Verpflichtungserklärung zur Informationssicherheit für Lieferanten

Inhaltsverzeichnis

1 Einleitung

MARKGRAF arbeitet seit mehreren Jahren daran, Cyber-Risiken für sich, seine Kunden und Lieferanten zu minimieren. MARKGRAF ist bereits seit 2022 nach ISO 27001 zertifiziert und sorgt mit einem Informationssicherheitsmanagementsystem für die Sicherheit von Informationen, Daten und Systemen. Diese Verpflichtungserklärung zur Informationssicherheit (im Folgenden „Verpflichtungserklärung“) legt die Mindestanforderungen an die Informationssicherheit fest, die von Lieferanten (im Folgenden „Lieferant“) erfüllt werden müssen, um die vertraulichen, integren und verfügbaren Informationen und Daten von MARKGRAF zu schützen.

Diese Lieferantenverpflichtung gilt für alle Lieferanten und Dienstleister. MARKGRAF behält sich jedoch vor, für Lieferanten in besonders sicherheitssensitiven Beziehungen, gesonderte Ergänzungen zu dieser Verpflichtungserklärung individuell zu vereinbaren.

2 Schutz der Vertraulichkeit

Vertraulichkeit bedeutet, dass Informationen und Daten, abhängig von Ihrer Klassifizierung, vor Offenlegung gegenüber unberechtigten Dritten zu schützen und deren Zugang zur Verarbeitung dieser Art von Informationen und Daten sehr restriktiv zu steuern und zu überwachen sind. Der Verlust der Vertraulichkeit kann

- internen / externen Imageverlust,
- finanzielle Einbußen,
- Gesetzesverstöße und
- existenzielle Bedrohungen für das Unternehmen nach sich ziehen.

Der Lieferant verpflichtet sich, alle Informationen und Daten von MARKGRAF, die im Rahmen der Geschäftsbeziehung zur Verfügung gestellt oder zugänglich gemacht werden, vertraulich zu behandeln. MARKGRAF setzt voraus, dass mit den eigenen Informationen und Daten sowie den Informationen und Daten von Dritten genau so verfahren wird.

Dies umfasst:

- Keine Weitergabe vertraulicher Informationen an unbefugte Dritte.
- Sicherstellung, dass nur autorisierte Mitarbeitende des Lieferanten Zugang zu vertraulichen Informationen und Daten haben und, dass diese Mitarbeitenden über die Vertraulichkeitsverpflichtungen informiert bzw. darauf verpflichtet sind.
- Nutzung vertraulicher Informationen und Daten darf ausschließlich für den Zweck erfolgen, für den sie bereitgestellt wurden.

Zusätzlich gilt die den Vertragsunterlagen beigelegte Version der Geheimhaltungsvereinbarung von MARKGRAF.

3 Schutz der Integrität

In der Informationssicherheit bedeutet Integrität die Sicherstellung der Unversehrtheit und Korrektheit von Informationen und Daten der Kunden, Dritter sowie der eigenen. Das Ziel ist es, Informationen und Daten vor unbemerkten Veränderungen zu schützen, sodass sie vollständig und unverändert bleiben.

Es gibt zwei Hauptaspekte der Integrität:

- **Datenintegrität:** Sicherstellung, dass Informationen und Daten nicht unbemerkt verändert werden können.
- **Systemintegrität:** Sicherstellung der korrekten Funktionsweise von IT-Systemen und Anwendungen.

Der Lieferant verpflichtet sich, Maßnahmen zu ergreifen, um die Integrität der Informationen und Daten von MARKGRAF, der eigenen Systeme, Informationen und Daten sowie der Informationen und Daten Dritter zu schützen.

Dazu gehören:

- Implementierung von Kontrollmechanismen, um Änderungen, Löschungen oder unbefugte Zugriffe auf Daten zu verhindern.
- Regelmäßige Überprüfung und Aktualisierung von Sicherheitsmaßnahmen, um sicherzustellen, dass sie den aktuellen Bedrohungen und Risiken entsprechen.
- Nutzung sicherer Kommunikationsmethoden für den Austausch von Informationen, z. B. Transportverschlüsselung von E-Mails und Datenübertragungen.

4 Sicherstellung der Verfügbarkeit

In der Informationssicherheit steht „Verfügbarkeit“ für die Garantie, dass Dienstleistungen, Funktionen eines IT-Systems, IT-Anwendungen oder IT-Netzen oder auch von Informationen und Daten der Kunden stets wie vorgesehen und vertraglich vereinbart genutzt werden können.

Der Lieferant verpflichtet sich, Maßnahmen zur Sicherstellung der Verfügbarkeit der Informationen, Daten und Systeme von und für MARKGRAF, der eigenen Systeme, Informationen und Daten sowie die Informationen und Daten Dritter zu ergreifen, wenn diese im Verantwortungsbereich des Lieferanten sind. Dazu gehören:

- Implementierung von Backup- und Wiederherstellungsverfahren, um Datenverlust zu verhindern.
- Durchführung regelmäßiger Tests der Backup- und Wiederherstellungsverfahren, um ihre Wirksamkeit zu gewährleisten.
- Ergreifen von Maßnahmen zur Minimierung von Ausfallzeiten und zur schnellen Wiederherstellung des Betriebs im Falle eines Vorfalls.

5 Sicherheitsmanagement

Der Lieferant verpflichtet sich zur Implementierung und Aufrechterhaltung von Prozessen und Verfahren im Bereich Informationssicherheit (bzw. Umsetzung eines Informationssicherheits-managementsystems), das mindestens folgende Anforderungen erfüllt:

- Benennung eines Verantwortlichen für die Informationssicherheit, der für die Umsetzung und Überwachung der Sicherheitsmaßnahmen verantwortlich ist.
- Durchführung regelmäßiger Risikoanalysen, um potenzielle Bedrohungen zu identifizieren und entsprechende Gegenmaßnahmen zu ergreifen.
- Dokumentation und regelmäßige Überprüfung aller Sicherheitsrichtlinien und -verfahren.
- Schulung der Mitarbeitenden in Bezug auf Informationssicherheit und Sensibilisierung für Sicherheitsrisiken.

Sicherheitsmanagementsysteme nach ISO 27001 und deren Zertifizierung gelten als umfassender Nachweis gelebter Informationssicherheit.

6 Umsetzung von technischen Sicherheitsmaßnahmen

Für die lieferanteneigenen IT-Systeme auf denen Informationen von MARKGRAF verarbeitet werden, verpflichtet sich der Lieferant angemessene Sicherheitsmaßnahmen, die dem Stand der Technik entsprechen, umzusetzen.

Darunter fallen:

- Einsatz von modernen Anti-Virus-Lösungen
- Einsatz von modernen Firewalls
- Zeitnahe technische Aktualisierung aller IT-Komponenten (Patch Management)
- Mechanismen zur Protokollierung von Sicherheitsereignissen und deren Meldung
- Endgeräte-Verschlüsselung (Festplattenverschlüsselung)
- Einsatz von E-Mail-Sicherheitslösungen
- Kontrolle und Management von externen Datenträgern

7 Verfahren für die Behandlung von Sicherheitsvorfällen

Der Lieferant verpflichtet sich, ein Verfahren für das Management von Sicherheitsvorfällen zu implementieren, das Folgendes umfasst:

- Nach Kenntnisnahme ohne schuldhaftes Zögern Benachrichtigung von MARKGRAF über Sicherheitsvorfälle und Incidents, die die Daten, Informationen oder Systeme von MARKGRAF betreffen könnten.
- Ergreifen von Sofortmaßnahmen zur Eindämmung und Behebung von Vorfällen oder Incidents in Abstimmung mit MARKGRAF, die Informationen oder Systeme von MARKGRAF betreffen könnten.
- Zusammenarbeit mit MARKGRAF bei der Untersuchung und Analyse des Vorfalls, wenn es Informationen oder Systeme von MARKGRAF betrifft, sowie bei der Implementierung von Maßnahmen zur Verhinderung zukünftiger Vorfälle.

8 Überprüfung und Audit

Der Lieferant erkennt das Recht von MARKGRAF an, Überprüfungen und Audits der Informationssicherheitsmaßnahmen des Lieferanten nach einer angemessenen Ankündigung, i.d.R. 14 Tage im Voraus, durchzuführen oder durchführen zu lassen. Die Kosten der Audits seitens des Lieferanten sind bis zu 2 Personentage inkludiert, sofern dies nicht anders in Einzelverträgen geregelt ist. Technische Audits, vor allem invasive Tests, erfodern die schriftliche Genehmigung des Lieferanten. Dazu gehören:

- Gewährung des Zugangs zu relevanten Informationen.
- Zusammenarbeit mit MARKGRAF und deren Beauftragten bei der Durchführung der Überprüfungen und Audits.
- Umsetzung von Korrekturmaßnahmen zur Behebung von festgestellten Mängeln innerhalb einer angemessenen Frist.

9 Beendigung der Geschäftsbeziehung

Im Falle der Beendigung der Geschäftsbeziehung verpflichtet sich der Lieferant:

- Alle vertraulichen Informationen von MARKGRAF unverzüglich zu löschen oder sicher an MARKGRAF zurückzugeben, sofern sie nicht den vertraglichen und gesetzlichen Aufbewahrungspflichten unterliegen.
- Eine schriftliche Bestätigung über die Löschung oder Rückgabe der Informationen an MARKGRAF zu übermitteln.

10 Sanktionen

Der Lieferant erkennt an, dass Verstöße gegen diese Verpflichtungserklärung schwerwiegende Folgen für MARKGRAF haben können und verpflichtet sich, im Falle eines Verstoßes alle angemessenen Maßnahmen zur Schadensbegrenzung zu ergreifen. Mögliche Sanktionen bei Verstößen umfassen:

- Vertragsstrafen gemäß den Bestimmungen des zugrunde liegenden Vertrags.
- Schadensersatzforderungen seitens MARKGRAF. **Diese werden wie folgt geregelt:**

→ Der Lieferant haftet bei einfacher Fahrlässigkeit für solche Schäden, die aus der Verletzung einer wesentlichen Vertragspflicht resultieren, und zwar beschränkt auf den typischen, vorhersehbaren Schaden und in der Höhe pro Kalenderjahr auf den Nettojahresauftragswert des betroffenen Einzelvertrages des Kalenderjahres, in dem die Haftungsfälle eintreten. Insbesondere ist die Haftung für Datenverlust auf den typischen Wiederherstellungsaufwand beschränkt, der bei regelmäßiger und gefahrentsprechender Anfertigung von Sicherungskopien eingetreten wäre (es sei denn, die Datensicherung ist Bestandteil der vertraglich vereinbarten Leistung). Wesentliche Vertragspflichten sind solche, deren Erfüllung die ordnungsgemäße Durchführung des Vertrages überhaupt erst ermöglicht und auf deren Einhaltung der Kunde regelmäßig vertraut oder vertrauen darf oder deren Verletzung die Erreichung des Vertragszwecks gefährdet.

11 Schlussbestimmungen

Diese Verpflichtungserklärung tritt mit der Vertragsunterzeichnung durch den Lieferanten in Kraft und gilt für die gesamte Dauer der Geschäftsbeziehung zwischen dem Lieferanten und MARKGRAF. Änderungen oder Ergänzungen dieser Verpflichtungserklärung bedürfen der Schriftform und der Zustimmung beider Parteien.