PUBLIC
ÖFFENTLICH

ANLAGE 17

INFORMATIONSSICHERHEITSRICHTLINIEN

Stand Dezember 2021

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. Mit wachsender Digitalisierung sind zu schützende „Informationswerte“ zunehmenden „Bedrohungen“ ausgesetzt. Systeme, deren Funktionen, Netze und Organisationen sind gefährdet durch *Cyber-Angriffe* (Schadsoftware, Hacking, Denial-of-Service-Angriffe, Phishing etc.), Sabotage, Spionage und Vandalismus, aber auch Elementarschäden durch Wasser, Feuer, Katastrophen und andere „Gefahren“.
Anl. 17 - 3	Ziel des Managements von Informationssicherheit, ist es ein angemessenes Informationssicherheitsniveau der MAN zu bewahren. Hierzu ist im Informationssicherheitsmanagementsystem (ISMS) ein Sicherheitsregelwerk (Security Policies) definiert, das die Einhaltung unternehmerischer Anforderungen der MAN fordert.
Anl. 17 - 4	Die primären Schutzziele für die „Informationswerte“ der MAN 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).
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 sorgfältig zu schützen. Die Geheimhaltungspflicht gilt nach Beendigung oder vollständiger Abwicklung der jeweiligen Beauftragung für einen Zeitraum gem. IT-AEB 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, wenn nicht anders angegeben oder zwischen den *Parteien* vereinbart, bei allen *Services* und Aktivitäten vom *Anfangsdatum* des *Vertrages* an, erfüllen bzw. einhalten wird.
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 die technischen und organisatorischen Maßnahmen zur Informationssicherheit zu überprüfen; MAN oder von MAN beauftragte Dritte dürfen hierzu bei Informationssicherheitsaudits die Räume des AN während der üblichen Geschäftszeiten betreten. Wenn Verstöße gegen die Vereinbarungen der jeweiligen Beauftragung und/oder die Informationssicherheitsrichtlinien festgestellt werden, trägt hierbei der AN die Kosten der Überprüfung und die Umsetzung risikomindernder Maßnahmen, es sei denn die Verstöße beruhen nicht auf einem Verschulden des AN.

Ref #	
Anl. 17 - 8	Für die Erbringung von ausgelagerten IT Diensten durch einen externen Dienstleister, die in das interne Kontrollsystem der MAN fallen (IFR Systeme), sind Kontrollen zum IT Outsourcing vorgesehen. Hierzu ist vom AN jährlich, ein unabhängiger Auditor zu beauftragen, der den mit der Leistung verbundenen Kontrollrahmen überprüft und in einem ISAE 3402 Bericht zusammenzufasst. In Abhängigkeit der erbrachten IT Dienstleistung kann der Bericht in mehrere Teile gefasst sein: 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 applications
Anl. 17 - 9	Die MAN wird dem AN bei Beauftragung und während der *Vertragslaufzeit* „Zugriff“ auf die jeweils aktuellen Dokumente der MAN Sicherheitsleitlinien sowie relevanter Regelungen und Anweisungen des Volkswagen Konzerns gewähren. Grundsätzlich gültig ist das Regelwerk zur Informationssicherheit der MAN Gruppe (**Anhang 17-A (Schutz- und Sicherheitsverfahren)**). Die Regelungen der Volkswagen Gruppe sind dort gültig, wo keine explizite Regelung der MAN vorliegt.
Anl. 17 - 10	Im Falle von Unterbeauftragungen, des an MAN erbrachten Services, stellt der AN sicher, dass die hier beschriebenen Anforderungen in gleicher Weise an den Unterlieferanten gestellt werden. Zudem stellt der AN sicher, dass MAN das in 17-7 beschriebene Prüfrecht auch beim Unterlieferanten eingeräumt wird.
Anl. 17 - 11	Die folgenden Anhänge sind Bestandteil dieser Anlage:
Anl. 17 - 12	**Anhang 17-A (Schutz- und Sicherheitsverfahren) und (Policy Pack)** enthält: Die organisatorischen Anweisungen beinhalten bestehende Richtlinien zur Informationssicherheit (Datenschutz und Datensicherheit) der MAN Gruppe sowie relevante Regelungen des Volkswagen Konzerns.

Ref #	
Anl. 17 - 13	**Auftragsverarbeitung**: Informationsverarbeitung im Auftrag liegt vor, wenn die Leistung des AN im Schwerpunkt mit der Verarbeitung von Informationen der MAN zu tun hat. Der AN muss durch eine Zertifizierung die Eignung zur sicheren Informationsverarbeitung nachweisen. Werden durch den AN Informationen im Auftrag der MAN verarbeitet, die einen hohen oder sehr hohen Schutzbedarf aufweisen, so ist eine **TISAX Zertifizierung** im entsprechenden TISAX Label nachzuweisen. In Abhängigkeit von der Serviceerbringung kann eine **ISO 27001 Zertifizierung** über den Geltungsbereich, der alle Auftragsverarbeitungsaktivitäten beinhaltet, ebenfalls die Eignung bescheinigen. Falls der AN keine gültige Informationssicherheitszertifizierung nachweisen kann, so kann ein Vertragsverhältnis nur dann eingegangen werden, wenn sich der AN zu einer **TISAX Zertifizierung** innerhalb der nächsten neun Monate nach Vertragsbeginn, verpflichtet. Zudem ist vom AN eine **Gap Analyse** nach der TISAX Methodik einschließlich eines Aktionsplans zur Erreichung der Zertifizierungsstufe im geplanten Zeitrahmen bereitzustellen (**LINK: VDA Information Security Assessment**[1])
Anl. 17 - 14	**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 noch nicht bei Angebotsabgabe einzureichen und wird erst im Zuge einer Vertragsunterzeichnung berücksichtigt.

[1] Information Security - VDA