Anwendungsbereich

1.1 Dieser Vertrag zur Auftragsverarbeitung (im Folgenden „Klauseln“) beruht im Wesentlichen auf den im Anhang zum DURCHFÜHRUNGSBESCHLUSS (EU) 2021/915 DER KOMMISSION vom 4. Juni 2021 über Standardvertragsklauseln zwischen Verantwortlichen und Auftragsverarbeitern gemäß Artikel 28 Absatz 7 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates und Artikel 29 Absatz 7 der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates aufgeführten Standardvertragsklauseln.

1.2 Mit diesen Klauseln soll die Einhaltung von Artikel 28 Absätze 3 und 4 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) sichergestellt werden.

1.3 Die Parteien haben diesen Klauseln zugestimmt, um die Einhaltung von Artikel 28 Absätze 3 und 4 der Verordnung (EU) 2016/679 zu gewährleisten.

1.4 Diese Klauseln gelten für die Verarbeitung personenbezogener Daten gemäß Anhang I.

1.5 Die Anhänge I bis III sind Bestandteil der Klauseln.

1.6 Diese Klauseln gelten unbeschadet der Verpflichtungen, denen der Verantwortliche gemäß der Verordnung (EU) 2016/679 unterliegt.

1.7 Diese Klauseln stellen für sich allein genommen nicht sicher, dass die Verpflichtungen im Zusammenhang mit internationalen Datenübermittlungen gemäß Kapitel V der Verordnung (EU) 2016/679 erfüllt werden.

2. Auslegung

2.1 Werden in diesen Klauseln die in der Verordnung (EU) 2016/679 definierten Begriffe verwendet, so haben diese Begriffe dieselbe Bedeutung wie in der betreffenden Verordnung.

2.2 Diese Klauseln sind im Lichte der Bestimmungen der Verordnung (EU) 2016/679 auszulegen.

2.3 Diese Klauseln dürfen nicht in einer Weise ausgelegt werden, die den in der Verordnung (EU) 2016/679 vorgesehenen Rechten und Pflichten zuwiderläuft oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneidet.

3. Beschreibung der Verarbeitung

Die Einzelheiten der Verarbeitungsvorgänge, insbesondere die Kategorien personenbezogener Daten und die Zwecke, für die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden, sind in Anhang I aufgeführt.

4. Pflichten der Parteien

4.1 Weisungen

4.1.1 Der Auftragsverarbeiter verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Verantwortlichen, es sei denn, er ist nach Unionsrecht oder nach dem Recht eines Mitgliedstaats, dem er unterliegt, zur Verarbeitung verpflichtet. In einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht dies nicht wegen eines wichtigen öffentlichen Interesses verbietet. Der Verantwortliche kann während der gesamten Dauer der Verarbeitung personenbezogener Daten weitere Weisungen erteilen. Diese Weisungen sind stets zu dokumentieren.

4.1.2 Der Auftragsverarbeiter informiert den Verantwortlichen, wenn er der Auffassung ist, dass vom Verantwortlichen erteilte Weisungen gegen die Verordnung (EU) 2016/679 oder geltende Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstoßen.

4.2 Zweckbindung

Der Auftragsverarbeiter verarbeitet die personenbezogenen Daten nur für den/die in Anhang I genannten spezifischen Zweck(e), sofern er keine weiteren Weisungen des Verantwortlichen erhält.

4.3 Dauer der Verarbeitung personenbezogener Daten

Die Daten werden vom Auftragsverarbeiter nur für die in Anhang I angegebene Dauer verarbeitet.

4.4 Sicherheit der Verarbeitung

4.4.1 Der Auftragsverarbeiter ergreift mindestens die in Anhang II aufgeführten technischen und organisatorischen Maßnahmen, um die Sicherheit der personenbezogenen Daten zu gewährleisten. Dies umfasst den Schutz der Daten vor einer Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu den Daten führt (im Folgenden „Verletzung des Schutzes personenbezogener Daten"). Bei der Beurteilung des angemessenen Schutzniveaus tragen die Parteien dem Stand der Technik, den Implementierungskosten, der Art, dem Umfang, den Umständen und den Zwecken der Verarbeitung sowie den für die betroffenen Personen verbundenen Risiken gebührend Rechnung.

4.4.2 Der Auftragsverarbeiter gewährt seinem Personal nur insoweit Zugang zu den personenbezogenen Daten, die Gegenstand der Verarbeitung sind, als dies für die Durchführung, Verwaltung und Überwachung des Vertrags erforderlich ist. Der Auftragsverarbeiter gewährleistet, dass sich die zur Verarbeitung der erhaltenen personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

4.6 Dokumentation und Einhaltung der Klauseln

4.6.1 Die Parteien müssen die Einhaltung dieser Klauseln nachweisen können.

4.6.2 Der Auftragsverarbeiter bearbeitet Anfragen des Verantwortlichen bezüglich der Verarbeitung von Daten gemäß diesen Klauseln umgehend und in angemessener Weise.

4.6.3 Der Auftragsverarbeiter stellt dem Verantwortlichen alle Informationen zur Verfügung, die für den Nachweis der Einhaltung der in diesen Klauseln festgelegten und unmittelbar aus der Verordnung (EU) 2016/679 hervorgehenden Pflichten erforderlich sind. Auf Verlangen des Verantwortlichen gestattet der Auftragsverarbeiter ebenfalls die Prüfung der unter diese Klauseln fallenden Verarbeitungstätigkeiten in angemessenen Abständen oder bei Anzeichen für eine Nichteinhaltung und trägt zu einer solchen Prüfung bei. Bei der Entscheidung über eine Überprüfung oder Prüfung kann der Verantwortliche einschlägige Zertifizierungen des Auftragsverarbeiters und/oder dessen Unterauftragsverarbeitern berücksichtigen.

4.6.4 Der Verantwortliche kann die Prüfung selbst durchführen oder einen unabhängigen Prüfer beauftragen. Die Prüfungen können auch Inspektionen in den Räumlichkeiten oder physischen Einrichtungen des Auftragsverarbeiters umfassen. Zur Durchführung von Inspektionen ist der Verantwortliche berechtigt, im Rahmen der üblichen Geschäftszeiten nach angemessener Vorankündigung (in der Regel mindestens 14 Kalendertage), sofern im Einzelfall nicht eine Inspektion ohne Vorankündigung für den Kontrollzweck zwingend erforderlich erscheint, auf eigene Kosten, ohne übermäßige Störung des Betriebsablaufs und unter strikter Geheimhaltung von Betriebs- und Geschäftsgeheimnissen des Auftragsverarbeiters die Geschäftsräume des Auftragsverarbeiters zu betreten, in denen personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet werden. Inspektionen sind grundsätzlich auf einmal pro Kalenderjahr begrenzt. Hiervon unberührt bleiben Inspektionen aus wichtigem, vom Verantwortlichen darzulegendem Grund. Der Auftragsverarbeiter übernimmt die Kosten der Kontrolle, soweit diese wegen eines Gesetzes- oder Vertragsverstoßes durch den Auftragsverarbeiter erforderlich wurde.

4.6.5 Beauftragt der Verantwortliche einen unabhängigen Prüfer mit der Durchführung der Überprüfung, hat der Verantwortliche den unabhängigen Prüfer schriftlich ebenso zu verpflichten, wie auch der Verantwortliche aufgrund

von dieser Klausel 4.6 gegenüber dem Auftragsverarbeiter verpflichtet ist. Zudem hat der Verantwortliche den unabhängigen Prüfer auf Verschwiegenheit und Geheimhaltung zu verpflichten, es sei denn, dass der unabhängige Prüfer einer beruflichen Verschwiegenheitsverpflichtung unterliegt. Auf Verlangen des Auftragsverarbeiters hat der Verantwortliche ihm die Verpflichtungsvereinbarungen mit dem unabhängigen Prüfer unverzüglich vorzulegen. Der Verantwortliche darf keinen Wettbewerber des Auftragsverarbeiters mit der Inspektion beauftragen.

4.6.6 Der Auftragsverarbeiter ist berechtigt, nach eigenem Ermessen unter Berücksichtigung der gesetzlichen Verpflichtungen des Verantwortlichen, Informationen nicht zu offenbaren, die sensibel im Hinblick auf die Geschäfte des Auftragsverarbeiters sind oder wenn der Auftragsverarbeiter durch deren Offenbarung gegen gesetzliche oder andere vertragliche Regelungen verstoßen würde. Der Verantwortliche ist nicht berechtigt, Zugang zu Daten oder Informationen über andere Kunden des Auftragsverarbeiters, zu Informationen hinsichtlich Kosten, zu Qualitätsprüfungs- und Vertrags-Managementberichten sowie zu sämtlichen anderen vertraulichen Daten des Auftragsverarbeiters, die nicht unmittelbar relevant für die vereinbarten Überprüfungszwecke sind, zu erhalten.

4.7 Einsatz von Unterauftragsverarbeitern

4.7.1 Der Auftragsverarbeiter besitzt die allgemeine Genehmigung des Verantwortlichen für die Beauftragung von Unterauftragsverarbeitern, die in der vereinbarten Liste gemäß Anhang III aufgeführt sind. Der Auftragsverarbeiter unterrichtet den Verantwortlichen mindestens 14 Kalendertage im Voraus ausdrücklich in schriftlicher Form über alle beabsichtigten Änderungen dieser Liste durch Hinzufügen oder Ersetzen von Unterauftragsverarbeitern und räumt dem Verantwortlichen damit ausreichend Zeit ein, um vor der Beauftragung des/der betreffenden Unterauftragsverarbeiter/s Einwände gegen diese Änderungen erheben zu können. Der Auftragsverarbeiter stellt dem Verantwortlichen die erforderlichen Informationen zur Verfügung, damit dieser sein Widerspruchsrecht ausüben kann.

4.7.2 Beauftragt der Auftragsverarbeiter einen Unterauftragsverarbeiter mit der Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Verantwortlichen), so muss diese Beauftragung im Wege eines Vertrags erfolgen, der dem Unterauftragsverarbeiter im Wesentlichen gleiche Datenschutzpflichten auferlegt wie diejenigen, die für den Auftragsverarbeiter gemäß diesen Klauseln gelten.

4.8 Internationale Datenübermittlungen

Der Verantwortliche erklärt sich damit einverstanden, dass in Fällen, in denen der Auftragsverarbeiter einen Unterauftragsverarbeiter gemäß Klausel 4.7 für die Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Verantwortlichen) in Anspruch nimmt und diese Verarbeitungstätigkeiten eine Übermittlung personenbezogener Daten im Sinne von Kapitel V der Verordnung (EU) 2016/679 beinhalten, der Auftragsverarbeiter und der Unterauftragsverarbeiter die Einhaltung von Kapitel V der Verordnung (EU) 2016/679 sicherstellen können, indem sie einen Sicherungsmechanismus nach Art. 44 ff. DSGVO nutzen (insbesondere einen Angemessenheitsbeschluss oder Standardvertragsklauseln, die von der Kommission gemäß Artikel 46 Absatz 2 der Verordnung (EU) 2016/679 erlassen wurden).

5. Unterstützung des Verantwortlichen

5.1 Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich über jeden Antrag, den er von der betroffenen Person erhalten hat. Er beantwortet den Antrag nicht selbst, es sei denn, er wurde vom Verantwortlichen dazu ermächtigt.

5.2 Unter Berücksichtigung der Art der Verarbeitung unterstützt der Auftragsverarbeiter den Verantwortlichen bei der Erfüllung von dessen Pflicht, Anträge betroffener Personen auf Ausübung ihrer Rechte zu beantworten.

5.3 Abgesehen von der Pflicht des Auftragsverarbeiters, den Verantwortlichen gemäß Klausel 5.2 zu unterstützen, unterstützt der Auftragsverarbeiter unter Berücksichtigung der Art der Datenverarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen zudem bei der Einhaltung der in den Artikeln 32 bis 36 genannten Pflichten.

6. Meldung von Verletzungen des Schutzes personenbezogener Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten arbeitet der Auftragsverarbeiter mit dem Verantwortlichen zusammen und unterstützt ihn entsprechend, damit der Verantwortliche seinen Verpflichtungen gemäß den Artikeln 33 und 34 der Verordnung (EU) 2016/679 nachkommen kann, wobei der Auftragsverarbeiter die Art der Verarbeitung und die ihm zur Verfügung stehenden Informationen berücksichtigt.

7. Verstöße gegen die Klauseln und Beendigung des Vertrags

7.1 Falls der Auftragsverarbeiter seinen Pflichten gemäß diesen Klauseln nicht nachkommt, kann der Verantwortliche – unbeschadet der Bestimmungen der Verordnung (EU) 2016/679 – den Auftragsverarbeiter anweisen, die Verarbeitung personenbezogener Daten auszusetzen, bis er diese Klauseln einhält oder der Vertrag beendet ist. Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich, wenn er aus welchen Gründen auch immer nicht in der Lage ist, diese Klauseln einzuhalten.

7.2 Der Auftragsverarbeiter ist berechtigt, den Vertrag zu kündigen, soweit vom Verantwortlichen erteilte Weisungen gegen die Verordnung (EU) 2016/679 oder geltende Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstoßen und der Verantwortliche auf der Erfüllung dieser Anweisungen besteht, nachdem er vom Auftragsverarbeiter darüber in Kenntnis gesetzt wurde, dass seine Anweisungen gegen geltende rechtliche Anforderungen gemäß Klausel 4.1.2 verstoßen.

7.4 Nach Beendigung des Vertrags löscht der Auftragsverarbeiter nach Wahl des Verantwortlichen alle im Auftrag des Verantwortlichen verarbeiteten personenbezogenen Daten und bescheinigt dem Verantwortlichen, dass dies erfolgt ist, oder er gibt alle personenbezogenen Daten an den Verantwortlichen zurück und löscht bestehende Kopien, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Bis zur Löschung oder Rückgabe der Daten gewährleistet der Auftragsverarbeiter weiterhin die Einhaltung dieser Klauseln.

ANHANG I - Beschreibung der Verarbeitung

Kategorien betroffener Personen, deren personenbezogene Daten verarbeitet werden

- Beschäftigte des Verantwortlichen

Kategorien personenbezogener Daten, die verarbeitet werden

- Logfiles, etwa IP-Adresse, eindeutige Nutzerkennung (UPN), Datum und Uhrzeit des Aufrufs sowie den Aufruftyp, verwendete Browsertyp und -version, verwendetes Betriebssystem, URL der Portalseite zum Zeitpunkt des Aufrufs, auf dem Portal vorgenommene Aktionen, Aufrufe von Backenddiensten
- Authentifizierungsdaten, etwa Eindeutige Nutzerkennung (UPN), Firmenadresse, Company-ID, Vor- und Nachname, E-Mail-Adresse, Telefonnummer
- Gerätedaten der Kühl- und Gefriergeräte und des SmartModules, etwa Modell, Seriennummer, Artikelnummer und Telemetriedaten wie z. B. Temperatur, Türöffnungsstatus, Netzwerkdaten (wie beispielsweise Mac- und IP-Adresse SmartModules, (W)LAN-Status)
- Benachrichtigungsfunktionen E-Mail (Eindeutige Nutzerkennung (UPN), Company-ID, E-Mail-Adresse des Empfängers, Metadaten zu den Nachrichten, Inhalt der Nachricht, Firmenadresse, Links zu Reports)
- Benachrichtigungsfunktion SMS- und Anruf (Eindeutige Nutzerkennung (UPN), Company-ID, Telefonnummer des Empfängers, Metadaten zu den Nachrichten, Inhalt der Nachricht bzw. der Anrufbenachrichtigung)

Verarbeitete sensible Daten (falls zutreffend) und angewandte Beschränkungen oder Garantien, die der Art der Daten und den verbundenen Risiken in vollem Umfang Rechnung tragen, z.B. strenge Zweckbindung, Zugangsbeschränkungen (einschließlich des Zugangs nur für Mitarbeiter, die eine spezielle Schulung absolviert haben), Aufzeichnungen über den Zugang zu den Daten, Beschränkungen für Weiterübermittlungen oder zusätzliche Sicherheitsmaßnahmen

- Es werden keine sensiblen Daten verarbeitet.

Art der Verarbeitung

- Die Art der Verarbeitung ist in den Nutzungsbedingungen konkret beschrieben. Mittels der browserbasierten Anwendung wird eine durchgängige Aufzeichnung der Temperaturen, Alarmzuständen sowie Schaltzuständen von Komponenten sichergestellt. Eine Alarmierung bei zu hoher oder zu niedriger Temperatur kann eingestellt werden. Die Alarmierung kann hierbei mittels E-Mail oder SMS-Benachrichtigung erfolgen. Daneben können Reports erstellt und heruntergeladen werden, um ggf. diversen Dokumentationspflichten nachkommen zu können

Zweck(e), für den/die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden

- Gewährleistung der Stabilität sowie Netz- und Informationssicherheit
- Authentifizierung auf dem Portal im Rahmen der Nutzung
- Benutzer und Berechtigungsverwaltung im Portal
- Versand von Benachrichtigungen
- Übermittlung von Reports auf digitalem Wege
- Zuletzt gewählte Sprache für das Portal, Internationalisierung des Lo-gins
- Speicherung der Login-Daten nach einem erfolgreichen Login (wie z.B. Name, UPN, Tokens)

Dauer der Verarbeitung

- Die Dauer der Verarbeitung entspricht der Laufzeit der Nutzungsvereinbarung.

ANHANG II - Technische und organisatorische Maßnahmen einschließlich zur Gewährleistung der Sicherheit der Daten

Für die Bereitstellung und Hosting des Portals greift der Auftragsverarbeiter auf die Leistungen von Unterauftragsverarbeiter zurück, deren technische und organisatorische Maßnahmen im Folgenden dargestellt werden:

1. Vertraulichkeit

1.1 Zutrittskontrolle

Ziel: Kein unbefugter Zutritt zu Datenverarbeitungsanlagen

- Automatisches Zugangskontrollsystem, Ausweisleser
- Chipkarten / Transpondersysteme
- 2 Faktor Schließsystem im Data Center (Biometrie)
- Zutrittsregelungen zum Betreten des Data Centers
- Manuelles Schließsystem
- Sicherheitsschlösser
- Schlüsselregelung / Liste / Dokumentation
- Türsicherung
- Türen mit Knauf Außenseite
- Elektronische Türen
- Haupteingänge außerhalb der Bürozeiten geschlossen
- Zutritt nur mit Ausweis möglich
- Besucherzugang nur über Empfang
- Protokoll der Besucher
- Werksumzäunung
- Schranken/Vereinzelungsanlagen
- Mitarbeiter- sowie Besucherausweise
- Besucher in Begleitung durch Mitarbeiter
- persönliches Abholen der Besucher
- Sicherung des Werksgeländes durch Wachpersonal
- Sicherung durch Kameras
- Sorgfalt bei Auswahl des Wachpersonals

1.2 Zugangskontrolle

Ziel: Keine unbefugte Systembenutzung

- Login mit Benutzername + Passwort
- Passwortrichtlinie
- Allg. Richtlinien IT- Sicherheit (Computer Use Policy, Passwortrichtlinie, Account Policy, Mobile Device usw.)
- Automatische Desktopsperre
- Next Generation Anti-Virus-Software Clients
- Next Generation Anti-Viren-Software Server
- BIOS Schutz (mit PIN/Passwort)
- Sperre externer Schnittstellen
- Verschlüsselung von Notebooks / Tablet
- Verschlüsselung von Datenträgern
- Verwalten von Benutzerberechtigungen

- Identity Access Management System
- Verschlüsselung Smartphones
- Mobile Device Management
- Netzwerkzugangskontrolle LAN/WIFI (NAC)
- Firewall
- Einsatz von VPN Technologie
- Erstellung von Benutzerrollen
- Passwort Managementsystem

1.3 Zugriffskontrolle

Ziel: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems

- Einsatz Berechtigungskonzepte
- Verwaltung der Berechtigungen durch Administratoren
- Genehmigung von Berechtigungen durch Dateneigentümern
- Minimale Anzahl an System-Administratoren/Applikations-Administrator
- Gesicherte Nutzung von USB-Schnittstellen
- Sichere Aufbewahrung von Datenträgern
- Tresor für Sicherungen
- Ordnungsgemäße Vernichtung von Datenträgern
- Externer Aktenvernichter bzw. Dienstleistern nach den aktuellen Vorgaben der Datenrichtlinie
- Akten Schredder
- Protokollierung von Zugriffen auf Anwendungen / Servern

1.4 Trennungskontrolle

Ziel: Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden

- Trennung von Produktiv- und Testumgebung
- Physikalische Trennung (Systeme / Datenbanken / Datenträger)
- Steuerung über Berechtigungskonzept
- Regelmäßige Prüfung der Berechtigungen
- Trennung von Daten und Systemen / Anwendungen
- Mandantenfähigkeit relevanter Anwendungen
- Festlegung von Datenbankrechten

1.5 Pseudonymisierung

Ziel: Verarbeitung von personenbezogenen Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einem Betroffenen zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechenden technischen und organisatorischen Maßnahmen unterliegen;

- Übermittlung von Daten in anonymisierter oder pseudonymisierter Form bzw. verschlüsselt
- Interne Anweisung zum sorgfältigem Umgang mit personenbezogenen Daten
- Löschung von personenbezogenen Daten nach Ablauf der gesetzlichen Löschfrist
- Trennung der Zuordnungsdaten

2. Integrität

2.1 Weitergabekontrolle

Ziel: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport

- Email-Verschlüsselung auf dem Transportweg (innerhalb des Konzerns)
- Verwendung von dedizierten Verbindungen
- Einsatz von VPN
- Datenträger Asset und Zuordnung zu Personen
- Protokollierung der Zugriffe und Abrufe
- Sichere Transportbehälter
- Bereitstellung über verschlüsselte Verbindungen
- Sorgfalt bei der Auswahl von Transport-Personal und Fahrzeugen
- Persönliche Übergabe mit Protokoll und Unterschrift
- Nutzung von Signaturen
- Nutzung von Zertifikaten

2.2 Eingabekontrolle

Ziel: Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind

- Technische Protokollierung der Eingabe, Änderung und Löschung der Daten
- Regelmäßige Plausibilitätsprüfungen
- Aufbewahrungs- und Löschfrist
- Klare Zuständigkeiten für Löschungen
- Nachvollziehbarkeit von Eingaben, Änderung und Löschung von Daten durch individuelle Benutzernamen
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzeptes mit Dateneigentümer und Genehmigungen
- Protokollierung von Änderungen, welche in automatische Verarbeitungen übernommen werden

3. Verfügbarkeit und Belastbarkeit

Ziel: Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust

- Server- und Storage-Systeme im gesicherten Data Center
- Data Center klimatisiert
- Feuer- und Rauchmeldeanlagen, sowie Brandfrüherkennung
- Data Center Überwachung Temperatur und Feuchtigkeit
- Kameraüberwachung im Data Center
- Meldungen beim Zutritt zum Data Center
- Keine sanitären Anschlüsse im Data Center
- Feuerlöscher im und / oder vor dem Data Center
- Redundante USV Anlagen
- Schutz gegen Umwelteinflüsse (Sturm, Wasser)
- RAID System / Festplattenspiegelung
- Getrennte Partitionen für Betriebssysteme und Daten
- Regelmäßige Software Updates
- Regelmäßige Durchführung einer Schwachstellenanalyse zu Hard- und Software
- Virenschutzsystem

- Backup & Recovery-Konzept
- Kontrolle des Sicherungsvorgangs
- Regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse
- Existenz eines Notfallplans
- Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Data Centers
- Datenschutztresor

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Datenschutzmanagement

- Interner Datenschutzbeauftragter
- Datenschutzorganisation/Datenschutzmanagement
- Datenschutz-Leitfäden/Handlungsempfehlungen
- Zentrale Dokumentation aller Verarbeitungstätigkeiten und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf / Berechtigung
- Formalisierter Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener ist vorhanden
- Die Datenschutz-Folgenabschätzung (DSFA) wird bei Bedarf durchgeführt
- Mitarbeiter über Datenschutz geschult bzw. sensibilisiert
- Mitarbeiter auf Vertraulichkeit/ Datengeheimnis verpflichtet

IT-Security-Management

- Interner Informationssicherheitsbeauftragter
- Information Security Managementsystem
- Liebherr IT-Security Policies
- Regelmäßige IT-Security Audits
- Mitarbeiter über Datensicherheit geschult

Incident Response

- Intrusion Prevention System (IPS)
- Einsatz von Firewall und regelmäßige Aktualisierung
- Einsatz von Spamfilter und regelmäßige Aktualisierung
- Einsatz von Virenscanner und regelmäßige Aktualisierung
- Dokumentierte Vorgehensweise zum Umgang mit Sicherheits-vorfällen
- Dokumentation von Sicherheitsvorfällen und Datenpannen
- Einbindung von DSB und ISB in Sicherheitsvorfälle und Datenpannen
- Formaler Prozess und Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen
- Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Datenschutzverletzungen (auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörde)

Datenschutzfreundliche Voreinstellungen

- Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind
- Einfache Ausübung des Widerrufrechts des Betroffenen durch technische Maßnahmen

Auftragskontrolle

- Vorhandene Muster-Vereinbarungen zur Auftragsverarbeitung
- Definierter Prozess für eine eindeutige Vertragsgestaltung
- Sorgfältige Auswahl von Auftragnehmern
- Prüfung der Vereinbarungen
- Kontrolle der Vertragsausführung

ANHANG III - Liste der Unterauftragsverarbeiter

Der Verantwortliche hat die Inanspruchnahme folgender Unterauftragsverarbeiter genehmigt:

Name	Anschrift	Kontaktperson	Beschreibung der Verarbeitung
Liebherr-Hausgeräte Vertriebs- und Service GmbH	Konrad-Zuse-Straße 4+6, 89081 Ulm, Deutschland		Bereitstellung und Hosting des Portals
Liebherr-Hausgeräte Ochsenhausen GmbH (als Unterauftragsverarbeiter der Liebherr-Hausgeräte Vertriebs- und Service GmbH)	Memminger Straße 77-79, 88416 Ochsenhausen, Deutschland		Hosting Azure Cloud, Bereitstellung & technische Betreuung des Portals, Authentifizierung, Lizenzverwaltung

WEPA Apothekenbedarf GmbH & Co KG, D-56204 Hillscheid
www.wepa-apothekenbedarf.de
T +49 (0)2624 107-361
F +49 (0)800 5252500 (gebührenfrei)
info@wepa-apothekenbedarf.de
wepa.shop
wepa.cloud
wepa.school