Informationssicherheitsplan

Anhang zu den EU-Rechtsvorschriften

Dieser Anhang beschreibt die Verpflichtungen von Infor in Bezug auf spezifische Anforderungen gemäß den anwendbaren EU-Richtlinien und Verordnungen zur Cybersicherheit und Data Governance sowie den nationalen Umsetzungsgesetzen („***Geltendes Recht zur Cybersicherheit und Data Governance***“) und ist, sofern auf den Kunden anwendbar (wie unten definiert), in die vom Kunden mit Infor abgeschlossenen Verträge (zusammenfassend die „***Verträge***“) integriert. Im Falle eines Widerspruchs oder einer Unstimmigkeit zwischen den Bestimmungen dieses Anhangs und anderen Bestimmungen der Verträge in Bezug auf Cybersicherheitsfragen hat dieser Anhang Vorrang.

I. ALLGEMEINES

1. DEFINITIONEN

1.1 Begriffe, die in diesem Anhang verwendet, aber nicht definiert werden, haben die Bedeutung, die im Informationssicherheitsplan unter www.infor.com/security-plan (der „ISP“) angegeben ist. Die Begriffe „IKT-Prozess“, „IKT-Produkt“, „IKT-Dienstleistung“, „Sicherheitsvorfälle“, „Netz- und Informationssysteme“, „Risiko“, „Erhebliche Cyber-Bedrohung“, "Wechsel", "Wechselentgelte", "Interoperabilität", "exportierbare Daten" und "digitale Vermögenswerte" haben die Bedeutung, die ihnen im jeweils Geltenden Recht zur Cybersicherheit und Data Governance zugewiesen wird.

2. COMPLIANCE UND ZUSAMMENARBEIT

2.1 Infor wird das für ihre Geschäftstätigkeit Geltende Recht zur Cybersicherheit und Data Governance einhalten und auf angemessene Anfragen mit der jeweils zuständigen staatlichen Behörde und/oder dem Kunden in Bezug auf Infor's Einhaltung ihrer Verpflichtungen aus dem Vertrag im Hinblick auf das Geltende Recht zur Cybersicherheit und Data Governance zusammenarbeiten. Sowohl Infor als auch der Kunde werden den jeweils anderen über jede wesentliche Änderung oder jedes Ereignis, jede Schwierigkeit, jedes Risiko oder jede Information benachrichtigen und hinweisen, die sich nachteilig auf die IKT-Dienstleistungen oder die Erfüllung des Vertrages auswirken könnten (es sei denn, die Weitergabe solcher Informationen ist nach Geltendem Recht untersagt).

3. WIRKSAMKEITSDATUM

3.1 Die Bedingungen dieses Anhangs treten an dem Datum in Kraft, an dem das jeweils Geltende Recht zur Cybersicherheit und Data Governance anwendbar und durchsetzbar wird.

4. AKTUALISIERUNGEN

4.1 Der Kunde erkennt an, dass die in diesem Anhang beschriebenen technischen und organisatorischen Sicherheitsmaßnahmen aktualisierten Anforderungen unterliegen können, die sich aus dem Geltendem Recht zur Cybersicherheit und Data Governance sowie dem technischen Fortschritt und der Entwicklung ergeben und dass Infor die Maßnahmen von Zeit zu Zeit aktualisieren oder ändern kann, vorausgesetzt, dass solche Aktualisierungen und Änderungen nicht zu einer Verschlechterung der Gesamtsicherheit der dem Kunden bereitgestellten Dienste führen.

5. GELTENDES RECHT

5.1 Dieser Anhang unterliegt dem im Vertrag festgelegten Recht und wird entsprechend diesem ausgeführt, es sei denn, das Geltende Recht zur Cybersicherheit und Data Governance schreibt eine spezielle Rechtswahl vor; in diesem Fall gilt für diesen Anhang, dass das jeweils vorgeschriebene Geltende Recht Vorrang vor dem im Vertrag festgelegten Geltendem Recht hat.

6. HAFTUNG

6.1 Infor und der Kunde vereinbaren, dass die Gesamthaftung jeder Partei und ihrer Verbundenen Unternehmen (wie im Vertrag definiert), die sich aus oder im Zusammenhang mit diesem Anhang ergibt, unabhängig davon, ob sie auf Vertragsverletzung, unerlaubter Handlung oder aus anderem Grund zwischen den Parteien (einschließlich der Verbundenen Unternehmen) beruht, den im Vertrag vereinbarten Regelungen zur Haftungsbeschränkung unterliegt. Darüber hinaus haftet Infor nicht für Verstöße des Kunden gegen Geltendes Recht zur Cybersicherheit

und Data Governance oder für die Nichteinhaltung der Anforderungen der zuständigen Behörden durch den Kunden.

II. NIS-2-RICHTLINIE

1. ANWENDUNGSBEREICH UND DEFINITIONEN

1.1 Die in Abschnitt II dieses Anhangs festgelegten Bedingungen gelten ausschließlich für EU Kunden, die die Kriterien und Schwellenwerte von „wichtigen“ oder „wesentlichen“ Einrichtungen erfüllen und somit unter den Anwendungsbereich der NIS-2-Richtlinie fallen. Zur Klarstellung wird Abschnitt I in diesen Abschnitt II aufgenommen.

1.2 **„NIS-2-Richtlinie“** bezeichnet die Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der EU, die die Verordnung (EU) Nr. 910/2014 und die Richtlinie (EU) 2018/1972 ändert und die Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie) aufhebt, sowie alle entsprechenden Durchführungsverordnungen.

2. GOVERNANCE

2.1 Infor verfügt innerhalb ihres eigenen Sicherheitsbereichs über Leitungsorgane, die für die Genehmigung, Überwachung und Verantwortung der Umsetzung der Cybersicherheits-Risikomanagement-Maßnahmen von Infor, einschließlich des ISP, zuständig sind.

3. INFORMATIONSSICHERHEITSPROGRAMM

3.1 Infor hat den ISP umgesetzt und wird ihn aufrechterhalten, damit er: (A) darauf ausgelegt ist, (1) die Sicherheit und Vertraulichkeit der Netzwerk- und Informationssysteme von Infor zu gewährleisten; (2) gegen erwartete Bedrohungen oder Gefahren für die Sicherheit oder Integrität der Netzwerk- und Informationssysteme von Infor zu schützen; und (3) gegen unbefugten Zugriff auf oder die Nutzung von Netzwerk- und Informationssystemen zu schützen; und (B) die Richtlinie von Infor zur Reaktion auf Sicherheitsvorfälle darlegt.

3.2 Der ISP ist unter www.infor.com/security-plan verfügbar.

4. CYBERSICHERHEITS - RISIKOMANAGEMENT- MASSNAHMEN

4.1 Infor hat Cybersicherheits-Risikomanagement-Maßnahmen umgesetzt und wird diese aufrechterhalten, die:

(A) in einem angemessenen Verhältnis zu den Risiken stehen, die für das Netzwerk- und Informationssystemen von Infor bestehen, wobei der Stand der Technik und gegebenenfalls einschlägige europäische und internationale Standards sowie die Kosten der Implementierung berücksichtigt werden;

(B) auf einem „gefahrenübergreifenden“ Ansatz basieren, der darauf abzielt, Infors Netzwerk- und Informationssysteme und deren physische Umgebung vor Sicherheitsvorfällen zu schützen; und

(C) mindestens Folgendes umfassen: (a) Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme; (b) Maßnahmen zur Identifizierung von Risiken für Sicherheitsvorfälle, einschließlich Verfahren zur Bewältigung von Sicherheitsvorfällen; (c) Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement; (d) Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen Infor und seinen direkten Lieferanten oder Dienstleistern; (e) Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschließlich Management und Offenlegung von Schwachstellen; (f) Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit; (g) grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit; wie Prinzipien des Zero-Trust, Software-Updates, Gerätekonfiguration, Netzwerksegmentierung, Identitäts- und Zugangsmanagement oder Nutzersensibilisierung, regelmäßige Cybersicherheitsschulungen für Mitarbeiter und Sensibilisierung für Cyberbedrohungen, Phishing oder Social-Engineering-Techniken (h) Konzepte und Verfahren für den Einsatz von Kryptografie und Verschlüsselung; (i) Sicherheit des Personals, Konzepte für die Zugriffskontrolle und -Management von Anlagen; (j) Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung,

gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb von Infor.

5. LIEFERKETTE

5.1 Infor gewährleistet, dass die von Infor implementierten Sicherheitsmaßnahmen für die Lieferkette die folgenden Kriterien berücksichtigen: (a) die spezifischen Schwachstellen jedes direkten Lieferanten und Dienstleisters von Infor; (b) die Gesamtqualität der Produkte und Cybersicherheitspraktiken der Lieferanten und Dienstleister von Infor, einschließlich ihrer sicheren Entwicklungsverfahren; und gegebenenfalls (c) die Ergebnisse von koordinierten Sicherheitsrisikobewertungen spezifischer kritischer IKT-Dienste, IKT-Produkte oder IKT-Prozesslieferketten, die von EU-Mitgliedstaaten und der jeweils zuständigen Behörde durchgeführt werden.

5.2 Infor führt eine Due-Diligence-Prüfung bei seinen Dienstleistern durch, um deren Cybersicherheits-Risikomanagement-Maßnahmen zu bewerten, und schließt mit diesen Dienstleistern Verträge ab, die im Wesentlichen ähnliche Anforderungen an das Geltende Recht zur Cybersicherheit und Data Governance wie dieser Anhang enthalten.

5.3 Infor wird auf Anfrage des Kunden angemessene Nachweise über die umgesetzten Sicherheitsmaßnahmen in der Lieferkette innerhalb eines angemessenen Zeitrahmens bereitstellen.

6. REAKTION AUF SICHERHEITSVORFÄLLE

6.1 Infor wird seine Netzwerk- und Informationssysteme auf unbefugten Zugriff überwachen und eine Richtlinie zur Reaktion auf Sicherheitsvorfälle umsetzen, die Maßnahmen festlegt, die zu ergreifen sind, wenn Infor einen Sicherheitsvorfall entdeckt oder davon Kenntnis erlangt.

6.2 Wenn Infor von einem erheblichen Sicherheitsvorfall Kenntnis erlangt, der den Kunden betrifft, wird Infor:

(A) den Kunden wie folgt benachrichtigen:

(1) Unverzüglich und ohne unangemessene Verzögerung (und in jedem Fall innerhalb von 24 Stunden nach Kenntnisnahme des erheblichen Sicherheitsvorfalls): (a) den Kunden über das Auftreten des erheblichen Sicherheitsvorfalls informieren; und (b) dem Kunden detaillierte Informationen über den erheblichen Sicherheitsvorfall bereitstellen, einschließlich der folgenden: (i) ob der Verdacht besteht, dass der erhebliche Sicherheitsvorfall möglicherweise auf rechtswidrige oder böswillige Handlungen zurückzuführen ist oder grenzüberschreitende Auswirkungen haben könnte; (ii) alle Informationen, um grenzüberschreitende Auswirkungen des erheblichen Sicherheitsvorfalls zu bestimmen; und (iii) eine erste Bewertung des erheblichen Sicherheitsvorfalls, einschließlich seines Schweregrads und seiner Auswirkungen, sowie gegebenenfalls die Kompromittierungsindikatoren angegeben.

(2) Unverzüglich und ohne unangemessene Verzögerung dem Kunden die folgenden ergänzenden Informationen über den erheblichen Sicherheitsvorfall bereitstellen: (a) eine ausführliche Beschreibung des Sicherheitsvorfalls, einschließlich seines Schweregrads und seiner Auswirkungen; (b) Angaben zur Art der Bedrohung bzw. zugrunde liegenden Ursache, die wahrscheinlich den Sicherheitsvorfall ausgelöst hat; (c) Angaben zu den getroffenen und laufenden Abhilfemaßnahmen; (d) gegebenenfalls die grenzüberschreitenden Auswirkungen des Sicherheitsvorfalls.

(B) eine Untersuchung durchführen und eine angemessene Analyse der Ursache(n) des erheblichen Sicherheitsvorfalls durchführen;

(C) dem Kunden regelmäßige Updates zu laufenden Untersuchungen bereitstellen;

(D) einen geeigneten Plan entwickeln und umsetzen, um die Ursache des erheblichen Sicherheitsvorfalls zu beseitigen und zu beheben, soweit die Ursache in der Verantwortung von Infor liegt;

(E) bei der angemessenen Untersuchung des Kunden und seinen Bemühungen, um die Einhaltung der für einen solchen erheblichen Sicherheitsvorfall geltenden Meldepflichten zusammenzuarbeiten, einschließlich der Unterstützung bei der Erstellung eines Berichts über den erheblichen Sicherheitsvorfall an die zuständigen Behörden.

6.3 Erhält Infor Kenntnis von einer erheblichen Cyberbedrohung, die sich auf den Kunden auswirkt (einschließlich veröffentlichter Sicherheitslücken in Infor-Anwendungen, die der Definition einer erhebliche Cyberbedrohung entsprechen), wird Infor:

(A) den Kunden unverzüglich und ohne unangemessene Verzögerung über die erhebliche Cyberbedrohung informieren

(B) dem Kunden detaillierte Informationen über die Auswirkungen der erheblichen Cyberbedrohung auf den Kunden zur Verfügung stellen, soweit Infor darüber Kenntnis hat;

(C) eine Untersuchung durchführen und eine angemessene Analyse der Ursache(n) der erhebliche Cyberbedrohung durchführen

(D) einen geeigneten Plan entwickeln und umsetzen, um die Ursache der erhebliche Cyberbedrohung zu beheben, sofern diese erhebliche Cyberbedrohung eintritt und die Ursache in der Kontrolle von Infor liegt; und

(E) der angemessenen Aufforderung des Kunden nachkommen, um Informationen über die erhebliche Cyberbedrohung bereitzustellen, die der Kunde für seine erforderlichen Meldepflichten in Bezug auf die erhebliche Cyberbedrohung an Dritte verwenden kann, falls solche gemäß des Geltenden Rechts zur Cybersicherheit und Data Governance erforderlich sind.

7. AUDIT

7.1 Infor wird mindestens eine der folgenden Zertifizierungen und Bescheinigungen in Bezug auf seine Cloud-Dienste (je nach Anwendbarkeit) besitzen und aufrechterhalten und wird dem Kunden auf schriftliche Anfrage einen Nachweis über solche Zertifizierungen und/oder Bescheinigung vorlegen:

(1) SSAE SOC 2 Type 2 (auch bekannt als AICPA TSC 2014 Type 2)
(2) ISO 27001:2022
(3) FedRAMP

Infor wird sicherstellen, dass ihre Drittdienstleister mindestens eine der oben genannten Zertifizierungen und Bescheinigungen in Bezug auf die Dienstleistungen besitzen oder aufrechterhalten, die dieser Drittdienstleister für Infor und/oder Infor-Kunden erbringt, oder einen zufriedenstellenden alternativen Nachweis über seine Maßnahmen zum Management von Cybersecurity-Risiken in Bezug auf den Umfang der erbrachten Dienstleistungen erbringen.

7.2 Zusätzlich zu den in Abschnitt 7.1 beschriebenen Prüfberichten wird Infor auf Verlangen des Kunde und vorbehaltlich der Vertraulichkeitsverpflichtungen des Vertrages, nicht mehr als einmal jährlich, es sei denn, der Kunde handelt aufgrund eines Ersuchens einer zuständigen Regierungsbehörde (in diesem Fall gilt die jährliche Beschränkung nicht), unverzüglich schriftlich auf alle angemessenen Anfragen oder Fragebögen des Kunden (und/oder seiner Vertreter) bezüglich des Inhalts des Sicherheitsprogramms von Infor antworten und angemessene Nachweise über die Einhaltung der Anforderungen dieses Anhangs erbringen, einschließlich allgemein verfügbarer Kopien von Daten, Dokumenten und Informationen im Hinblick auf die Dienstleistungen, die zur Unterstützung des Kunden bei der Einhaltung von verbindlichen Anfragen oder Anordnungen der zuständigen staatlichen Behörden erforderlich sind. Infor wird die entsprechenden Informationen ohne unnötigen Verzug zur Verfügung stellen (und in jedem Fall innerhalb des in der verbindlichen Anfrage oder Anordnung angegebenen Zeitrahmens, die der Kunde von der zuständigen staatlichen Behörde erhalten hat).

7.3 Der Kunde kann einmal pro Jahr die Einhaltung der Pflichten von Infor aus diesem Anhang, einschließlich der Überprüfung der IT-Sicherheitspraktiken von Infor und der entsprechenden Kontrollumgebungen, gemäß dem in diesem Abschnitt 7 beschriebenen Verfahren prüfen, wenn:

(A) Infor keine ausreichenden Nachweise für die Einhaltung der in diesem Anhang beschriebenen Maßnahmen zum Management von Cybersicherheitsrisiken durch die in Abschnitt 7.2 genannten Berichte und Unterlagen oder gegebenenfalls durch andere Prüfberichte oder sonstige Informationen, die Infor seinen Kunden allgemein zur Verfügung stellt, erbracht hat;

(B) ein schwerwiegender Sicherheitsvorfall eingetreten ist;

(C) Infor den Kunden benachrichtigt, dass es Gegenstand eines behördlichen Antrags auf Zugang zu Kundendaten ist;

(D) ein Audit von einer für den Kunden zuständigen staatlichen Behörde förmlich verlangt wird; oder

(E) ein zwingend Geltendes Recht zur Cybersicherheit und Data-Governance dem Kunden ein direktes Prüfungsrecht einräumt.

7.4 Vor Beginn einer Prüfung werden der Kunde und Infor den Umfang, den Zeitpunkt, die Dauer, die Kontroll- und Nachweisanforderungen einvernehmlich festlegen. Der Kunde kann ein unabhängiges, akkreditiertes Drittunternehmen mit der Durchführung der Prüfung in seinem Namen beauftragen, vorausgesetzt, das Drittunternehmen wird von dem Kunden und Infor einvernehmlich bestimmt (dies schließt keine Drittunternehmen ein, die entweder ein Wettbewerber von Infor sind oder nicht angemessen qualifiziert oder unabhängig sind). Der Kunde bestätigt, dass die Prüfung ohne unzumutbare Beeinträchtigung der Geschäftsaktivitäten von Infor (oder dessen Subunternehmer), während der regulären Geschäftszeiten und mit angemessener Vorankündigung sowie unter Einhaltung der geltenden Sicherheitsrichtlinien und Vertraulichkeitsverfahren von Infor (oder dessen Subunternehmer) durchgeführt wird. Wenn Vor-Ort-Prüfungen von physischen Rechenzentren, Systemen oder Einrichtungen nicht zulässig sind, wird Infor mit dem Kunden (und ggf. seinen Unterauftragnehmern) zusammenarbeiten, um eine einvernehmliche Lösung zu finden, die ausreicht, um die Informationen bereitzustellen, die der Kunde benötigt, um die Prüfungsanforderungen gemäß des Geltenden Rechts zur Cybersicherheit und Data-Governance zu erfüllen. Weder der Kunde noch der Prüfer haben Zugang zu Daten von anderen Kunden von Infor oder zu den Systemen von Infor oder Einrichtungen von Infor, die nicht an den für den Kunden erbrachten Dienstleistungen beteiligt sind. Der Kunde stellt die Ergebnisse einer Prüfung Infor zur Verfügung. Die Parteien werden sich einvernehmlich auf entsprechende Berichte oder Abhilfemaßnahmen einigen. Infor wird wirtschaftlich angemessene Anstrengungen unternehmen, um vereinbarte Abhilfemaßnahmen umzusetzen.

7.5 Der Kunde trägt alle Kosten und Gebühren im Zusammenhang mit der Prüfung, einschließlich aller angemessenen Kosten und Gebühren, die Infor für die Prüfung aufwendet, und aller Kosten und Gebühren, die Infor bei einem Subunternehmer entstehen, sofern die Prüfung einen Subunternehmer betrifft, es sei denn, die Prüfung ergibt einen wesentlichen Verstoß von Infor gegen diesen Anhang; in diesem Fall trägt Infor seine eigenen Kosten für den Teil der Prüfung, der mit dem Verstoß zusammenhängt.

III. DORA

1. ANWENDUNGSBEREICH UND DEFINITIONEN

1.1 Die in Abschnitt III dieses Anhangs festgelegten Bedingungen gelten ausschließlich für EU-Kunden, die die Kriterien und Schwellenwerte für Finanzunternehmen erfüllen und somit unter den Anwendungsbereich von DORA fallen. Zur Klarstellung wird Abschnitt I in diesen Abschnitt III aufgenommen. Bestimmte Absätze in Abschnitt II gelten ebenfalls, sofern in diesem Abschnitt III ausdrücklich darauf verwiesen wird.

1.2 **"DORA"** bezeichnet die Verordnung über die digitale operationale Resilienz im Finanzsektor (Verordnung (EU) 2022/2554) des Europäischen Parlaments und des Rates vom 14. Dezember 2022.

2. DIENSTLEISTUNGEN

2.1 Die von Infor an den Kunden erbrachten IKT-Dienstleistungen sind in dem Vertrag beschrieben.

3. STANDORT

3.1 Es wird klargestellt, dass Produktionsdaten des Kunden am ausgewählten Bereitstellungsort gespeichert werden und Infor keine Produktionsdaten des Kunden ohne vorherige schriftliche Zustimmung und Anweisung des Kunden außerhalb dieses Standorts verschieben wird. Auf Anweisung des Kunden kann in begrenztem Umfang auf personenbezogene Daten von außerhalb des ausgewählten Bereitstellungsortes für Unterstützungs- und Supportzwecke des Kunden zugegriffen werden. Infor wird den Kunden im Voraus informieren, wenn eine Änderung der im Vertrag festgelegten Bedingungen der Standorte (d.h. der Regionen oder Länder) beabsichtigt wird, an denen die Dienstleistungen erbracht und die Kundendaten gespeichert und verarbeitet werden.

4. SICHERHEITSPROGRAMM UND SLAS

4.1 Es gelten die oben in Abschnitt II.3 und Abschnitt II.4 beschriebenen Maßnahmen zum Management von Cybersicherheits-Risiken. Die Verpflichtungen von Infor zur Reaktion auf Sicherheitsvorfälle in Abschnitt II.6 gelten ebenfalls. Es wird klargestellt, dass die Insolvenz von Infor als Verpflichtung zur Rückgabe von Kundendaten gemäß dem ISP angesehen wird.

4.2 Die Verfügbarkeitsverpflichtungen von Infor sind im Service Level Agreement unter https://www.infor.com/service-level-description („SLA“) beschrieben. Produktspezifische Support-Verpflichtungen sind im Bestellformular beschrieben, falls diese gelten.

5. PROGRAMME ZUR SCHULUNG UND SENSIBILISIERUNG FÜR IKT-SICHERHEIT

5.1 Sollte Infor im Rahmen der Dienstleistungen auf die Netzwerk-Informationssysteme des Kunden zugreifen, kann der Kunde von Infor verlangen, unter angemessener Vorankündigung, an einem geeigneten Programm zur Sensibilisierung für IKT-Sicherheit und/oder einer Schulung zur digitalen Betriebsfestigkeit teilzunehmen, die der Kunde im Zusammenhang mit seinem Geschäft anbietet oder durchführt („Schulung“). In diesem Zusammenhang vereinbaren die Parteien, dass:

(A) Die Häufigkeit, der Zeitpunkt und die Dauer einer solchen Schulung von den Parteien im Voraus vereinbart wird;

(B) Infor sich das Recht vorbehält, ihre angemessenen und ordnungsgemäß entstandenen Kosten vom Kunden erstatten zu lassen; und

(C) die Teilnahme von Infor nicht dazu führen darf, dass Infor daran verhindert, abgehalten oder beeinträchtigt wird, die IKT-Dienstleistungen zu erbringen oder anderweitig ihre Verpflichtungen aus dem Vertrag zu erfüllen.

6. KÜNDIGUNG

6.1 Zusätzlich zu den im Vertrag und an anderer Stelle in diesen Bedingungen festgelegten Kündigungsrechten kann der Kunde, entsprechend Art. 28 Abs. 7 DORA und vorbehaltlich des Kündigungsverfahrens im Vertrag, den Vertrag ganz oder teilweise nur in den folgenden Fällen kündigen: (i) wenn Infor es versäumt hat, einen erheblichen Verstoß gegen das Geltende Recht zur Cybersicherheit und Data Governance oder diesen Anhang zu beheben; (ii) wenn der Kunde Umstände feststellt, die geeignet sind, die Erbringung der IKT-Dienstleistungen durch Infor zu beeinträchtigen, einschließlich wesentlicher Änderungen, die den Vertrag oder die Situation von Infor betreffen, (iii) wenn nachweisbare Schwächen in Bezug auf das gesamte IKT-Risikomanagement von Infor und insbesondere in Bezug auf die Art und Weise, wie Infor die Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit von Daten, seien es personenbezogene oder anderweitig sensible Daten oder nicht personenbezogene Daten, sicherstellt, festgestellt werden, oder (iv) wenn die zuständige staatliche Behörde den Kunden aufgrund der Bedingungen oder Umstände in Bezug auf Infor oder den Vertrag nicht mehr wirksam beaufsichtigen kann.

7. UMGANG MIT DEN ZUSTÄNDIGEN STAATLICHEN BEHÖRDEN

7.1 Infor wird mit den zuständigen staatlichen Regierungs- und Aufsichtsbehörden des Kunden, einschließlich der von ihnen benannten Personen, uneingeschränkt zusammenarbeiten.

IV. DATENVERORDNUNG

1. ANWENDUNGSBEREICH UND DEFINITIONEN

1.1 Die in Abschnitt IV dieses Anhangs dargelegten Bedingungen gelten ausschließlich für EU-Kunden und nur insoweit, als Infor die Kriterien und Schwellenwerte für einen Anbieter von Datenverarbeitungsdiensten nach der Datenverordnung erfüllt. Zur Klarstellung wird darauf hingewiesen, dass Abschnitt I Bestandteil dieses Abschnitts IV ist; bestimmte Absätze in Abschnitt II gelten ebenfalls, sofern in diesem Abschnitt IV ausdrücklich darauf Bezug genommen wird.

1.2 "**Datenverordnung**" bezeichnet die Verordnung (EU) 2023/2854 des Europäischen Parlaments und des Rates vom 13. Dezember 2023 über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung sowie zur Änderung der Verordnung (EU) 2017/2394 und der Richtlinie (EU) 2020/1828.

2. ZUGRIFF DES KUNDEN AUF DATEN

2.1 Der in Abschnitt II.3 oben beschriebene ISP regelt die Möglichkeit des Kunden, während der Laufzeit des Vertrags auf Kundendaten zuzugreifen, sowie die Rückgabe und Vernichtung von Kundendaten bei Beendigung oder Ablauf der Cloud-Dienste.

3. WECHSELPROZESS

3.1 Wie in diesem Anhang beschrieben, kann der Kunde zu einem Datenverarbeitungsdienst wechseln, der von einem anderen Anbieter von Datenverarbeitungsdiensten angeboten wird, oder Kundendaten auf eine On-Premises IKT-Infrastruktur übertragen, vorbehaltlich des spezifischen Prozesses von Infor ("Wechselprozess"), vorausgesetzt der Kunde:

(A) zeigt dies Infor mindestens zwei (2) Monaten vorher unter Einhaltung der im Vertrag festgelegten Anforderungen für Mitteilungen und Erklärungen schriftlich an;

(B) schließt eine für beide Seiten akzeptable Vereinbarung über Übergangsdienste mit Infor ab, die die unten beschriebenen Informationen enthält; und

(C) zahlt alle anfallenden Gebühren (unten definiert).

3.2 In der Vereinbarung über Übergangsdienste wird Folgendes festgelegt:

(A) Ob der Kunde (i) seine Kundendaten exportiert und zu einem definierten alternativen Anbieter verschiebt, (ii) seine Kundendaten exportiert und von der Cloud auf ein On-Premises System verlagert oder (iii) seine Kundendaten löscht;

(B) Die Kategorien von Kundendaten, die während des Wechsels portiert werden können, sowie die Kategorien von Daten, die aufgrund des Risikos einer Verletzung von Geschäftsgeheimnissen vom Wechsel ausgenommen sind, sofern einschlägig.

(C) Fristen für den Abschluss des Wechselvollzugs, einschließlich der Fristen für den Datenabruf nach Ablauf der zwischen den Parteien vereinbarten Übergangsfrist;

(D) Alle technischen Einschränkungen oder sonstige Einschränkungen der Durchführbarkeit des Wechsels, einschließlich gegebenenfalls Details zur Interoperabilität, die von Infor zur Verfügung gestellt werden;

(E) Anfallende Gebühren für den Wechsel, einschließlich der Folgenden:

(1) der volle Betrag, der für die gesamte aktuelle verbindlich vereinbarte Abonnement-Laufzeit, die in dem zugrundeliegenden Bestellformular vereinbart ist, und noch an Infor zu zahlen ist (dieser Betrag fällt nicht unter den Begriff "Wechselentgelt" und fällt gesondert hierzu an); und;

(2) Wechselentgelte, soweit dies nach geltendem Recht zulässig ist; und

(F) Alle zusätzlichen Unterlagen, die vom Kunden ausgeführt werden müssen, wie z. B. ein neuer On-Premises-Software-Lizenzvertrag, der den Cloud Services-Vertrag ersetzt, wenn der Kunde den in Abschnitt IV.3.2(A)(ii) oben beschriebenen Wechsel durchführt.

3.3 Während des Wechselvollzugs wird Infor:

(A) das gleiche Sicherheitsniveau beibehalten, wie es im jeweiligen zugrundeliegenden ISP beschrieben ist;

(B) mit der gebotenen Sorgfalt handeln, um Geschäftskontinuität aufrechtzuerhalten und die Bereitstellung der Cloud-Services gemäß den Verträgen mit dem Kunden fortzusetzen; und

(C) den Kunden (und andere vom Kunden autorisierte Dritte, die schriftlichen oder beruflichen Geheimhaltungsverpflichtungen unterliegen), angemessen zu unterstützen, einschließlich der angemessenen Unterstützung der Ausstiegsstrategie des Kunden, durch Transparenz und der Zur-Verfügung-Stellung auf Anfrage des Kunden von allgemein verfügbarer Information, die für den

Wechsel relevant ist, einschließlich Information in Bezug auf die Interoperabilität exportierter Kundendaten. Ungeachtet des Vorstehenden ist Infor nicht verpflichtet, Informationen weiterzugeben oder dem Kunden (oder anderen Dritten) Unterstützung zu leisten, die ein Risiko für das geistige Eigentum und die Geschäftsgeheimnisse von Infor darstellen oder einen wirtschaftlichen Nachteil für Infor darstellen würden.

3.4 Der Kunde ist für den Import und die Implementierung von Kundendaten in seine eigenen Systeme bzw. in die Systeme des übernehmenden Anbieters verantwortlich.

3.5 Im Rahmen der Datenverordnung können die Parteien, die in der Vereinbarung über Übergangsdienste festgelegten Fristen verlängern.

3.6 Sobald der Wechsel abgeschlossen ist (oder nach Ablauf der zweimonatigen Anzeigefrist, wenn der Kunde keinen Wechsel wünscht, sondern stattdessen die Löschung seiner Kundendaten bei Beendigung der Cloud-Services haben möchte), gelten das/die zugrundeliegende(n) Bestellformular(e) und alle zugrundeliegenden Verträge mit dem Kunden als beendet.

3.7 Infor und der Kunde (und gegebenenfalls der vom Kunden benannte alternative Anbieter) arbeiten nach Treu und Glauben zusammen, den Wechsel effektiv zu gestalten, die rechtzeitige Übertragung von Kundendaten zu ermöglichen und die Kontinuität des Datenverarbeitungsdienstes aufrechtzuerhalten.

3.8 Infor ist nicht verpflichtet, einen Wechsel anzubieten für:

(A) Nicht-Produktionsumgebungen, die zu Test- und Evaluierungszwecken und für einen begrenzten Zeitraum genutzt werden;

(B) Dienste, die ein hochkomplexen oder kostspieligen Wechsel erfordern oder bei denen ein Wechsel ohne erhebliche Eingriffe in die Kundendaten oder die Servicearchitektur unmöglich ist; und/oder

(C) Dienste, bei denen die meisten zentralen Funktionen auf die spezifischen Bedürfnisse eines einzelnen Kunden zugeschnitten wurden oder wenn alle Komponenten für die Zwecke eines einzelnen Kunden entwickelt wurden und wenn diese Datenverarbeitungsdienste nicht im größeren kommerziellen Maßstab über den Dienstleistungskatalog des Anbieters von Datenverarbeitungsdiensten angeboten werden.

3.9 Infor ist nicht verpflichtet, neue Technologien oder Dienste zu entwickeln oder digitale Vermögenswerte, die durch Rechte des geistigen Eigentums geschützt sind oder ein Geschäftsgeheimnis darstellen, gegenüber einem Kunden oder einem anderen Anbieter von Datenverarbeitungsdiensten offenzulegen oder die Sicherheit und Integrität des Kunden oder von Infor zu beeinträchtigen.

4. HAFTUNG UND ENTSCHÄDIGUNG

4.1 Mehrere juristische Personen können berechtigt sein, Dienstleistungen im Rahmen der Verträge zu erwerben oder zu nutzen (einschließlich, aber nicht beschränkt auf Verbundene Unternehmen des Kunden und Autorisierte User), und solche anderen juristischen Personen als der Kunde, der den Antrag zum Wechsel gestellt hat, könnten daher von dem Antrag zum Wechsel gemäß diesem Abschnitt betroffen sein ("Betroffene Parteien"). Es liegt in der alleinigen Verantwortung des Kunden, sicherzustellen, dass der Kunde über alle Rechte und Berechtigungen in Bezug auf den Wechsel und Kundendaten verfügt, bevor er seine Rechte aus diesem Vertrag ausübt.

4.2 Der Kunde verteidigt, entschädigt und hält Infor schadlos von und gegen alle Verluste, Kosten und Aufwendungen, soweit diese sich aus Ansprüchen, Forderungen, Klagen oder Verfahren ergeben, die von Betroffenen Parteien gegen Infor erhoben oder eingeleitet werden und in denen behauptet wird, dass der Antrag zum Wechsel die Rechte oder Lizenzen der Betroffenen Partei verletzt, vorausgesetzt, dass Infor (A) den Kunden unverzüglich schriftlich über einen solchen Anspruch gegen Infor informiert, (B) dem Kunden die alleinige Kontrolle über die Abwehr und Beilegung eines solchen Anspruchs gegen Infor überträgt (mit der Ausnahme, dass der Kunde einen solchen Anspruch gegen Infor nicht beilegen kann, es sei denn, er entbindet Infor bedingungslos von jeglicher Haftung und verlangt von Infor nicht die Zahlung von Geld oder ein Schuldeingeständnis), und (C) dem Kunden auf dessen Kosten jede angemessene Unterstützung gewährt. Die oben genannten Verteidigungs- und Entschädigungsverpflichtungen gelten nicht, wenn sich ein solcher Anspruch gegen Infor aus der Verletzung der Verträge, einschließlich dieses Anhangs, und/oder der zugrundeliegenden Bestellformulare durch Infor ergibt.

4.3 Infor haftet nicht für Schäden, Verluste, Kosten oder Aufwendungen, die sich aus oder im Zusammenhang mit dem Antrag zum Wechsel ergeben. Dieser Haftungsausschluss umfasst unter anderem Probleme im Zusammenhang mit der Integrität oder dem Verlust von Kundendaten, Systemausfallzeiten, Kompatibilitätsproblemen oder anderen Unterbrechungen oder Ausfällen, die während oder als Folge des Antrags zum Wechsel auftreten können. Der Kunde übernimmt die volle Verantwortung für den erfolgreichen Wechsel der Kundendaten.

4.4 Zur Klarstellung: Nichts in diesem Abschnitt IV entbindet oder schränkt die Verpflichtung des Kunden ein, alle im Rahmen der Verträge und/oder eines Bestellformulars fälligen Gebühren für die gesamte aktuelle verbindliche Abonnement-Laufzeit zu zahlen, die in den jeweiligen zugrundeliegenden Bestellformularen festgelegt ist. Wenn sich der Kunde vor Ablauf der aktuellen Abonnement-Laufzeit des zugrundeliegenden Bestellformulars für einen Wechsel entscheidet, erkennt der Kunde an und stimmt zu, dass ein solcher Wechsel den Kunden unter keinen Umständen zu einer Rückerstattung der zuvor im Rahmen der zugrundeliegenden Verträge und/oder des zugrundeliegenden Bestellformulars gezahlten Gebühren berechtigt.

5. BEHÖRDLICHES ZUGRIFFSVERLANGEN

5.1 Für den Fall, dass Infor rechtsverbindliche Anfragen einer Behörde zur Offenlegung von in der EU gehosteten nicht personenbezogenen Daten eines EU-Kunden erhält oder Anfragen einer Behörde zum direkten Zugriff auf in der EU gehosteten nicht personenbezogene Daten eines EU-Kunden erhält, wird Infor, soweit gesetzlich zulässig, versuchen, diese Anfrage an den Kunden umzuleiten. Wenn Infor die Anfrage nicht an den Kunden umleiten kann, wird Infor (i) die Anfrage ablehnen, es sei denn, das Befolgen der Anfrage ist gesetzlich vorgeschrieben, (ii) solche Anfragen anfechten, die im Konflikt mit geltendem Recht stehen, zu weit gefasst sind oder ein anderer angemessener Einwand erhoben werden kann, (iii) den Kunden unverzüglich benachrichtigen und eine Kopie der Anfrage bereitstellen, sofern dies nicht gesetzlich verboten ist, (iv) wenn Infor dazu gezwungen ist, nur die Mindestmenge an in der EU gehosteten nicht-personenbezogenen Daten eines EU-Kunden, offenzulegen, die zur Erfüllung der Anfrage erforderlich ist, und (v) wenn dies nach dem Recht des Bestimmungslandes zulässig ist, auf schriftliche Anfrage des Kunden (nicht mehr als einmal jährlich für die Dauer der Verträge) dem Kunden so viele relevante Informationen wie möglich über empfangene Zugriffsverlangen zur Verfügung zu stellen. Zur Vermeidung von Missverständnissen wird darauf hingewiesen, dass behördliche Zugriffsverlangen in Bezug auf personenbezogene Daten separat in der zwischen den Parteien abgeschlossenen Datenverarbeitungsvereinbarung ("DPA") geregelt sind.