ANHANG 17-A
SCHUTZ- UND SICHERHEITSVERFAHREN

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.

Inhaltsverzeichnis

1.0 EINFÜHRUNG 4

1.1 Organisatorische Anweisungen 4

1.2 Sicherheitsanweisung 5

1.3 Auftragsdatenverarbeitung 7

1.4 Datenschutzrichtlinie 7

2.0 SICHERHEIT 8

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 Regelwerk der MAN Gruppe zur Informationssicherheit. 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.

Insbesondere ist eine den Regelungen entsprechende Risikobehandlung verbindlich zu gewährleisten.

1.1 Organisatorische Anweisungen

Die Organisatorischen Anweisungen beinhalten bestehende Richtlinien zum Schutz und zur Informationssicherheit (Datenschutz und Datensicherheit) der Konzernmutter Volkswagen AG sowie der MAN Gruppe. Diese werden im Folgenden benannt:

Richtlinie	Datei
MAN Konzernrichtlinie MAN 13.1 Informationssicherheit inkl. Konzernanweisung 1 „Standard für Informationssicherheit“	MAN-13.1-Konzernrichtlinie-de.pdf MAN-13.1-Konzernrichtlinie-Anweisung-1-d
MAN 13.1 Konzernanweisung 3 „Management von Informationssicherheitsvorfällen“ MAN 13.1 Konzernanweisung 4 „Klassifizierung von Informationswerten“ MAN 13.1 Konzernanweisung 7 „Informationssicherheit für Benutzer mit privilegierten IT Rechten“ MAN 13.1 Konzernanweisung 8 „Informationssicherheit bei der Zusammenarbeit mit IT Service Providern“	MAN-13.1-Konzernrichtlinie-Anweisung-3-d MAN-13.1-Konzernrichtlinie-Anweisung MAN-13.1-Konzernrichtlinie-Anweisung-4-d MAN-13.1-Konzernrichtlinie-Anweisung MAN-13.1-Konzernrichtlinie-Anweisung-7-d
MAN 13.1 Glossar „ Zusatzinformation zur Konzernrichtlinie MAN 13.1 „	MAN-13.1-Zusatzinformation-Glossar-de.p

1.2 Sicherheitsanweisung

Die IT Sicherheitsanweisungen beinhalten die MAN Sicherheitspolitik, die Sicherheitsleitlinien und die Sicherheitsregelungen und Ausführungsbestimmungen zur Informationssicherheit (Datenschutz und Datensicherheit) sowie der Konzernmutter Volkswagen AG (Dokumente der Volkswagen AG sind als Leitlinie zu betrachten):

Richtlinie	Datei
MAN Konzernrichtlinie MAN 13.1 Informationssicherheit	Siehe 1.1
MAN 13.1 Konzernanweisung 1 „Standard für Informationssicherheit“	Siehe 1.1
MAN 13.1 Konzernanweisung 3 „Management von Informationssicherheitsvorfällen“	Siehe 1.1
MAN 13.1 Konzernanweisung 4 „Klassifizierung von Informationswerten“	Siehe 1.1
MAN 13.1 Konzernanweisung 7 „Informationssicherheit für Benutzer mit privilegierten IT Rechten“	Siehe 1.1
MAN 13.1 Konzernanweisung 8 „Informationssicherheit bei der Zusammenarbeit mit IT-Service Providern“	Siehe 1.1
Volkswagen AG Informationssicherheit – Handlungsleitlinie für Systembetreiber und Administratoren Regelungs Nr 02.03 Version 3.0	 regelung-nr--02-03-i s-handlungsleitlinie-fu
Volkswagen AG Informationssicherheit – Handlungsleitlinie für Systementwickler Regelung Nr 02.04 v3.0	 regelung-nr--02-04- is-handlungsleitlinie
Volkswagen AG Informationssicherheit - Handlungsleitlinien für Dienstleister Regelung Nr 02.06 v3.0	 regelung-nr--02-06- handlungsleitlinien

Volkswagen AG Informationssicherheit - Übergreifende Regelungen und Prozesse - Dienstleistung durch Dritte – Regelung Nr 03.01.16 v1.0	 regelung-nr-03-01-16-dienstleistung-d  vergabe-von-konzern-it-dienstleistunge  vergabe-von-konzern-it-dienstleistunge
Volkswagen AG Informationssicherheit – Anforderungen Cloudcomputing	 cloudcomputing-anforderungen-final.xl

1.3 Auftragsdatenverarbeitung

Die Auftragsdatenverarbeitung beschreibt die Vorgaben der MAN zum Datenschutz der Auftragsdatenverarbeitung. Der AN wird im Rahmen der Erbringung der Services die Regelungen zur Auftragsdatenverarbeitung der MAN einhalten und dies schriftlich zusichern (siehe hierzu Anhang 17-E (Fragenkatalog ADV) und Anhang 17-F (Auftragsdatenverarbeitungsvertrag)).

1.4 Datenschutzrichtlinie

Die Datenschutz – Richtlinien und Anweisungen beschreiben die bestehenden Datenschutz – Richtlinien und Anweisungen der MAN. Der AN wird im Rahmen der Erbringung der Services die Regelungen zum Datenschutz einhalten.

2.0 SICHERHEIT

Zu den Aufgaben des AN gehören:

(a) Einhaltung der Anforderungen und bestehenden Sicherheitsprozesse der MAN, Organisatorische Anweisungen, IT Sicherheitsanweisungen, Geheimhaltungs-verpflichtung, Auftragsdatenverarbeitung), Datenschutz – Richtlinien und Anweisungen) 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 mindestens der Standard des deutschen Bundesdatenschutzgesetzes (BDSG) bzw. der EU-Datenschutzgrundverordnung (DSGVO) einzuhalten. Diese sindauch in Ländern anzuwenden, die über keine eigene gesetzliche Regelung verfügen.

(e) Für jedes neue System und jede neue Anwendung ist eine formale Bewertung der Informationssicherheit durch die IS-Sicherheitsorganisation MAN und/oder der Konzernmutter Volkswagen AG (ISSO) 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 Sicherheitsorganisation festgelegt.

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

(i) Die jährliche Durchführung eines von der MAN gestellten ISMS Assessments, sowie die Definition von Maßnahmen zur Risikobehandlung und ein entsprechendes Reporting.