ANLAGE 17

INFORMATIONSSICHERHEITSRICHTLINIEN

Stand November 2017

Richtlinien für den Anbieter

Dieses Dokument enthält spezifische Informationen, die MAN den Anbietern für die Beantwortung der Ausschreibung zur Verfügung stellt.

Anweisungen für den Anbieter

1. Der Anbieter verpflichtet sich, keine Änderungen oder Modifikationen an diesem Dokument vorzunehmen.
2. Die Antwort des Anbieters auf diese Ausschreibung sollte die Informationen in diesem Dokument widerspiegeln und diesen Angaben entsprechen.
3. Einwände oder Probleme in Verbindung mit den in den Dokumenten enthaltenen Definitionen machen die Anforderungen dieses Dokuments oder der Ausschreibung weder ungültig noch bewirken sie eine Modifizierung der Anforderungen. Von einer Aufnahme der vorgeschlagenen Änderungen des Anbieters kann der Anbieter nur ausgehen, sofern die MAN diese dem Anbieter gegenüber ausdrücklich schriftlich bestätigt hat.

Ref #	
Anl. 17 - 1	**ÜBERBLICK**
Anl. 17 - 2	Gesetzliche Regelungen fordern für sensible Unternehmenswerte „Sicherheitsmaßnahmen“, die zur Aufrechterhaltung des Geschäftsbetriebs einer Organisation von entscheidender Wichtigkeit sind. Im Zeitalter zunehmender Digitalisierung sind zu schützende „Informationswerte“ zunehmenden „Bedrohungen“ ausgesetzt. *Systeme*, Netze und Organisationen sind gefährdet durch Cyber-Angriffe (bösartiger Code, Denial-of-Service-Angriffe, Schadsoftware, Hacking, Spam etc.), Sabotage, Spionage und Vandalismus, aber auch Elementarschäden durch Wasser, Feuer sowie *Katastrophen* und andere „Gefahren“.
Anl. 17 - 3	Das Ziel eines Schutz-und Informationssicherheits-Managements (Safety and Information Security Management), generell als *Informationssicherheits-Managementsystem (Information Security Management System (ISMS))* bezeichnet, ist die Definition eines Sicherheitsregelwerks (Security Policy), um sowohl organisatorische Anforderungen als auch Anforderungen der *Governance* der MAN aufrecht zu erhalten.
Anl. 17 - 4	Die primären Schutzziele der „Informationssicherheit“ sind „Vertraulichkeit“, „Integrität“, „Verfügbarkeit“ (engl. Confidentiality, Integrity and Availability). Die erweiterten Schutzziele sind Authentizität, „Zurechenbarkeit“, „Nicht-Abstreitbarkeit“ und „Verlässlichkeit“ (engl. Authenticity, Accountability, Non-Repudiation and Reliability) der „Informationswerte“.
Anl. 17 - 5	Der AN wird die Geschäftsbeziehung mit MAN sowie sämtliche im Rahmen dieser Geschäftsbeziehung ausgetauschten Informationen streng geheim halten. Er verpflichtet sich diese Informationen gemäß diesen zur Verfügung gestellten Informationssicherheitsrichtlinien der MAN, mittels geeigneter Maßnahmen vor Dritten zu schützen. Die Geheimhaltungspflicht gilt nach Beendigung oder vollständiger Abwicklung der jeweiligen Beauftragung für einen Zeitraum von zehn (10) Jahren weiter. Die Geheimhaltungsverpflichtung gilt unabhängig von einem Vertragsschluss auch für in der Angebotsphase erlangte Kenntnisse. Im Übrigen gelten die Bestimmungen der separaten, vom AN zu unterzeichnenden, Geheimhaltungsverpflichtungserklärung.
Anl. 17 - 6	In dieser Anlage sind die Sicherheitsanforderungen aufgeführt, die der AN bei allen *Services* und Aktivitäten vom *Anfangsdatum* des *Vertrages* an (wenn nicht anders angegeben oder zwischen den *Parteien* vereinbart) erfüllen bzw. einhalten wird. Die Anhänge dieser Anlage enthalten zwei Selbst-Assessments, die vom AN vor Vertragsabschluss auszufüllen sind, sowie spezifische Informationen, welche die MAN dem AN zur Verfügung stellt.

Ref #	
Anl. 17 - 7	Der AN räumt MAN das jederzeit auszuübende Recht ein, nach vorheriger Anmeldung sämtliche Daten zu Geschäftsvorfällen zwischen MAN und dem AN bei dem AN einzusehen und zu überprüfen sowie Maßnahmen der Informationssicherheit zu überprüfen; MAN oder von MAN beauftragte Dritte dürfen hierzu bei Informationssicherheitsaudits die Räume des AN während der üblichen Geschäftszeiten betreten. Die Kosten der Überprüfung und die Umsetzung risikomindernder Maßnahmen trägt der AN, wenn hierbei Verstöße gegen die Vereinbarungen der jeweiligen Beauftragung und/oder die Informationssicherheitsrichtlinien festgestellt werden, es sei denn, solche Verstöße beruhen nicht auf einem Verschulden des AN.
Anl. 17 - 8	Für die Erbringung von ausgelagerten IT Diensten, die in das interne Kontrollsystems der MAN fallen, sind Kontrollen zum IT Outsourcing. vorgesehen, Hierzu ist vom AN regelmäßig, ein unabhängiger Auditor zu beauftragen, der den mit der Leistung verbun-denen Kontrollrahmen überprüft und in einem ISAE 3402 Bericht zusammenzufasst. Der Bericht besteht aus folgenden beiden Teilen: 1. ISAE 3402 Type 2 Report – Basic Infrastructure Services System provided from the datacentres in Scope 2. ISAE 3402 Type 2 Add-on Report – Database and Middleware Systems for ICFR relevant application
Anl. 17 - 9	Die MAN wird dem AN bei Beauftragung und während der *Vertragslaufzeit* „Zugriff“ auf die jeweils aktuellen Dokumente der MAN Sicherheitsleitlinien sowie relevanten Regelungen und Anweisungen der Konzernmutter Volkswagen AG gewähren. Grundsätzlich gültig ist das Regelwerk der MAN Gruppe zur Informationssicherheit (**Anhang 17-A (Schutz- und Sicherheitsverfahren)**). Liegen explizite Regelungen der MAN Gruppe zu einem spezifischen Thema vor, gelten die Regelungen der MAN Gruppe verbindlich über die jeweilige Regelung der Volkswagen Gruppe.
Anl. 17 - 10	Im Falle von Unterbeauftragungen, des an MAN erbarchten Services, stellt der AN sicher, daß die hier beschriebenen Anforderungen ebenfalls an den Unterlieferranten gestellt werden. Zudem stellt der AN sicher, daß MAN das in 17-7 beschriebene Prüfrecht auch beim Unterlieferranten eingeräumt wird.

Anl. 17 - 11	Die folgenden Anhänge sind Bestandteil dieser Anlage:
Anl. 17 - 12	**Anhang 17-A (Schutz- und Sicherheitsverfahren)** enthält: 1. Die organisatorischen Anweisungen beinhalten bestehende Richtlinien zur Informationssicherheit (Datenschutz und Datensicherheit) der Konzernmutter Volkswagen AG sowie der MAN Gruppe. 2. Die Informationssicherheitsanweisungen beinhalten die MAN Sicherheitspolitik, die Sicherheitsleitlinien und die Sicherheitsregelungen und Ausführungsbestimmungen zur Informationssicherheit (Datenschutz und Datensicherheit) sowie jene der Konzernmutter Volkswagen AG.
Anl. 17 - 13	**Anhang 17-D (Information Security Assessment)** enthält ein Formular zur Erhebung eines Information Security Assessments und ist vom AN auszufüllen.
Anl. 17 - 14	**Anhang 17-E (Fragenkatalog ADV)** enthält ein Formular zur Erhebung eines Auftragsdatennachverarbeitungs-Assessments und ist vom AN auszufüllen.
Anl. 17 - 15	**Anhang 17-F (Auftragsdatenverarbeitungsvertrag)** beschreibt die Vorgaben der MAN zum Datenschutz der Auftragsdatenverarbeitung. Der Entwurf zur Auftragsdatenverarbeitungsvereinbarung dient zunächst nur zur Ansicht. Eine unterschriebene Version ist somit nicht bei Angebotsabgabe einzureichen und wird im Zuge einer Vertragsunterzeichnung berücksichtigt.
Anl. 17 - 16	**Anhang 17-G Fragenkatalog zu Nachweisen internationaler Normen und Zertifizierungen** enthält ein Formular zur Erhebung des Reifegrades bezüglich der Konformität zu internationalen Normen. Diese Fragen sind gemäß der Erfülltheit mit Ja/Nein zu beantworten und ggf. kurz zu kommentieren.