GRUNDLEGENDE ANFORDERUNGEN AN DIE INFORMATIONSSICHERHEIT

(Stand: 29.10.2025)

Kontaktdaten Schnellecke Group Security:

INFORMATION-SECURITY@SCHNELLECKE.COM

Die Bestimmungen dieser Anlage enthalten grundlegende Anforderungen der Schnellecke Group AG & Co. KG (Auftraggeberin) an die Informationssicherheit des Auftragsnehmers.
Die Auftraggeberin sieht im Hinblick auf das Vertragsverhältnis die Einhaltung der Anforderungen als Basis für die Zusammenarbeit.

1. GRUNDLEGENDE PFLICHTEN DES AUFTRAGNEHMERS

a. Vertraulichkeit und Datenschutz
Der Auftragnehmer verpflichtet sich, alle im Rahmen dieses Vertrags erhaltenen Informationen gemäß ihrer Klassifizierung (siehe unter 1.e.) zu behandeln und ausschließlich für die vertraglich vereinbarten Zwecke zu verwenden. Er stellt sicher, dass alle geltenden Datenschutzgesetze, einschließlich der DSGVO, eingehalten werden.

b. Informationssicherheitskonzept
Der Auftragnehmer verfügt über ein geeignetes Informationssicherheitskonzept inklusive der Beschreibung der technischen und organisatorischen Umsetzung der unter 2. beschriebenen Mindestanforderungen an die Informationssicherheit.

c. Nachweis von Zertifikaten
Der Auftragnehmer weist der Auftraggeberin aktuell gültige Zertifikate (TISAX, ISO27001, SOC2) nach.

d. Laufende Aktualisierung und Überprüfung
Der Auftragnehmer wird eine laufende Überprüfung und Anpassung des Informationssicherheitskonzeptes durchführen, insbesondere bei veränderten gesetzlichen oder behördlichen Regelungen und die Auftraggeberin darüber informieren (siehe Kontaktdaten oben).

e. Schutzbedarf und Klassifizierung von Informationen
Der Auftragnehmer sorgt für einen angemessenen Schutz der Informationen der Auftraggeberin unter Berücksichtigung der Vorgaben aus geltenden Standards, wie ISO27001 und dem aktuellen Stand der Technik. Hierbei sind die Schutzziele Vertraulichkeit, Verfügbarkeit und Integrität zu berücksichtigen.

f. Löschung und Rückgabe von Informationen
Nach Beendigung des Vertragsverhältnisses verpflichtet sich der Auftragnehmer alle erhaltenden Informationen der Auftraggeberin zu löschen/vernichten. Ausgenommen davon sind lediglich Informationen, die einer rechtlichen oder vertraglichen Aufbewahrungsverpflichtung unterliegen.

g. Kontaktperson beim Auftragnehmer
Der Auftragnehmer hat der Auftraggeberin einen verantwortlichen Ansprechpartner für Informationssicherheitsvorfälle zu benennen und Änderungen mitzuteilen.

h. Auditrecht
Die Auftraggeberin ist nach vorheriger Ankündigung berechtigt die Informationssicherheitsmaßnahmen, -kontrollen und -prozesse im Verantwortungsbereich des Auftragnehmers zu überprüfen. Der Auftragnehmer wird solche Überprüfungen ermöglichen und angemessen unterstützen.

2. MINDESTANFORDERUNGEN AN TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN ZUR INFORMATIONSSICHERHEIT

a. Richtlinien und Organisation
Der Auftragnehmer verfügt über aktuelle und geeignete Richtlinien zur Informationssicherheit und hat Verantwortlichkeiten für Informationssicherheit klar benannt und definiert. Daneben wird der Schutzbedarf der Informationen des Auftragnehmers systematisch ermittelt und inventarisiert.

b. Überprüfung und Einhaltung der Richtlinien
Die Richtlinien zur Informationssicherheit unterliegen einer regelmäßigen und anlassbezogenen Prüfung. Es sind Verfahren zur Einhaltung der Richtlinien etabliert.

c. Risikomanagement
Der Auftragnehmer bewertet, identifiziert und behandelt Informationssicherheitsrisiken systematisch.

d. Security Incident Management
Der Auftragnehmer hat geeignete Verfahren zum Umgang mit Sicherheitsvorfällen etabliert, welche eine angemessene Reaktion auf Vorfälle ermöglichen. Bei auftretenden Sicherheitsvorfällen ist die Kontaktperson bei der Auftraggeberin (siehe Kontaktdaten oben) unverzüglich zu informieren.

e. Geschäftskontinuität
Der Auftragnehmer wird angemessene Maßnahmen zur Begrenzung von Auswirkungen von Bedrohungen (z. B. Naturkatastrophen, physische Angriffe, Cyber-Angriffe) für die Leistungserbringung definieren und umsetzen. Ergänzend ist ein Business Continuity Management mit Notfallplänen und Notfalltests zu etablieren, wenn der Vertragsgegenstand als verfügbarkeitskritisch einzustufen ist.

f. Schulung und Sensibilisierung
Der Auftragnehmer stellt sicher, dass das Personal ausreichend und regelmäßig zu den Themen Cyber- und Informationssicherheit unterwiesen und sensibilisiert werden.

g. Schutz von Betriebsmitteln und Informationswerten
Der Lieferant führt eine Inventarisierung aller Betriebsmittel und Informationswerte durch und implementiert Maßnahmen zu deren Schutz. Regelmäßige Sicherheitsüberprüfungen und Wartungen sind durchzuführen.

h. Physische Sicherheit
Der Auftragnehmer verfügt über angemessene Maßnahmen zum physischen Schutz der Informationen in seinem Verantwortungsbereich. Dies beinhaltet definierte Sicherheitszonen, Maßnahmen zum Schutz vor unautorisierten Zutritt zu Gebäuden/ Räumen des Auftragnehmers und Verhaltensregeln für Mitarbeiter, insbesondere „Clean Desk“ Vorgaben.

i. Zugangs- und Zutrittssteuerung
Der Auftragnehmer wird Maßnahmen zum Schutz gegen unberechtigten Zugang, unberechtigte/versehentliche Veränderung oder Löschung sowie unberechtigte Übertragung treffen. Er wird Verfahren einsetzen, die gewährleisten, dass der Zugang zu schützenswerten Informationen und IT-Systemen nur autorisierten Personen gestattet wird.

j. Kryptographie
Der Lieferant verpflichtet sich, alle sensiblen Daten während der Übertragung und Speicherung durch den Einsatz von Verschlüsselungstechnologien zu schützen. Die verwendeten Verschlüsselungsalgorithmen und -schlüssel müssen den aktuellen Sicherheitsstandards entsprechen.

k. Datensicherung
Der Lieferant erstellt regelmäßig Datensicherungen und bewahrt diese sicher auf. Verfahren zur Wiederherstellung von Daten im Falle eines Verlusts sind zu implementieren und regelmäßig zu testen.

l. Schwachstellen- und Patchmanagement
Der Lieferant überprüft regelmäßig auf Sicherheitslücken und behebt diese zeitnah. Ein Patchmanagement-Prozess zur Aktualisierung von Software und Systemen ist zu implementieren.

m. Protokollierung und Überwachung
Der Lieferant richtet Protokollierungs- und Überwachungsmechanismen ein, um Sicherheitsvorfälle zu erkennen und darauf zu reagieren. Die Protokolle sind regelmäßig auf verdächtige Aktivitäten zu überprüfen.

n. Netzwerksicherheit
Der Lieferant richtet Protokollierungs- und Überwachungsmechanismen ein, um Sicherheitsvorfälle zu erkennen und darauf zu reagieren. Die Protokolle sind regelmäßig auf verdächtige Aktivitäten zu überprüfen.

o. Subunternehmer
Der Auftragnehmer wird seine Subunternehmer hinsichtlich der Einhaltung von Informationssicherheitsvorgaben überprüfen. Er wird vor der Weitergabe von schutzbedürftigen Informationen gültige Geheimhaltungsvereinbarungen abschließen.