Semantix

Foreword

Attached you will find the Data Processing Appendix, which describes in detail the Supplier's responsibility for handling and processing Personal Data. The Appendix is complex and can be difficult to understand, which is why we are providing this short summary as a supplement to help you understand the meaning of the Appendix. This summary is only meant as an aid and is not intended to replace the actual Appendix. Upon signing the Appendix, you agree to the text in the Appendix and are not, in any way, agreeing to any text in this summary.

The Appendix has been created in response to the new European Union (EU) regulations under the General Data Protection Regulation (GDPR). The GDPR is intended to strengthen and unify data protection for all individuals within the EU. The Appendix outlines and details how Suppliers to Semantix are expected to process and handle Personal Data.

Summary of Data Processing Appendix

As a supplier, you shall:

- Follow the laws for processing Personal Data
- Follow any written instructions provided by Semantix
- Not use Personal Data for any purpose other than the purpose defined by Semantix
- Treat all Personal Data as confidential
- Not use subcontractors unless given prior written consent by Semantix
- Have written contracts with subcontractors (if you have subcontractors)
- Be responsible for the fact that all subcontractors follow the same rules set out in this Appendix
- Delete all data, including Personal Data, upon termination of the Agreement with Semantix
- Notify Semantix if any governmental authorities request access to any Personal Data originating from Semantix
- Not share or transfer data to any other third party unless given permission by Semantix
- Not transfer or process Personal Data in a non-European Economic Area (EEA) country without prior written consent by Semantix
- Implement and maintain organisational, operational, managerial, physical and technical measures to protect Personal Data at an appropriate security level to prevent misuse or disclosure of Personal Data
- Comply with a request from Semantix to review the supplier's security documentation (e.g. if you are an agency) and/or written self-assessment stating compliance with the Appendix
- Allow Semantix or a third party auditor, with 12 days written notice, to conduct an audit of the supplier's processing activities
    - E.g. an audit can be done via a questionnaire, or it can be an on-site audit
- Pay for improvements at its own expense if the audit reveals problems with security
- Provide Semantix with written notice at latest 24 hours upon a Personal Data breach (12 hours for IT suppliers)
- Work with Semantix to find a solution to the Personal Data breach
- Comply with the rights of Data Subjects (the persons whose Personal Data have been used or stored), including potentially delete Personal Data
- Not hold Semantix liable in any way for the Supplier's failure to follow its obligations under the Appendix

- Compensate Semantix for damage claims directed against Semantix when such claim is caused by the Supplier.