

Ergänzung zur Datensicherheit und zum Datenschutz

1. Bezeichnung der Parteien

Die Parteien vereinbaren, dass für alle Daten, die sie von oder im Auftrag des Unternehmens oder anderweitig im Zusammenhang mit der Erfüllung der Verpflichtungen des Lieferanten erhalten („Unternehmensdaten“), das Unternehmen der Verantwortliche und der Lieferant der Auftragsverarbeiter ist. Jede Partei verpflichtet sich, alle relevanten Datenschutzgesetze und die jeweiligen Verpflichtungen aus dieser Ergänzung einzuhalten. Der Lieferant stellt sicher, dass jeder Unterauftragsverarbeiter, der Zugang zu Unternehmensdaten hat, die Verpflichtungen des Lieferanten aus dieser Ergänzung erfüllt.

2. Verwendung personenbezogener Daten

Alle personenbezogenen oder einzigartigen Informationen zu einer bestimmten Person und alle sensiblen finanziellen Informationen über oder von Personen, einschließlich aller Informationen, die verwendet werden können, um eine bestimmte Person zu identifizieren oder zu kontaktieren, wie Vor- und Nachname, E-Mail-Adresse, Telefonnummer, Sozialversicherungsnummer, Kontodaten, Kreditkartennummer oder andere Daten („personenbezogene Daten“), werden vom Lieferanten nur dann abgerufen, verwendet, gepflegt, erfasst, geändert, zusammengeführt, weitergegeben oder offengelegt, wenn dies für die Erfüllung seiner Verpflichtungen aus einem Vertrag mit dem Unternehmen erforderlich ist oder wenn dies anderweitig vom Unternehmen verlangt wird. Bei der Verarbeitung von personenbezogenen Daten im Auftrag des Unternehmens stellt der Lieferant sicher, dass jede Person, die in seinem Auftrag oder unter seiner Aufsicht handelt, die personenbezogenen Daten nur gemäß den schriftlichen Anweisungen des Unternehmens verarbeitet. Der Lieferant informiert das Unternehmen unverzüglich über alle geltenden gesetzlichen Anforderungen, die eine Verarbeitung der Daten in einer Weise erfordern, die von den Verarbeitungsanweisungen abweicht, es sei denn, diese Informationen sind durch dieses Gesetz verboten, oder die Verarbeitungsanweisungen können gegen geltende Gesetze verstoßen.

3. Datenschutz- und Sicherheitsrichtlinie

Der Lieferant ergreift auf eigene Kosten geeignete technische und organisatorische Maßnahmen im Zusammenhang mit der Verarbeitung von Unternehmensdaten und personenbezogenen Daten durch den Lieferanten und hält diese aufrecht, um die Einhaltung der geltenden Datenschutzgesetze sicherzustellen. Darüber hinaus gewährleistet der Lieferant, dass er rechtlich und betrieblich ausreichende technische Maßnahmen ergriffen und umgesetzt hat, um die Daten vor unbeabsichtigter, unbefugter oder unrechtmäßiger Vernichtung, Verlust, Veränderung, Offenlegung und Zugriff sowie vor allen anderen unrechtmäßigen Aktivitäten zu schützen. Der Lieferant stellt sicher, dass seine Mitarbeiter und Vertreter, die Unternehmensdaten und personenbezogene Daten im Auftrag des Unternehmens verarbeiten, Vereinbarungen unterzeichnet haben, die sie verpflichten, Unternehmensdaten und personenbezogene Daten vertraulich zu behandeln und alle angemessenen Schritte zu unternehmen, um sicherzustellen, dass die Vertreter des Lieferanten, die Unternehmensdaten und personenbezogene Daten verarbeiten, eine angemessene Schulung über die Einhaltung dieser Ergänzung und der einschlägigen Gesetze erhalten.

4. Mitarbeiter und Unterauftragnehmer

Der Lieferant ist nicht berechtigt, einen anderen Auftragsverarbeiter damit zu beauftragen, im Auftrag des Unternehmens bestimmte Vorgänge durchzuführen, die die Verarbeitung Unternehmensdaten oder personenbezogener Daten beinhalten, ohne vorher die schriftliche Zustimmung des Unternehmens einzuholen. Wenn das Unternehmen seine schriftliche Zustimmung erteilt, schließt der Lieferant einen verbindlichen schriftlichen Vertrag mit dem Unterauftragsverarbeiter ab („Verarbeitungsvertrag“), der dem Unterauftragsverarbeiter dieselben Verpflichtungen in Bezug auf den Datenschutz auferlegt, wie die Verpflichtungen, die in dieser Ergänzung enthalten sind. Auf Anforderung des Unternehmens stellt der Lieferant Kopien der abgeschlossenen Verarbeitungsverträge zur Verfügung. Der Lieferant stellt sicher, dass Dritte, die befugte Empfänger von Unternehmensdaten oder personenbezogenen Daten sind, zugestimmt haben, die Informationen nur für die Geschäftszwecke des Unternehmens und in Übereinstimmung mit allen geltenden Gesetzen, Regeln und Vorschriften sowie allen Unternehmensrichtlinien und in Übereinstimmung mit den in dieser Ergänzung beschriebenen Sicherheitsverfahren zu verwenden.

5. Zusammenarbeit, Überprüfung und Inspektionen

Der Lieferant bietet dem Unternehmen die angemessene Unterstützung, Informationen und Kooperation, um sicherzustellen, dass die Verpflichtungen des Unternehmens eingehalten werden, die sich aus den relevanten Gesetzen ergeben, insbesondere in Bezug auf: (i) Datensicherheit; (ii) Benachrichtigungen über Datenschutzverletzungen; (iii) die Beantwortung von Anfragen von Regulierungsbehörden oder Einzelpersonen in Bezug auf Unternehmensdaten oder personenbezogenen Daten und/oder die Datenschutz- oder Sicherheitspraktiken des Unternehmens; und (iv) die Durchführung von Datenschutz-Folgenabschätzungen. Der Lieferant ergreift auf eigene Kosten geeignete technische und organisatorische Maßnahmen und erhält diese aufrecht, um das Unternehmen bei der Erfüllung seiner Verpflichtungen, auf Anfragen von Einzelpersonen in Bezug auf Datenschutzdaten zu reagieren, zu unterstützen. Dazu gehört auch, dass alle Anfragen in Bezug auf Unternehmensdaten oder personenbezogene Daten aufgezeichnet und innerhalb von drei Tagen nach Eingang der Anfrage an das Unternehmen weitergeleitet werden. Das Unternehmen behält sich das Recht vor, vor Ort stichprobenartige Überprüfungen durchzuführen, um sicherzustellen, dass der Lieferant seinen Verpflichtungen aus dieser Ergänzung in Bezug auf den Datenschutz nachkommt, wobei das Unternehmen den Lieferanten innerhalb einer angemessenen Frist im Voraus darüber informiert und sicherstellt, dass die Prüfer verbindlichen Vertraulichkeitsverpflichtungen unterliegen und dass die Überprüfung oder Inspektion so durchgeführt

wird, dass sie nur eine minimale Unterbrechung der Geschäftstätigkeit des Lieferanten und anderer Kunden verursacht. Der Lieferant arbeitet auch auf andere Weise mit dem Unternehmen zusammenarbeiten, um die Einhaltung der Verpflichtungen durch den Lieferanten zu überwachen.

6. Kein Export (Lieferanten oder Dienstleistungen mit Sitz im EWR)

Der Lieferant darf keine Unternehmensdaten in ein Land außerhalb des Europäischen Wirtschaftsraums („EWR“) oder an eine internationale Organisation (ein „Internationaler Empfänger“) übermitteln, ohne die vorherige schriftliche Zustimmung des Unternehmens einzuholen. Wenn das Unternehmen der Übermittlung von Unternehmensdaten an einen internationalen Empfänger zustimmt, hat der Lieferant dafür zu sorgen, dass diese Übermittlung (und jede weitere Übermittlung) unter folgenden Bedingungen erfolgt: (i) auf der Grundlage eines schriftlichen Vertrags, der Bestimmungen über die Sicherheit und Vertraulichkeit aller personenbezogener Daten enthält; (ii) gemäß einem rechtlich durchsetzbaren Mechanismus für grenzüberschreitende Datenübermittlungen von personenbezogenen Daten, die gemäß den relevanten Gesetzen durchgeführt werden (deren Form und Inhalt der schriftlichen Zustimmung des Unternehmens bedarf); (iii) unter Einhaltung der vorliegenden Ergänzung; und (iv) unter Einhaltung der sonstigen relevanten Datenschutzgesetze.

7. Dokumentation

Der Lieferant führt vollständige, genaue und aktuelle schriftliche Aufzeichnungen über alle im Auftrag des Unternehmens durchgeführten Verarbeitungsaktivitäten („Verarbeitungsunterlagen“) und stellt dem Unternehmen auf Anfrage rechtzeitig die Informationen (einschließlich der Verarbeitungsunterlagen) zur Verfügung, die das Unternehmen vernünftigerweise benötigt, um die Einhaltung der Verpflichtungen des Lieferanten gemäß den relevanten Datenschutzgesetzen und dieser Ergänzung nachzuweisen, die das Unternehmen den Aufsichtsbehörden gegenüber offenlegen kann. Die Verarbeitungsunterlagen müssen mindestens eine Beschreibung aller vom Lieferanten im Auftrag des Unternehmens verarbeiteten personenbezogenen Daten, die Art der Verarbeitung, den Zweck der Verarbeitung, eine Einwilligungserklärung (falls vorhanden) und alle anderen Informationen enthalten, die das Unternehmen vernünftigerweise benötigt.

8. Verletzungen des Schutzes personenbezogener Daten

Im Falle eines tatsächlichen oder vermuteten Zugriffs auf oder einer tatsächlichen oder vermuteten Beschaffung von Unternehmensdaten oder personenbezogenen Daten durch einen unbefugten Dritten ist der Lieferant verpflichtet, das Unternehmen unverzüglich (spätestens jedoch 12 Stunden nach Bekanntwerden der potenziellen Datenschutzverletzung) über die potenzielle Datenschutzverletzung zu informieren und dem Unternehmen unverzüglich schriftlich oder per E-Mail (wenn möglich innerhalb von 24 Stunden nach Bekanntwerden der potenziellen Datenschutzverletzung) Einzelheiten mitzuteilen, die das Unternehmen vernünftigerweise verlangt. Darüber hinaus verpflichtet sich der Lieferant, die potenzielle Datenschutzverletzung zu untersuchen und zu beheben, und, falls eine Datenschutzverletzung dazu führt, dass der Lieferant oder das Unternehmen rechtlich verpflichtet sind, die betroffenen Personen zu benachrichtigen oder falls die potenzielle Datenschutzverletzung betroffene Personen gefährden könnte, verpflichtet sich der Lieferant, dem Unternehmen Zusicherungen geben, die für das Unternehmen zufriedenstellend sind, dass sich eine Verletzung des Schutzes Unternehmensdaten oder personenbezogener Daten nicht wiederholt. Der Lieferant gewährleistet, dass bei einer Verletzung des Schutzes Unternehmensdaten oder personenbezogener Daten alle erforderlichen Schritte dokumentiert werden und dass nach einem Vorfall eine Überprüfung sowohl der Ereignisse als auch der gegebenenfalls ergriffenen Maßnahmen zur Änderung der Geschäftspraktiken in Bezug auf die Datenschutzbestimmungen durchgeführt wird. Der Lieferant verpflichtet sich, mit dem Unternehmen bei der Bearbeitung der Angelegenheit, insbesondere bei allen Untersuchungen, Berichten oder anderen Verpflichtungen, die nach geltenden Gesetzen oder Vorschriften erforderlich sind, einschließlich der Beantwortung von behördlichen Anfragen oder Untersuchungen, oder bei anderen Anfragen des Unternehmens, uneingeschränkt zu kooperieren und mit dem Unternehmen zusammenzuarbeiten, um anderweitig auf Schäden, die durch die Verletzung verursacht wurden, zu reagieren und diese zu beheben. Der Lieferant ist nicht berechtigt ohne vorherige schriftliche Genehmigung des Unternehmens Dritte über die Verletzung zu informieren.

9. Informationsmanagement

Der Lieferant verpflichtet sich, auf schriftliche Aufforderung des Unternehmens unverzüglich alle Unternehmensdaten oder personenbezogenen Daten entweder sicher zu löschen oder in Papierform oder in elektronischer Form an das Unternehmen zurücksenden, sobald die Verarbeitung der Unternehmensdaten oder personenbezogenen Daten durch den Lieferanten nicht mehr für die Erfüllung der Verpflichtungen des Lieferanten aus der schriftlichen Vereinbarung des Lieferanten mit dem Unternehmen („Lieferantenvertrag“) erforderlich ist. So schnell wie möglich nach Erbringung der Dienstleistungen im Lieferantenvertrag löscht der Lieferant alle vorhandenen Kopien von Unternehmensdaten oder personenbezogenen Daten in elektronischer und gedruckter Form sicher, es sei denn, die Speicherung von Daten ist nach geltenden Gesetzen erforderlich, und wenn ja, teilt der Lieferant dies dem Unternehmen schriftlich mit.

10. Schadenersatz und Unterlassungsansprüche

Der Lieferant stimmt zu, dem Unternehmen alle Kosten zu erstatten und das Unternehmen gegen alle Kosten schadlos zu halten, die anfallen, um auf Schäden zu reagieren und/oder diese zu beheben, die durch einen Verstoß gegen die vorliegende Ergänzung verursacht werden, einschließlich Verletzungen des Schutzes Unternehmensdaten oder personenbezogener Daten und aller Handlungen, die sich daraus ergeben, dass der Lieferant außerhalb oder entgegen den gesetzlichen Anweisungen des Unternehmens handelt oder dass der Lieferant seine Verpflichtungen zum

Datenschutz und zum Schutz der Privatsphäre gemäß dieser Ergänzung wesentlich verletzt. Außerdem erkennt der Lieferant an und stimmt zu, dass im Falle eines drohenden oder tatsächlichen Verstoßes gegen diese Ergänzung ein irreparabler Schaden entsteht, für den ein Schadenersatz kein ausreichendes Rechtsmittel darstellt, und dass der Lieferant neben allen anderen Rechtsmitteln berechtigt ist, bestimmte Leistungs- und Unterlassungsansprüche geltend zu machen, insbesondere zum Schutz vor der Offenlegung oder missbräuchlichen Verwendung von Unternehmensdaten oder personenbezogenen Daten, als Rechtsmittel für einen solchen Verstoß des Lieferanten gegen diese Ergänzung ohne Sicherheit und unbeschadet anderer Rechte, die gemäß dieser Ergänzung oder gemäß geltenden Gesetzen verfügbar sind. Darüber hinaus gilt die Nichteinhaltung einer der Bestimmungen dieser Ergänzung durch den Lieferanten als wesentlicher Vertragsbruch, und das Unternehmen kann die Lieferantenvertrag gegenüber dem Lieferanten kündigen, ohne haftbar zu sein. Im Falle eines Rechtsstreits im Zusammenhang mit dieser Ergänzung haftet die nicht obsiegende Partei gegenüber der obsiegenden Partei und zahlt ihr und ihren Mitarbeitern, Beratern, Vertretern und verbundenen Unternehmen die angemessenen Anwaltskosten, die ihr im Zusammenhang mit diesem Rechtsstreit, einschließlich etwaiger Rechtsmittel, entstehen.