PUBLIC
ÖFFENTLICH

ANHANG 17-A
SCHUTZ- UND SICHERHEITSVERFAHREN

Stand März 2023

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.

Inhaltsverzeichnis

1.0 EINFÜHRUNG

In diesem Anhang sind die Schutz- und Sicherheitsanweisungen benannt, 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 MAN wird dem AN bei Beauftragung Zugriff auf die jeweils aktuellen MAN Schutz- und Sicherheitsanweisungen sowie relevanten Regelungen und Anweisungen der Konzernmutter Volkswagen AG gewähren. Die Anweisungen werden jährlich überprüft und gegebenenfalls angepasst. Der AN ist verpflichtet, alle für die Erbringung der Services relevanten Sicherheitsanforderungen der MAN einzuhalten.

Grundsätzlich gültig ist das aktuelle Regelwerk der MAN Marke zur Informationssicherheit. Liegen explizite Regelungen der MAN zu einem spezifischen Thema vor, gelten die Regelungen der MAN verbindlich über die jeweilige Regelung der Volkswagen Gruppe.

Insbesondere ist eine den Regelungen entsprechendes Risikomanagement verbindlich zu gewährleisten.

1.1 Organisatorische Anweisungen

Die Organisatorischen Anweisungen beinhalten bestehende Richtlinien zur Informationssicherheit der MAN Truck & Bus. Diese werden im Folgenden benannt:

Richtlinie	Datei
MAN Truck & Bus Markenrichtlinie 13.1 Informationssicherheit inkl.Anweisung 1 „Standard für Informationssicherheit“	Siehe Policy Pack
MAN Truck & Bus Markenrichtlinie 13.1 Anweisung 3 „Klassifizierung von Informationswerten“ und Anlage 03.1 „Umgang mit klassifizierten Informationen“ Anweisung 6 „Informationssicherheit für Systembetrieb und Administration“ Anweisung 7 „Informationssicherheitanforderungen zur Entwicklung sicherer Anwendungen“ und Anlage 07.1 „Anforderungen zur Entwicklung sicherer Anwendungen“ Anweisung 8 „Informationssicherheit für Lieferanten“ und Anlage 08.1 „Verfahren und Anforderungen im Rahmen der Lieferantenüberprüfung“	Siehe Policy Pack
MAN Truck & Bus Markenrichtlinie 13.1 „Zusatzinformation zur Markenrichtlinie MAN Truck & Bus 13.1 “	Siehe Policy Pack

1.2 Sicherheitsanweisung

Die Informationssicherheitsanweisungen beinhalten darüber hinaus detailliertere Sicherheitsregelungen und Ausführungsbestimmungen zur Informationssicherheit der Konzernmutter Volkswagen AG, die ebenfalls als bindend zu betrachten sind:

Anweisung	Datei
Volkswagen AG Informationssicherheit – Handlungsleitlinie für Systembetreiber und Administratoren Regelungs Nr 02.03	Siehe Policy Pack
Volkswagen AG Informationssicherheit – Handlungsleitlinie für Systementwickler Regelung Nr 02.04	Siehe Policy Pack
Volkswagen AG Informationssicherheit – Handlungsleitlinien für Dienstleister Regelung Nr 02.06	Siehe Policy Pack
Volkswagen AG Informationssicherheit - Übergreifende Regelungen und Prozesse – Dienstleistung durch Dritte – Regelung Nr 03.01.16	Siehe Policy Pack
Volkswagen AG Informationssicherheit – Übergreifende Regelungen und Prozesse – Cloud Security – Regelung Nr 03.01.17	Siehe Policy Pack

1.3 Auftragsdatenverarbeitung

Der AN wird im Rahmen der Erbringung der Services die Regelungen zur Auftragsdatenverarbeitung der MAN einhalten und dies vertraglich zusichern (siehe hierzu Auftragsdatenverarbeitungsvertrag.

1.4 Datenschutzrichtlinie

Die Datenschutzrichtlinie beschreibt die bestehenden Anforderungen der MAN an den Datenschutz. Der AN wird im Rahmen der Erbringung der Services die Regelungen zum Datenschutz einhalten (siehe hierzu Markenrichtlinie MR 4.06 „Umgang mit personenbezognen Daten und Organisation des Datenschutzes“ im Policy Pack).

2.0 SICHERHEIT

Zu den Aufgaben des AN gehören:

(a) Einhaltung der Anforderungen und bestehenden Sicherheitsprozesse der MAN, Organisatorische Anweisungen, IT Sicherheitsanweisungen, Geheimhaltungsverpflichtung, Auftragsdatenverarbeitung, Datenschutzrichtlinie und Information Security Assessment in ihrem jeweils gültigen Stand, sofern nicht anderweitig modifiziert und zwischen den Parteien vereinbart.

(b) Der AN wird bei der Erbringung der Vertragsleistungen den aktuellen Standard der Informationssicherheit einhalten, die Anforderungen und Maßnahmen der in insbesondere Ziffer 1.0 genannten Dokumente durchführen und einhalten sowie dabei insbesondere MAN Systeme nach dem aktuellen Stand der Technik gegen unbefugte Zugriffe Dritter (z.B. Hacker-Angriffe) sowie gegen unerwünschte Datenübermittlung (z.B. Spam) sichern. Sofern dem AN insbesondere Gefährdungen oder Sicherheitsrisiken der Daten- und Informations-/Systemsicherheit bekannt werden, muss er MAN unverzüglich hierüber in elektronischer Form (E-Mail) unterrichten und – in enger Abstimmung mit MAN und auf eigene Kosten – umgehend wirksame Gegenmaßnahmen einleiten, welche die Erbringung der Vertragsleistungen nicht einschränken

(c) Einhaltung der in den jeweiligen Ländern der Leistungserbringung gültigen gesetzlichen Regelungen in Bezug auf Datenschutz und Datensicherheit.

(d) Zusätzlich zu den landesspezifischen gesetzlichen Regelungen ist der Standard der EU-Datenschutzgrundverordnung (DSGVO) einzuhalten. Dieser ist auch dort anzuwenden, wo keine entsprechende gesetzliche Regelung existiert.

(e) Für jedes neue System und jede neue Anwendung ist eine formale Bewertung der Informationssicherheit durch die IS-Organisation der MAN (ISi Assessment) und/oder der Volkswagen Group Information Security einzuplanen. Erst nach Freigabe darf diese Neuentwicklung eingesetzt werden.

(f) Einhaltung des notwendigen Sicherheitsniveaus der MAN.

(g) Die unaufgeforderte Vorlage eines monatlichen Reports zur Informationssicherheit, der die wesentlichen Risikobereiche im Rahmen der Erbringung der Services beschreibt. Die

Risikobereiche werden vom AN vor Vertragsschluss gemeinsam mit der MAN festgelegt und das Reporting abgestimmt.

(h) Die Durchführung von regelmäßigen Schwachstellenanalysen oder Penetrationstests mittels geeigneter Werkzeuge und ein entsprechendes Reporting.

(i) Die regelmäßige Aktualisierung des Reifegrades für Informationssicherheit (VDA ISA), sowie die Definition von Maßnahmen zur Risikobehandlung und ein entsprechendes Reporting.