

GRUNDLEGENDE ANFORDERUNGEN ZU INFORMATIONSSICHERHEIT**Für Verträge mit IT-gestützter Verarbeitung von Daten von IDEN-TEC SOLUTIONS AG**

1. Dieses Dokument „Grundlegende Anforderungen zu Informationssicherheit“ gilt grundsätzlich für alle Auftragnehmer und/oder Lieferanten („Lieferant“), welche Leistungen gleich welcher Art an die IDEN-TEC SOLUTIONS AG, einschließlich der mit ihr verbundenen Unternehmen (im Folgenden „IDEN-TEC“), soweit nicht vergleichbare Bestimmungen der mit ihr verbundenen Unternehmen vorrangig zur Anwendung kommen, erbringen. Der Lieferant verpflichtet sich alle Informationen und Daten, die der Lieferant für IDEN-TEC erhebt oder verarbeitet, oder auf die er Zugriff hat, stets nach dem jeweils aktuellen Stand der Technik wirksam gegen unberechtigten Zugriff, Veränderung, Zerstörung oder Verlust, unerlaubte Übermittlung, anderweitige unerlaubte Verarbeitung und sonstigem Missbrauch zu sichern. Dafür verfügt der Lieferant über ein geeignetes Sicherheitskonzept.

2. Der Lieferant stimmt sein Sicherheitskonzept mit IDEN-TEC ab. Insbesondere sind die im Lastenheft oder in anderen schriftlichen Spezifikationen definierten Anforderungen und Vorgaben für die Informationssicherheit einzuhalten und für das Sicherheitskonzept zu berücksichtigen. Der zuständige Informationssicherheitsbeauftragte von IDEN-TEC unterstützt dabei im Rahmen seiner Möglichkeiten. IDEN-TEC kann einen geeigneten, regelmäßig schriftlichen Nachweis über die Umsetzung und Einhaltung des Sicherheitskonzepts verlangen. Bei Anlass zu Zweifeln ermöglicht der Lieferant IDEN-TEC auch eine Besichtigung vor Ort und erteilt notwendige Auskünfte.

3. Der Lieferant benennt einen mit hinreichenden Befugnissen ausgestatteten Ansprechpartner für Security Management, der für sämtliche Themen zur Informationssicherheit zur Verfügung steht, z.B. für Incident Management (Management von Informations sicherheitsvorfällen).

4. Der Lieferant hat IDEN-TEC über wesentliche Änderungen der Datenverarbeitung in Textform zu informieren. Änderungen sind insbesondere dann wesentlich, wenn sie das Sicherheitskonzept betreffen. Die Mitteilung muss den Umfang der Änderung und die Auswirkung auf das Sicherheitskonzept beschreiben. Bei einer absehbaren Minderung der Schutzwirkung ist vor der Änderung die Zustimmung von IDEN-TEC in Textform einzuholen.

5. Die Informationen und Daten von IDEN-TEC dürfen vom Lieferanten nur für die vertraglich vereinbarten Zwecke und soweit dies zur Vertragserfüllung erforderlich ist genutzt werden. Bei Verarbeitung von Daten verschiedener Auftraggeber durch den Lieferanten ist deren Trennung nachprüfbar zu gewährleisten (Mandantentrennung).

6. Ein Zugriff auf Datenverarbeitungsanlagen („DV-Anlagen“) von IDEN-TEC oder dessen Unterauftragnehmer darf nur mit vorheriger Erlaubnis von IDEN-TEC im erlaubten und für die Vertragserfüllung erforderlichen Umfang durch die dazu berechtigten Personen erfolgen. Der Lieferant verpflichtet sich, keinem Unbefugten die ihm zur Nutzung des Systems zugewiesenen Zugriffsberechtigungen bekannt zu geben. Dem Lieferanten ist es nur nach vorheriger Zustimmung von IDEN-TEC gestattet, etwaigen Subunternehmern oder freien Mitarbeitern im vertragserforderlichen Umfang den Zugriff auf die DV-Anlagen von IDEN-TEC, seiner Beauftragten oder Subunternehmer zu ermöglichen. Der Lieferant muss IDEN-TEC unverzüglich mitteilen, wenn Mitarbeiter des Lieferanten, Subunternehmens oder freie Mitarbeiter mit Zugangs- oder Zugriffsberechtigungen für DV-Anlagen von IDEN-TEC, seiner Beauftragten oder Subunternehmer nicht mehr mit der Erfüllung der vertragsgegenständlichen Leistung befasst sind, damit IDEN-TEC bestehende Zugangs- und Zugriffsberechtigungen entziehen kann.

7. Alle von IDEN-TEC als vertraulich oder geheim eingestufte Informationen von IDEN-TEC oder Dritten sind vom Lieferanten durch geeignete kryptographische Maßnahmen nach aktuellem Stand der Technik bei der Übertragung sowie bei einer Speicherung auf mobilen Datenträgern zu schützen; bei einer Übertragung oder Speicherung innerhalb einer gesicherten Umgebung ist dies nicht erforderlich. Der Lieferant weist auf Anforderung von IDEN-TEC nach, dass die Umgebungen für die Verarbeitung vertraulicher oder geheimer Daten nach dem jeweils aktuellen Stand der Technik ausgelegt sind.

8. Der Lieferant hat IDEN-TEC bei Kenntniserlangen oder begründetem Verdacht auf Datenschutzverletzungen, Sicherheitsverletzungen und anderen Manipulationen des Verarbeitungsablaufs, die IDEN-TEC-Daten und -Services betreffen, unverzüglich zu informieren und sofort – in Abstimmung mit IDEN-TEC – alle erforderlichen Schritte zur Aufklärung des Sachverhalts einzuleiten und zur Schadensbegrenzung einzuleiten.

9. Findet die Datenverarbeitung bei IDEN-TEC oder im Datenaustausch mit IDEN-TEC-Systemen statt, so wird der Lieferant, sofern erforderlich, geeignete Maßnahmen ergreifen, damit es zu keiner Beeinträchtigung der IDEN-TEC-Infrastruktur (und von Dritten aus der IDEN-TEC-Umgebung heraus) kommt. Der Lieferant hat die jeweils gültigen Informationssicherheitsanforderungen von IDEN-TEC zu befolgen.

10. Der Lieferant wird IDEN-TEC unverzüglich informieren, falls durch Pfändung, Beschlagnahme oder sonstigen behördlichen Zugriff, in einem Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder

Maßnahmen Dritter die Gefahr besteht, dass nicht berechtigte Personen auf Daten von IDEN-TEC zugreifen. Der Lieferant wird die Dritten darüber informieren, dass es sich um Daten von IDEN-TEC handelt.

11. Der Lieferant informiert regelmäßig seine Mitarbeiter, Subunternehmer oder freien Mitarbeiter mit Zugangs- oder Zugriffsberechtigungen für DV-Anlagen von IDEN-TEC über relevante Themen der Informationssicherheit im Zusammenhang mit der Leistungserbringung für IDEN-TEC