



Data Processing Agreement

Schedule to the Business Intelligence as a Service Agreement (ITBIaaS)



1 The scope of the Data Processing Agreement

- 1.1 In this Schedule [DPA] (Data Processing Agreement) to the Business Intelligence as a Service Agreement (ITBIaaS), SMT Data will be referred to as the “Data Processor” and [Customer] will be referred to as the “Data Controller”.
- 1.2 The Data Processor will during the term of the Agreement be processing personal data on behalf of the Data Controller for the purposes set out in Attachment 1 (Purpose, types of personal data and data subjects).
- 1.3 Any defined terms used in this Schedule [DPA] (Data Processing Agreement) shall have the meaning set out in the Agreement. Any terms used in this Schedule [DPA] (Data Processing Agreement) shall be interpreted to have the meaning ascribed to them in the provisions laid down in the Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the “GDPR”) and any applicable laws implementing it and or any later amendments hereof, including any additional applicable local laws regulating the processing of personal data (hereinafter altogether referred to as the “Data Protection Legislation”).

2 Instructions and security

- 2.1 The Data Processor shall only process personal data based on documented instructions from the Data Controller, unless the Data Processor is required to process the personal data to comply with European Union or Member State law to which the Data Processor is subject. In that case, the Data Processor shall inform the Data Controller hereof before the Data Processor processes the data.
- 2.2 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Data Processor shall take all measures required pursuant to the Data Protection Legislation, including implementing appropriate technical and organizational security measures to protect the personal data against accidental or unlawful destruction, loss or alteration and against unauthorized disclosure, abuse or other processing in violation of the provisions laid down in the Data Protection Legislation.
- 2.3 At the Data Controller’s reasonable request, the Data Processor shall provide the information and documentation needed for the Data Controller to demonstrate compliance with the security provisions in the Data Protection Legislation.
- 2.4 Upon the Data Controller’s written request, the Data Processor shall permit the Data Controller or any third party appointed by the Data Controller (subject to reasonable and appropriate confidentiality undertakings), to audit the Data Processor’s data processing activities and compliance with all reasonable requests or directions by the Data Controller to enable the Data Controller to verify and/or procure that the Data Processor and/or subprocessors are in full compliance with their obligations under this Agreement and the Data



Protection Legislation. Unless required by the Data Protection Legislation or a data breach has occurred, no audits will be conducted more than once in any twelve (12) month period. The Data Processor shall be entitled to charge the Data Controller a reasonable fee for its assistance in relation to the conduct of any audits.

- 2.5 The Data Processor must upon the request of any public authority, grant the authority access to perform an audit or other investigation of the processing of personal data conducted by the Data Processor. The Data Processor shall without undue delay inform the Data Controller in writing upon receiving such request, unless this is expressly prohibited by the public authority.
- 2.6 The Data Processor will ensure that the Data Processor's employees processing personal data on its behalf have committed themselves to the obligation of confidentiality regarding any personal data processed under this Agreement. The obligation of confidentiality will continue after the termination of this Agreement.
- 2.7 The Data Processor will immediately inform the Data Controller if, in its opinion, an instruction infringes the Data Protection Legislation.
- 2.8 The Data Processor shall without undue delay notify the Data Controller of a data subject's request to exercise his/her rights under the Data Protection Legislation, forward the request to the Data Controller and provide cooperation and assistance in relation to the Data Controller's obligation to respond to said request. The Data Processor shall be entitled to charge the Data Controller a reasonable fee for its assistance
- 2.9 The Data Processor shall, taking into account the nature of the processing, assist the Data Controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Data Controller's obligation to respond to requests for exercising the data subject's rights laid down in the Data Protection Legislation.
- 2.10 The Data Processor shall provide all information necessary and assist the Data Controller taking into account the nature of processing, the state of the art, the costs of implementation, the scope, context and purpose of processing, in ensuring compliance with all applicable provisions under the Data Protection Legislation, including but not limited to information needed for the Data Controller to conduct a data protection impact assessment and assist the Data Controller with respect to prior consultations with data protection authorities as required by the Data Controller. The Data Processor shall be entitled to charge the Data Controller a reasonable fee for its assistance.

3 Sub-processing

- 3.1 The Data Processor may sub-contract its processing operations performed on behalf of the Data Controller to a sub-processor upon thirty (30) days' written notice to the Data Controller. The Data Controller shall be entitled to object to the Data Processor's use of a sub-processor. The sub-processors used when entering into the Agreement are set out in Attachment 2 (Sub-processors) to this Schedule [DPA] (Data Processing Agreement).



3.2 Where the Data Processor sub-contracts its obligations, as described in Article 3.1, it shall do so only by way of a written agreement with the sub-processor, which imposes materially the same data protection obligations on the sub-processor as are imposed on the Data Processor under this Agreement. The Data Controller is aware and acknowledges that the Data Processor engage Amazon Web Services in its provision of the services and that Amazon Web Services' processing of personal data in this context will be governed by the AWS GDPR Data Processing Addendum which is part of AWS Service Terms (available at <https://aws.amazon.com/service-terms>). Where the sub-processor fails to fulfil its data protection obligations under such written agreement the Data Processor shall remain fully liable to the Data Controller for the performance of the sub-processor's obligations. This does not affect the rights of data subjects under the GDPR towards the Data Controller and the Data Processor, including any sub-processors.

4 Transfer of Data outside the EEA

4.1 The Data Processor or any of its sub-processors may transfer personal data processed on behalf of the Data Controller out of the European Economic Area (the "EEA") upon thirty (30) days' written notice to the Data Controller, to the extent the Data Controller does not object to the transfer. Notwithstanding the foregoing, the Data Processor may transfer personal data out of the EEA if required under EU or Member State law to which the Data Processor is subject. The Data Processor will comply with the Data Protection Legislation and any requirements established by any data protection authority or other government authorities necessary for the granting of approval by such authorities for the transfer of personal data outside of the EEA. To the extent applicable, the Data Controller agrees to enter into the Commission's standard contractual clauses as set out by Commission Decision of 5 February 2010 with later amendments (the "Model Clauses"), either by providing a power of attorney to the Data Processor to enter into the Model Clauses on behalf of the Data Controller or by entering into the Model Clauses directly with the relevant sub-processor established outside the EEA. The Data Controller is aware and acknowledges that the Data Processor may transfer personal data to Amazon Web Services as part of its provision of the services and that such transfer will be governed by the Model Clauses which are incorporated into the AWS GDPR Data Processing Addendum which is part of the AWS Service Terms (available at <https://aws.amazon.com/service-terms>).

5 Data breach notification

5.1 The Data Processor shall without undue delay notify the Data Controller in case of any identified or potential breach of personal data processed under this Agreement. The Data Processor shall as per the request of the Data Controller assist the Data Controller with communication of any personal data breach to the affected data subjects and relevant authorities. Unless the data breach is due to the default of the Data Processors, the Data Processor shall be entitled to charge the Data Controller a reasonable fee for its assistance.

6 Liability

6.1 The Parties liability under this Data Processing Agreement shall be subject to the limitations applicable under the Business Intelligence as a Service Agreement (ITBIaaS).



Page 5

7

Termination

7.1

This Schedule [DPA] (Data Processing Agreement) shall remain in force as long as the Data Processor processes personal data on behalf of the Data Controller.

7.2

If the Agreement is terminated, the Data Processor will at the choice of the Data Controller, delete all the personal data to the Data Controller, and delete existing copies unless Union or Member State law requires storage of the personal data. If the Data Controller requires return of the personal data or a certification of destruction of the personal data, the Data Controller shall request the return or certification of destruction at the same time as the request for destruction of the personal data, and the Data Processor shall extract the personal data or certify in writing the destruction of the personal data, as applicable. The preparation of such certification or return of data shall be subject to separate payment.

8

Precedence

8.1

If any of the provisions of this Schedule [DPA] (Data Processing Agreement) conflict with the provisions of the Agreement or any other written or oral agreement concluded between the Parties, then the provisions of this Schedule [DPA] (Data Processing Agreement) shall prevail.



Attachment 1

Purpose, types of personal data and data subjects

- 1 The Data Processor will be processing personal data on behalf of the Data Controller for the following purposes:

The Data Processor process mainly technical data to provide business intelligence services in accordance with the Business Intelligence as a Service Agreement (ITBaaS). The data sets processed by the Data Processor may include incidental personal data on system users. This personal data may accordingly be processed by the Data Processor in relation to the provision of the business intelligence services.

- 2 The Data Processor will be processing the following types of personal data:

The personal data processed consist of user credentials belonging to users of the IT-systems in scope of the business intelligence services.

- 3 The Data Processor will be processing personal data regarding the following categories of data subjects:

The data subjects whose personal data is processed are users of the ITsystems in scope of the business intelligence services.

- 4 The Data Processor will be processing personal data for the following duration:

The Data Processor will process personal data during the term of the term of the Business Intelligence as a Service Agreement (ITBaaS).



Attachment 2

Sub-processors

1 Introduction

- 1.1 This Attachment 2 (Sub-processors) sets out the sub-processors' processing of personal data under the Agreement.

Sub-processor (Company name, registration no., address, contact details, including contact details of the data protection officer (if any) etc.)	Scope of processing	Types of personal data	Processing (and storage) locations (e.g. country/state)	How is personal data transferred to or access by the sub-processor	What is the legal basis for transfer of personal data outside the EU/EEA area (if applicable)
<i>Amazon Web Services EMEA SARL, 38 Avenue John F. Kennedy, L-1855, Luxembourg</i>	<i>Provision of infrastructure as a service used in the provision of the services under the Business Intelligence as a Service Agreement (ITBIaaS).</i>	User credentials belonging to users of the ITsystems in scope of the business intelligence services	<i>Ireland</i>	<i>FTPS</i>	<i>Commission's Standard Contractual Clauses</i>