Allgemeine Vorgaben zur Informationssicherheit für Auftragnehmer

Für Unternehmen der **eins** Gruppe hat Informationssicherheit eine hohe Bedeutung. Insbesondere die inetz GmbH als 100%-tige Tochter von **eins** ist ein ISO 27001 zertifiziertes Unternehmen. Zur Einhaltung der notwendigen Informationssicherheitsstandards innerhalb der **eins** Gruppe vereinbaren die Parteien in Ergänzung zu den allgemeinen Einkaufsbedingungen die hier folgenden Anforderungen an die Informationssicherheit für alle Leistungen im Bereich der Informations- und Telekommunikationstechnologie. Sie richten sich an alle Lieferanten, Partner und Auftragnehmer des Auftraggebers (im folgenden Auftragnehmer), die Leistungen im IT-Sicherheitsrelevanten Bereich erbringen, insbesondere Dienstleister der Datenverarbeitung, IT-Services und Berater, Cloud- und Application Service Provider, Dienstleister im Bereich Software as a Service, Lieferanten und Entsorger von Soft- und Hardware.

Informationssicherheit bedeutet, dass in allen Prozessen in denen Informations- und Telekommunikationstechnik eingesetzt wird, ein angemessenes Maß an Integrität, Verfügbarkeit und Vertraulichkeit von Daten und Systemen nach aktuellem Stand der Technik gewährleistet wird. Dazu stellt der Auftragnehmer die nachfolgenden Punkte sicher.

Allgemeines zur Leistungserbringung

1. Bei der Leistungserbringung ist sicherzustellen, dass der allgemeine Stand der Technik eingehalten wird. Dies umfasst die Einhaltung der einschlägigen DIN-Normen, GoBD, Datenschutzvorschriften und entsprechender internationaler und europäischer Normen (z.B. DIN ISO, DIN EN) als Mindeststandard. Insbesondere IT-Lieferungen und IT-Leistungen sind so zu erbringen, dass sie der Einhaltung der DIN ISO/IEC 27001, 27002, 27011, 27019 durch den Auftraggeber nicht entgegenstehen.
2. Bei Leistungen im Betrieb des Auftraggebers hat der Auftragnehmer dort geltende Sicherheitsvorschriften und Informationsrichtlinien einzuhalten, die ihm der Auftraggeber auf Anfrage zur Verfügung stellt. Bei Zugriff auf Informations- und Telekommunikationstechnologie des Auftraggebers hat der Auftragnehmer die dafür geltenden Informationssicherheitsrichtlinien und die nachfolgenden Regelungen strikt zu beachten, insbesondere auch bei Fernzugriffen (Remote-Zugriff).
    a. Eine Verarbeitung von Daten im Remotezugriff erfolgt nur, soweit dies im zugrundeliegenden Leistungsvertrag vereinbart oder geregelt ist. Hierunter fallen ebenfalls Tätigkeiten bei denen Daten von einem System in ein anderes migriert werden.
    b. Wenn es sich bei diesen Daten um personenbezogene Daten handelt oder handeln könnte, liegt eine Auftragsdatenverarbeitung vor. Die Parteien schließen in Ergänzung zu dem Hauptvertrag eine Vereinbarung zur Auftragsdatenverarbeitung.
3. Bei Vertragsbeendigung enden gleichzeitig Zugangsberechtigungen für Personal des Auftragnehmers zu Systemen und zum Betriebsgelände des Auftraggebers. Dafür bereitgestellte Ausweise und sonstige zur Authentifizierung zur Verfügung gestellten Gegenstände (z.B. Token) werden dem Auftraggeber unaufgefordert zurückgegeben.
4. Durch den Auftragnehmer sind Lieferungen und Leistungen, insbesondere elektronisch (z.B. via Email oder Datentransfer) übertragene Lieferungen und Leistungen, sowie sämtliche im Rahmen der Leistung eingesetzten Datenträger auf Schadsoftware (z.B. Trojaner, Viren, Spyware usw.), unter Verwendung aktuellster Prüf- und Analyseverfahren zu prüfen und hierdurch die Freiheit von Schadsoftware sicherzustellen. Wird Schadsoftware erkannt, darf der Datenträger nicht eingesetzt werden. Erkennt der Auftragnehmer beim Auftraggeber Schadsoftware, wird er den

DB.UF.0263 Stand: 01.03.2019

Auftraggeber unverzüglich darüber informieren. Die gleichen Verpflichtungen gelten für jede Form der elektronischen Kommunikation.

5. Der Auftragnehmer verpflichtet sich, alle Informationen und Daten des Auftraggebers nach dem Stand der Technik sofort wirksam gegen unberechtigten Zugriff, Veränderung, Zerstörung oder Verlust, unerlaubter Verarbeitung und sonstigen Missbrauch zu sichern. Bei der Sicherung von Auftraggeberdaten sind sämtliche Vorkehrungen und Maßnahmen nach dem aktuellen Stand der Technik zu beachten, um jederzeit Datenbestände verlust- und rechtssicher zu archivieren und wiederherzustellen.

Kontrollrechte

1. Der Auftraggeber ist dazu berechtigt, die Einhaltung der Vorschriften aus dieser Vereinbarung im erforderlichen Umfang in Form von Audits zu kontrollieren oder kontrollieren zu lassen. Der Auftragnehmer gewährt dazu dem Auftraggeber oder einer neutralen Stelle nach Absprache, ungehinderten Zutritt, Zugang und Zugriff zu informationsverarbeitenden Systemen, Programmen, Dateien und Informationen, die mit der Durchführung der Tätigkeiten in Verbindung stehen. Dem Auftraggeber sind durch den Auftragnehmer alle Auskünfte zu erteilen, die zur Erfüllung der Kontrollfunktion benötigt werden.
2. Ist der Auftragnehmer ISO 27001 bzw. BSI Grundschutz zertifiziert dient dies als Nachweis für die Einhaltung der hier beschriebenen Vorschriften. Dazu müssen alle für die Leistungserbringung relevanten Standorte, Prozesse, Organisationseinheiten und IT-Systeme im Anwendungsbereich der Zertifizierung enthalten sein. Ein Nachweis ist dem Auftraggeber auf Anfrage unverzüglich zu übergeben.
3. Der Auftraggeber ist dazu berechtigt, sämtliche Aktionen des Auftragnehmers innerhalb seiner Infrastruktur zu protokollieren und auszuwerten.
4. Sämtliche erbrachten Leistungen und damit zusammenhängende Tätigkeiten sind vom Auftragnehmer zu dokumentieren und auf Anfrage dem Auftraggeber zur Verfügung zu stellen.

DB.UF.0263 Stand: 01.03.2019