APPENDIX 17-A
PROTECTION AND SECURITY PROCEDURES

November 2017

Guidelines for the tendering party

This document contains specific information MAN provides to tendering parties for the purpose of responding to requests for proposal.

Instructions for the tendering party

1. The tendering party undertakes not to amend or modify this document in any way.
2. The tendering party's response to this request for proposal should reflect the information contained in this document and correspond to this data.
3. Any objections or problems in connection with the definitions contained in the documents do not render the requirements set out in this document or in the request for proposal invalid, nor do they result in said requirements being modified. The tendering party can only assume that the changes it proposes are accepted if MAN has expressly confirmed this to the tendering party in writing.

Contents

1.0 INTRODUCTION

This Appendix outlines the protection and security instructions for the Contractor to follow and / or comply with when rendering all services and activities as of the inception date of the contract (in the absence of any information or agreement between the Parties to the contrary).

When commissioning the Contractor, MAN shall guarantee that the latter has access to the latest version of the MAN protection and security instructions, as well as the relevant regulations and instructions of its parent company, Volkswagen AG, applicable in each case. The instructions are reviewed once a year and adjusted if necessary. The Contractor is obliged to comply with all MAN security requirements that are relevant for the performance of its services.

The set of rules of the MAN Group for information security is valid in principle. In the event that express regulations of the MAN Group are available for a specific issue, the regulations of the MAN Group are binding and take precedence over any regulation of the Volkswagen Group.

In particular, a binding guarantee shall be made that the Contractor's Risk Management is in line with the regulations.

1.1 Organizational Instructions

The Organizational Instructions contain existing guidelines on protection and information security (data protection and data security), both of Volkswagen AG (parent company) and of the MAN Group. These are outlined below:

Policy	File
MAN Group Policy MAN 13.1 Information Security, incl. Group instruction 1 "Standard for Information Security"	MAN-13.1-Group-Policy-en.pdf MAN-13.1-Group-Policy-Instruction-1-e

Group Policy MAN 13.1 MAN - Instruction 3 „Information Security Incident Management“ MAN - Instruction 4 „Classification of Information Assets“ MAN - Instruction 7 „Information Security for Users with privileged IT responsibilities“ MAN - Instruction 8 „Information Security for the collaboration with IT Service Providers“	MAN-13.1-Group-Policy-Instruction-3-e MAN-13.1-Group-Policy-Instruction-4-e MAN-13.1-Group-Policy-Instruction-7-e MAN-13.1-Group-Policy-Instruction-8-e
MAN 13.1 Glossary „Additional Information to Group Policy MAN 13.1”	MAN-13.1-Additional-Information-Glos:

1.2 Safety Instructions

The IT Security Instructions comprise the safety policy, the security guidelines, and the security regulations and performance provisions for information security (data protection and data security), both of MAN and of Volkswagen AG (parent company) (Volkswagen AG documents are to be considered guidelines):

Policy	File
Group Policy MAN 13.1 Information Security MAN - Instruction 1 „Standard for Information Security“	See 1.1
Group Policy MAN 13.1 MAN - Instruction 3 „Information Security Incident Management“ MAN - Instruction 4 „Classification of Information Assets“	See 1.1

MAN - Instruction 7 „Information Security for Users with privileged IT responsibilities“ MAN - Instruction 8 „Information Security for the collaboration with IT Service Providers“	
MAN 13.1 Glossary „Additional Information to Group Policy MAN 13.1”	See 1.1
Volkswagen AG Information Security Global Regulations and Processes - Third Party Service Delivery Management - No 02.03 Version 3.0	 regulation-nr--02-0 3-is-guidelines-for-s
Volkswagen AG Information Security Guidelines for System Developers - No 02.04 v3.0	 regulation-nr--02-0 4-is-guidelines-for-s
Volkswagen AG Information Security Guidelines - Information Security Guidelines for Suppliers - No 02.06 v3.0	 regulation-no--02-0 6-is-guidelines-for-s
Volkswagen AG Information Security Global Regulations and Processes - Third Party Service Delivery Management - No 03.01.16 v1.0	 regulation-no--03-0 1-16-third-party-ser  vergabe-von-konze rn-it-dienstleistung  vergabe-von-konze rn-it-dienstleistung
Volkswagen AG Information Security Requirements Cloudcomputing (german version only)	 cloudcomputing-an forderungen-final.xl

1.3 Data Processing

The term “data processing” describes the requirements set by MAN for data protection during the processing of data. When performing its services, the Contractor shall comply with the MAN data processing regulations and provide its assurance thereof in writing (in this respect, see Appendix 17-E (Data Processing Checklist) and Appendix 17-F (Data Processing Agreement)).

1.4 Data Protection Policy

The “Data Protection – Guidelines and Instructions” document describes the existing data protection guidelines and instructions at MAN. When performing its services, the Contractor shall comply with the data protection regulations.

2.0 SECURITY

The Contractor's duties include:

(a) Complying with the requirements and existing security processes at MAN, the Organizational Instructions, the IT Security Instructions, the nondisclosure agreement, data processing), Data Protection – Guidelines and Instructions), and Information Security Assessment) as amended, unless this has been modified by the Parties and an agreement to the contrary has been made

(b) When performing its contractual services, the Contractor shall comply with the latest standards of information security, observe and carry out the requirements and measures, respectively, outlined in the documents, in particular those referred to in sub-section 1.0, and, in doing so, use state-of-the-art technology to protect MAN systems both against unauthorized third-party attacks (e.g. hacker attacks) and the unwanted transmission of data (e.g. spam). Where the Contractor becomes aware of dangers or security risks to data and information / system security, in particular, it is obliged to notify MAN thereof in electronic form (e-mail) without delay and to immediately initiate efficient countermeasures that do not restrict the performance of contractual services – in close cooperation with MAN and at its own expense

(c) Observing the statutory provisions for data protection and data security that are valid in the countries where the services are performed

(d) In addition to the statutory provisions specific to the country (/ countries) in question, the standard enforced under the Federal Data Protection Act (BDSG) and / or the EU General Data Protection Regulation is to be complied with as a minimum. Said standard must also be applied in countries that do not have their own statutory provisions

(e) A formal assessment of information security to be performed by the MAN IS Security Organization and / or the IS Security Organization of Volkswagen AG (parent company) (ISSO) must be planned for all new systems and applications. The new development in question may not be implemented until it has been approved

(f) Maintaining the required MAN level of security

(g) Submitting a monthly report on information security outlining the main areas of risk within the framework of the performance of services without being requested to do so. The risk areas shall be determined by the Contractor in cooperation with the MAN Security Organization prior to the conclusion of the contract

(h) Carrying out regular vulnerability assessments or penetration tests using suitable tools, as well as reporting on the outcome

(i) Carrying out an ISMS assessment provided by MAN on an annual basis, as well as defining measures for dealing with risks and reporting on the outcome.