Lieferantenverträge

Best Practice

Die folgenden Leitfragen an Ihre Lieferanten bilden die Grundlage für die Ausarbeitung eines Lieferantenvertrags. Hierbei sollten Sie (abhängig vom Lieferanten) folgende Schlüsselelemente in Ihren Verträgen berücksichtigen, um insbesondere der Cybersicherheit als auch den Datenschutzanforderungen gerecht zu werden:

1. Die Verpflichtung, eigene Informatikmittel (also alle IT-Systeme und Netzwerke) gemäss aktuellem Stand der Technik vor Cyberangriffen dem Risiko angemessen zu schützen.
2. Die Verpflichtung, moderne, gewartete und dem Industriestandard entsprechende Verschlüsselungsmethoden zu verwenden, um sensible Daten bei der Übertragung zwischen Systemen und im Ruhestand in Online-Datenspeichern und Backups zu schützen.
3. Die Verpflichtung zur Zugriffstransparenz zwecks nachvollziehbarer Erstellung wer, wann. auf welche Daten oder Systeme zugreift.
4. Die Verpflichtung, Cyberangriffe, Datenschutzverletzungen und Schwachstellen der Organisation (innerhalb gewisser Stunden / Tage) an eine vordefinierte Stelle zu melden, damit schnell und adäquat auf Sicherheitsvorfälle reagiert werden kann.
5. Die Verpflichtung, entdeckte Schwachstellen umgehend auf eigene Kosten (Materialkosten, Arbeitsstunden und möglicherweise auch Kosten für externe Dienstleister) zu patchen.
6. Die Verpflichtung, dass der Lieferant bei der Bearbeitung von Daten die Anforderungen und Vorgaben des Datenschutzgesetzes (DSG) einhält. Namentlich ist darauf hinzuweisen, dass nur die für die Aufgabenerfüllung notwendigen Daten erhoben und verarbeitet werden sollen.
7. Die Verpflichtung, eine Liste sensibler Datentypen zu führen, die von Anwendungen verarbeitet werden sollen.
8. Die Verpflichtung, ein aktuelles Diagramm zu führen, aus dem hervorgeht, wie sensible Daten in die Systeme des Lieferanten gelangen und wo sie schliesslich gespeichert werden.
9. Die Verpflichtung, Informationen, welche der Lieferant über die Organisation hat, regelmässig mitzuteilen sowie, wenn nicht mehr benötigt, zu vernichten.
10. Definition der Service Level Agreements (SLAs) für die Bereitstellung der Dienstleistungen (z. B. Festlegung konkreter Leistungskriterien sowie Qualitätsstandards, welche der Lieferant erfüllen muss, welches die Kriterien für die Leistungsbewertungen und die Konsequenzen für die Nichterfüllung der Standards sind).
11. Aufnahme von Unter-Lieferanten/Subunternehmer-Regelungen: Verlangen Sie für den Fall, dass der Lieferant Unterlieferanten/Subunternehmer einsetzt, dass diese und die von ihm eingesetzten Mitarbeitenden denselben Cybersicherheits- und Datenschutzstandards unterliegen, die auch für den Hauptlieferanten gelten. Führen Sie eine Klausel ein, die eine vorherige Genehmigung für das Hinzufügen oder Ändern von Unterlieferanten/Subunternehmern durch Ihre Organisation erfordert.
12. Die Verpflichtung, eine Liste von Unter-Lieferanten (Drittunternehmen) zu führen, die Zugang zu Kundendaten haben. Diese Liste muss jederzeit auf Anfrage eingesehen werden können.
13. Eventuell die Verpflichtung, einen halbjährlichen Nachweis der eigenen Cybersicherheit zu erbringen, um die Compliance und Wirksamkeit der Sicherheitsmassnahmen zu gewährleisten (gegebenenfalls wäre im Vertrag die Form wie Sicherheitsaudits zu konkretisieren und es können detaillierte Anforderungen an die Sicherheitsaudits über den Status der Cybersicherheitsmassnahmen aufgeführt werden [z. B. Audits von einer unabhängigen und anerkannten Unternehmung], Protokollierungs-, Überwachungs- und Aufbewahrungspflichten des Lieferanten durch Überwachungssysteme vorgesehen werden, um verdächtige Aktivitäten oder potenzielle Sicherheitsverletzungen zu erkennen sowie die Erstellung eines Incident Response Plans, welcher klare Richtlinien für die Benachrichtigung, Eindämmung und Untersuchung von Sicherheitsvorfällen beinhaltet).
14. Eventuell Aufnahme von Haftungsklauseln, die den Lieferanten für direkte, indirekte und Folgeschäden haftbar macht, die durch Nichteinhaltung der Vertragspflichten entstehen, sowie von Konventionalstrafen bei einer Verletzung der vertraglichen Pflichten zur Cybersicherheit sowie zum Datenschutz.
15. Eventuell Forderung einer Haftpflicht- und/oder Cybersicherheitsversicherung für verursachten Schaden, wenn dieser durch Nichteinhalten von Verpflichtungen sowie durch Datenschutz und Datenschutzverletzungen entstanden ist.

\* \* \* \* \*