Fernwartungsbestimmung

Citadel Hotelsoftware GmbH

Für geschäftliche Kunden | Stand: 01.01.2024

Regelungen für technischen Support und sicheren Fernzugriff. Die Datenschutzregelungen beziehen sich auf diese Tätigkeiten. Dieses Dokument ergänzt die gesonderte Datenschutzerklärung und eine erforderliche Auftragsverarbeitungsvereinbarung (AVV); es ersetzt diese Dokumente nicht.

01 / Geltungsbereich und Vertragsgrundlagen

1.1 Diese Bestimmungen regeln Support- und Fernwartungsleistungen der Citadel Hotelsoftware GmbH (im Folgenden „Citadel“) für geschäftliche Kunden im Zusammenhang mit den von Citadel betreuten Softwareprodukten. Sie gelten ergänzend zu den jeweils vereinbarten Einzelverträgen und den wirksam einbezogenen Allgemeinen Geschäftsbedingungen.

1.2 Art und Umfang der geschuldeten Leistungen, Supportzeiten, Rufbereitschaft, Reaktionszeiten und Vergütung richten sich nach dem jeweils abgeschlossenen Supportvertrag beziehungsweise einer gesonderten Beauftragung. Die Veröffentlichung dieses Dokuments allein begründet keinen Anspruch auf eine bestimmte Supportleistung oder eine jederzeitige Erreichbarkeit.

1.3 Bei Abweichungen haben individuelle Vereinbarungen Vorrang. Eine erforderliche Vereinbarung zur Auftragsverarbeitung (AVV) nach Art. 28 DSGVO ergänzt diese Bestimmungen und geht bei spezifischen datenschutzrechtlichen Regelungen vor.

1.4 Maßgeblich sind die wirksam vereinbarten Vertragsunterlagen. Eine spätere Veröffentlichung geänderter Bestimmungen auf der Website ändert bestehende Vereinbarungen nicht automatisch.

02 / Supportleistungen und Leistungsabgrenzung

2.1 Soweit im Supportvertrag nichts Abweichendes vereinbart ist, gelten folgende reguläre Supportzeiten: Montag bis Freitag von 09:00 bis 12:00 Uhr sowie Montag bis Donnerstag von 13:00 bis 16:00 Uhr, jeweils ausgenommen gesetzliche Feiertage am Sitz von Citadel. Die Zeiten beziehen sich auf die dort geltende Ortszeit. Am Freitag endet die reguläre Supportzeit um 12:00 Uhr. Zusätzliche Hotline- oder Bereitschaftsleistungen richten sich nach dem jeweiligen Supportvertrag.

2.2 Je nach vertraglicher Vereinbarung umfasst der Support die Annahme und Bearbeitung von Störungsmeldungen, die Eingrenzung technischer Fehler, Unterstützung bei der Handhabung der betreuten Citadel-Produkte sowie die Wiederherstellung vereinbarter Softwarefunktionen im technisch möglichen Umfang.

2.3 Fernunterstützung, Versionsupdates, Wartungsleistungen und eine etwaige Hotline außerhalb der regulären Supportzeiten werden im vertraglich vereinbarten Umfang erbracht. Die Installation von Updates wird mit dem Kunden abgestimmt, soweit keine abweichende Vereinbarung besteht. Erhebliche Auswirkungen auf vereinbarte Funktionen oder Schnittstellen werden vorab erläutert und abgestimmt; ein allgemeines Recht zur einseitigen Einschränkung geschuldeter Funktionen wird nicht begründet. Gesetzliche Erhaltungs- und Mängelbeseitigungspflichten bleiben unberührt.

2.4 Nicht automatisch zum vereinbarten Support gehören insbesondere Schulungen, Organisations-, Steuer- oder Rechtsberatung, Leistungen für Fremdsoftware, Netzwerk- und Hardwareprobleme sowie die Beseitigung von Schadsoftware. Solche Leistungen können nach gesonderter Vereinbarung und Vergütung erbracht werden. Dies gilt nicht, soweit entsprechende Leistungen ausdrücklich vereinbart oder zur Erfüllung eigener gesetzlicher beziehungsweise vertraglicher Pflichten von Citadel erforderlich sind.

2.5 Ergibt die Fehleranalyse, dass zusätzliche Arbeiten außerhalb des vereinbarten Leistungsumfangs erforderlich sind, informiert Citadel den Kunden über Art und voraussichtliche Kosten. Kostenpflichtige Zusatzarbeiten erfolgen erst nach entsprechender Beauftragung oder auf einer bereits wirksam vereinbarten Grundlage. Gesetzliche und vertragliche Mängelbeseitigungspflichten werden dadurch nicht kostenpflichtig.

03 / Zweck und Umfang der Fernwartung

3.1 Fernwartung bezeichnet den zeitlich begrenzten technischen Zugriff auf vom Kunden hierfür freigegebene Systeme über eine Fernzugriffsverbindung. Sie dient insbesondere der Fehlerdiagnose, Störungsbehebung, Wartung, Konfiguration und Installation vereinbarter Softwareupdates.

3.2 Zugriffe erfolgen ausschließlich auf die für den konkreten Supportfall erforderlichen Systeme und Funktionen. Ein Zugriff auf weitere Server, Endgeräte, Anwendungen oder Datenbestände erfordert eine entsprechende Beauftragung oder Freigabe.

3.3 Citadel ist nicht zur dauerhaften Administration der gesamten IT-Infrastruktur des Kunden verpflichtet, sofern dies nicht gesondert vereinbart wurde.

04 / Freigabe und Durchführung der Fernwartung

4.1 Jede interaktive Fernwartungssitzung bedarf grundsätzlich einer Freigabe durch eine vom Kunden hierzu berechtigte Person. Die Freigabe kann über die Fernwartungssoftware oder einen dokumentierten Kommunikationsweg erfolgen. Dauerhaft eingerichtete unbeaufsichtigte Zugänge sind nur zulässig, wenn sie ausdrücklich gesondert vereinbart und angemessen abgesichert sind.

4.2 Der Kunde kann die Verbindung während einer interaktiven Sitzung beenden. Citadel beendet den Zugriff nach Abschluss der vereinbarten Arbeiten oder sobald die Berechtigung entfällt. Soweit ein laufender Eingriff nicht ohne Risiko unterbrochen werden kann, weist Citadel vorab oder bei Erkennbarkeit darauf hin und stimmt einen sicheren Abbruch ab. Das Recht des Kunden, die Zugriffsberechtigung zu entziehen, bleibt unberührt.

4.3 Der Kunde ermöglicht die notwendige Mitwirkung, benennt gegebenenfalls eine zuständige Kontaktperson und stellt erforderliche Zugänge nur in dem notwendigen Umfang bereit. Passwörter und sonstige Zugangsdaten dürfen nicht ungeschützt per E-Mail übermittelt werden.

4.4 Fernzugriffe werden über angemessen abgesicherte und verschlüsselte Verbindungen mit auf den erforderlichen Umfang beschränkten Berechtigungen durchgeführt. Individuell zuordenbare Zugänge sowie geeignete Authentifizierungsverfahren, bei entsprechendem Schutzbedarf auch Mehrfaktor-Authentifizierung, sind nach Maßgabe des Sicherheitskonzepts einzusetzen. Kann ein angemessen sicheres Verfahren nicht gewährleistet werden, wird die Verbindung nicht hergestellt beziehungsweise bis zur Klärung ausgesetzt.

05 / Installation und Sicherheitsvoraussetzungen

5.1 Die Fernwartung erfolgt über eine zwischen den Parteien abgestimmte Fernzugriffslösung. Der Kunde installiert beziehungsweise startet die hierfür erforderliche Software nach Anleitung von Citadel, soweit dies nicht anders vereinbart wurde.

5.2 Beide Seiten treffen ihrem Verantwortungsbereich entsprechende Sicherheitsmaßnahmen. Dazu gehören insbesondere aktuelle Schutzsoftware, System- und Sicherheitsupdates, Zugriffsschutz, angemessene Netzwerksicherheit und die Beschränkung administrativer Rechte auf das notwendige Maß.

5.3 Stellt eine Partei konkrete Sicherheitsrisiken fest, informiert sie die andere Partei unverzüglich im erforderlichen Umfang. Ein als unsicher erkannter Fernzugriff kann bis zur Klärung ausgesetzt werden.

06 / Datensicherung und Wiederherstellung

6.1 Die regelmäßige, vollständige und überprüfbare Sicherung der produktiv genutzten Daten und Systeme ist grundsätzlich Aufgabe des Kunden, soweit die Parteien keine ausdrückliche Übernahme bestimmter Sicherungsleistungen durch Citadel vereinbart haben.

6.2 Vor risikobehafteten Änderungen – insbesondere Updates, Datenbankarbeiten oder größeren Konfigurationsänderungen – stimmt Citadel erforderliche Sicherungsmaßnahmen mit dem Kunden ab. Eine Überprüfung des Vorhandenseins von Sicherungen durch Citadel ersetzt keine eigenständige Datensicherung und keinen Wiederherstellungstest.

6.3 Der Kunde soll Sicherungen räumlich beziehungsweise logisch getrennt und gegen unbefugten Zugriff geschützt aufbewahren sowie ihre Wiederherstellbarkeit regelmäßig testen. Eine vollständige Wiederherstellung kann nur im Rahmen der tatsächlich verfügbaren und funktionsfähigen Sicherungsstände erfolgen. Eine von Citadel ausdrücklich übernommene Sicherungs- oder Wiederherstellungspflicht wird durch diese Regelung nicht eingeschränkt. Ein Mitverschulden des Kunden wegen fehlender angemessener Sicherungen richtet sich nach dem Gesetz; ein automatischer Anspruchsausschluss wird nicht vereinbart.

07 / Vertraulichkeit und datensparsame Verarbeitung

7.1 Beide Parteien behandeln ihnen im Rahmen des Supports bekannt gewordene Betriebs- und Geschäftsgeheimnisse sowie vertrauliche Informationen auch nach Beendigung ihrer Zusammenarbeit vertraulich. Gesetzliche Offenlegungspflichten bleiben unberührt.

7.2 Citadel beschränkt Einsichtnahme, Kopien, Exporte und Änderungen von Kunden- und Gästedaten auf das zur konkreten Aufgabenerfüllung erforderliche Maß. Daten dürfen nicht zu eigenen, mit dem Auftrag unvereinbaren Zwecken verwendet werden.

7.3 Personen, die im Auftrag von Citadel an personenbezogenen Daten mitwirken, werden im erforderlichen Umfang auf Vertraulichkeit verpflichtet. Vertrauliche Dateien, Bildschirmaufzeichnungen oder Datenbankkopien dürfen nur verarbeitet werden, soweit hierfür eine rechtliche Grundlage und – soweit erforderlich – dokumentierte Weisungen vorliegen.

7.4 Für Supportanfragen sollen nach Möglichkeit anonymisierte Beispieldaten und auf den Fehler beschränkte Screenshots verwendet werden. Nicht erforderliche personenbezogene Angaben, Zugangsdaten und Geheimnisse sind vor der Übermittlung zu entfernen oder zu schwärzen. Besonders schutzbedürftige Datenbestände sind vor einem Zugriff mitzuteilen, damit erforderliche Schutzmaßnahmen abgestimmt werden können. Eine Übermittlung solcher Daten erfolgt nur, soweit sie erforderlich und rechtlich zulässig ist.

08 / Datenschutzrechtliche Verantwortlichkeiten und AVV

8.1 Der Kunde entscheidet grundsätzlich über Zwecke und wesentliche Mittel der Verarbeitung seiner Gäste-, Mitarbeiter- und Betriebsdaten und ist insoweit regelmäßig Verantwortlicher im Sinne der DSGVO. Citadel kann bei Fernwartung und Support, soweit im Auftrag personenbezogene Daten verarbeitet werden, als Auftragsverarbeiter tätig werden. Die datenschutzrechtliche Rolle ist anhand der tatsächlichen Leistung zu bestimmen.

8.2 Ist eine Auftragsverarbeitung gegeben, müssen die Parteien vor Beginn der entsprechenden Verarbeitung eine den Anforderungen von Art. 28 Abs. 3 DSGVO entsprechende Vereinbarung zur Auftragsverarbeitung abschließen beziehungsweise wirksam einbeziehen. Diese Fernwartungsbestimmungen allein ersetzen eine solche Vereinbarung nicht.

8.3 Die AVV regelt insbesondere Gegenstand, Dauer, Art und Zweck der Verarbeitung, Kategorien betroffener Personen und Daten, Weisungen, technische und organisatorische Maßnahmen, Unterauftragsverarbeiter, Kontrollrechte, Unterstützungspflichten und die Behandlung von Daten nach Vertragsende.

8.4 Citadel verarbeitet auftragsbezogene personenbezogene Daten nur auf dokumentierte Weisung, soweit keine vorrangige rechtliche Verpflichtung besteht; im Fall einer nach ihrer Auffassung rechtswidrigen Weisung informiert Citadel den Kunden nach Maßgabe von Art. 28 DSGVO.

8.5 Soweit Citadel Kontaktdaten von Ansprechpartnern, Vertrags-, Abrechnungs- oder erforderliche Nachweisdaten für eigene rechtmäßige Zwecke verarbeitet, ist diese Verarbeitung gesondert von einer Auftragsverarbeitung zu beurteilen. Rechtsgrundlagen, Informationspflichten und Aufbewahrung richten sich nach der tatsächlichen Verarbeitung und der hierfür geltenden Datenschutzerklärung. Diese Bestimmungen ersetzen keine erforderlichen Datenschutzinformationen.

09 / Technische und organisatorische Maßnahmen

9.1 Citadel trifft für ihre jeweilige Verarbeitung angemessene technische und organisatorische Maßnahmen nach Art. 32 DSGVO. Das erforderliche Schutzniveau richtet sich unter anderem nach Verarbeitungszweck, Stand der Technik, Eintrittswahrscheinlichkeit und Schwere möglicher Risiken.

9.2 Dazu zählen nach Erforderlichkeit die Kontrolle und Beschränkung von Zugriffen, sichere Authentifizierung, Verschlüsselung der Übertragung, Berechtigungsverwaltung, Schutz der eingesetzten Endgeräte, sichere Verarbeitung von Supportdateien sowie Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der Maßnahmen.

9.3 Die konkret vereinbarten Maßnahmen und etwaige Unterauftragsverarbeiter werden, soweit erforderlich, in der AVV beziehungsweise ihren Anlagen beschrieben. Diese Bestimmungen enthalten keine Zusage für eine bestimmte Fernwartungssoftware oder einen bestimmten Datenstandort. Verwendete Lösungen, relevante Verarbeitungsorte und erforderliche Schutzmaßnahmen müssen vor dem jeweiligen Einsatz geprüft und, soweit erforderlich, mit dem Kunden vereinbart beziehungsweise genehmigt sein.

10 / Protokollierung und Dokumentation

10.1 Fernwartungsvorgänge werden in einem dem Zweck angemessenen Umfang dokumentiert. Hierzu können unter anderem Zeitpunkt, bearbeitender Mitarbeiter, Kunde, betroffene Systeme, Freigabe, wesentliche Tätigkeiten und Ende der Verbindung gehören.

10.2 Die Dokumentation dient der Nachvollziehbarkeit, Sicherheit, Bearbeitung des Supportfalls und Erfüllung gesetzlicher Pflichten. Umfang und Aufbewahrungsdauer werden nach Erforderlichkeit und den geltenden Datenschutzvorgaben bestimmt; zusätzliche technische Sitzungsaufzeichnungen erfolgen nur mit entsprechender Rechtsgrundlage und transparenter Information. Eine pauschale Erlaubnis zur Aufzeichnung von Bildschirminhalten oder Gesprächen wird nicht erteilt. Berechtigte Zugriffe auf Protokolle werden beschränkt; Löschfristen oder die Kriterien ihrer Bestimmung sind für die jeweilige Verarbeitung festzulegen.

10.3 Der Kunde erhält auf berechtigte Anfrage die für die Nachvollziehbarkeit des konkreten Supportfalls erforderlichen Informationen, soweit dem keine schutzwürdigen Rechte Dritter oder rechtliche Einschränkungen entgegenstehen.

11 / Sicherheitsvorfälle und Datenschutzverletzungen

11.1 Erkennen die Parteien im Rahmen der Fernwartung einen sicherheitsrelevanten Vorfall, stimmen sie die erforderlichen Sofortmaßnahmen unter Berücksichtigung der jeweiligen Verantwortungsbereiche ab.

11.2 Soweit Citadel als Auftragsverarbeiter von einer Verletzung des Schutzes personenbezogener Daten Kenntnis erlangt, informiert Citadel den Kunden unverzüglich im Sinne von Art. 33 Abs. 2 DSGVO und unterstützt ihn im nach der AVV geschuldeten Umfang. Die Meldung an eine Aufsichtsbehörde und die Benachrichtigung betroffener Personen obliegen grundsätzlich dem hierfür verantwortlichen Unternehmen. Soweit erforderliche Informationen noch nicht vollständig vorliegen, wird die Meldung ohne unangemessene Verzögerung durch weitere Informationen ergänzt. Eigene gesetzliche Pflichten von Citadel bleiben unberührt.

11.3 Ein Sicherheitsvorfall kann Anlass sein, eine Fernwartungssitzung auszusetzen, Zugriffsberechtigungen zu sperren und Beweismittel sachgerecht zu sichern.

12 / Einsatz weiterer Dienstleister und Übermittlung in Drittländer

12.1 Werden bei einer Auftragsverarbeitung weitere Auftragsverarbeiter eingesetzt, gelten die Anforderungen aus Art. 28 Abs. 2 und 4 DSGVO. Die erforderliche vorherige Genehmigung und Informationspflichten werden in der AVV geregelt.

12.2 Eine Übermittlung personenbezogener Daten in Staaten außerhalb des Europäischen Wirtschaftsraums erfolgt nur unter den Voraussetzungen der Art. 44 ff. DSGVO und unter Berücksichtigung der vertraglichen Festlegungen. Für konkrete eingesetzte Anbieter, Verarbeitungsorte und Garantien ist die jeweilige AVV nebst Anlagen maßgeblich.

13 / Vergütung, Leistungsgrenzen und Haftung

13.1 Vergütung, Abrechnung von Zusatzleistungen und vereinbarte Servicelevels richten sich nach den bestehenden Verträgen. Der bloße Eingang einer Supportanfrage oder eine automatische Bestätigung verspricht keine bestimmte Reaktions- oder Behebungszeit. Aus dem vereinbarten Leistungsmodell sowie dem Gesetz folgende Ansprüche auf Fehlerbehebung, Nacherfüllung, Gebrauchserhaltung und weitere Rechte bleiben unberührt. Lässt sich eine Störung nicht per Fernwartung beheben, stimmen die Parteien das weitere Vorgehen ab; eine geschuldete Leistung entfällt nicht allein deshalb.

13.2 Für die Haftung gelten die individuellen Vereinbarungen und die wirksam einbezogenen Allgemeinen Geschäftsbedingungen, soweit sie mit zwingendem Recht vereinbar sind. Die gesetzlichen Ansprüche betroffener Personen, insbesondere nach Art. 82 DSGVO, werden durch diese Bestimmungen nicht eingeschränkt. Zwingende Haftung, insbesondere für Vorsatz sowie für Schäden aus der Verletzung des Lebens, des Körpers oder der Gesundheit, bleibt unberührt. Die Haftung für grobe Fahrlässigkeit wird durch diese Bestimmungen nicht ausgeschlossen oder begrenzt.

13.3 Die Parteien wirken angemessen daran mit, Schäden zu vermeiden und zu begrenzen. Keine Bestimmung dieser Fernwartungsregelung hebt gesetzlich zwingende Rechte auf.

14 / Beendigung der Sitzung und Vertragsende

14.1 Nach Abschluss einer Fernwartungssitzung wird die Verbindung beendet; temporär eingeräumte Berechtigungen und Zugangsdaten sind, soweit erforderlich, zurückzunehmen oder zu deaktivieren.

14.2 Nach Beendigung der vertraglichen Zusammenarbeit richten sich Rückgabe, Löschung und gegebenenfalls gesetzlich gebotene weitere Aufbewahrung personenbezogener Daten nach der anwendbaren AVV und den gesetzlichen Vorschriften. Unabhängige Dokumentations- und Nachweispflichten bleiben unberührt.

14.3 Für im Auftrag verarbeitete personenbezogene Daten richtet sich die Rückgabe oder Löschung nach der Entscheidung des Kunden und der AVV, soweit keine gesetzliche Aufbewahrungspflicht entgegensteht. Nicht mehr erforderliche Arbeitskopien und Exporte aus Supportfällen sind einschließlich vorhandener Kopien entsprechend zu löschen. Soweit Daten in Sicherungen zunächst verbleiben, sind diese gegen weitere Nutzung zu sperren und nach dem vereinbarten Lösch- und Sicherungskonzept zu entfernen.

15 / Schlussbestimmungen und Kontakt

15.1 Änderungen und Ergänzungen erfolgen nach Maßgabe der zugrunde liegenden Vertragsvereinbarungen und der gesetzlichen Formvorschriften. Die Unwirksamkeit einzelner Bestimmungen berührt die Wirksamkeit der übrigen Bestimmungen nicht; anstelle unwirksamer Regelungen gelten die gesetzlichen Vorschriften.

15.2 Kontakt für Support und Abstimmungen: Citadel Hotelsoftware GmbH, Alter Münsterweg 29, 48231 Warendorf, Deutschland. Allgemeiner Kontakt: info@citadel.de. Supportanfragen können über das Citadel Serviceportal beziehungsweise die vertraglich vereinbarten Kontaktwege gestellt werden.