PUBLIC
ÖFFENTLICH

APPENDIX 17-A
PROTECTION AND SECURITY PROCEDURES

December 2021

PUBLIC
ÖFFENTLICH

Guidelines for the tendering party

This document contains specific information that 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 (unless otherwise specified or agreed between the parties)).

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 current set of rules of the MAN Group for information security is valid in principle. If explicit MAN Group regulations exist on a specific topic, the MAN Group regulations shall apply with binding effect over the respective Volkswagen Group regulation.

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 information security 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”	See Policy Pack
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“	See Policy Pack
MAN 13.1 Glossary „Additional Information to Group Policy MAN 13.1”	See Policy Pack

1.2 Security Instructions

The Informationsecurity instructions also contain more detailed security regulations and implementation provisions on information security of the parent company Volkswagen AG, which are also to be regarded as binding:

Instruction	File
Volkswagen AG Information Security Global Regulations and Processes - Third Party Service Delivery Management - No 02.03 Version 3.0	See Policy Pack
Volkswagen AG Information Security Guidelines for System Developers - No 02.04 v3.0	See Policy Pack
Volkswagen AG Information Security Guidelines - Information Security Guidelines for Suppliers - No 02.06 v3.0	See Policy Pack
Volkswagen AG Information Security Global Regulations and Processes - Third Party Service Delivery Management - No 03.01.16 v2.1	See Policy Pack
Volkswagen AG Information Security Global Regulations and Processes - Third Party Service Delivery Management Appendix Cloud Computing - No 03.01.16	See Policy Pack
Volkswagen AG Information Security Global Regulations and Processes - Cloud Security - No 03.01.17 v3.0	See Policy Pack

1.3 Data Processing

When performing its services, the Contractor shall comply with the MAN data processing regulations and ensure this contractually (in this respect, see Appendix 17-F (Data Processing Agreement)).

1.4 Data Protection Policy

The data protection -policy describes MAN's existing requirements for data protection. The provider shall comply with the regulations on data protection in the context of providing the services (in this respect, see MAN_4.6_en_Policy_Main_Document_v2.0 in Policy Pack).

2.0 SECURITY

The Contractor's duties include:

(a) Complying with the requirements and existing security processes of MAN, Organizational Instructions, IT Security Instructions, Confidentiality agreement, data processing, data protectionpolicy and Information Security Assessment as amended from time to time, unless otherwise modified and agreed between the Parties.

(b) When provisioning 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 unsolicited transmission of data (e.g. spam). If the Contractor becomes aware of any dangers or security risks to data and information / system security in particular, it must inform MAN of this immediately in electronic form (e-mail) and – in close consultation with MAN and at its own expense - immediately initiate effective countermeasures that do not restrict the provision of contractual services.

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

(d) In addition to the country-specific legal regulations, the standard of the EU General Data Protection Regulation (GDPR) must be adhered to. This is also to be applied in case no corresponding legal regulations exist.

(e) For new systems and applications, a formal information security assessment conducted by the IS organization of MAN (ISi Assessment) and/or Volkswagen Group Information Security must be scheduled. Only after approval may this new development be used/implemented.

(f) Maintaining the required MAN level of security

(g) The unsolicited submission of a monthly information security report describing the main risk areas in the context of the provision of the services. The risk areas shall be defined by the Contractor together with the MAN prior to conclusion of the contract and the reporting shall be coordinated.

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

(i) Regular update of the Information Security Maturity Level (VDA ISA), as well as the definition of measures for risk treatment and corresponding reporting.