Appendix: Data Processing Agreement pursuant to Article 28 of the GDPR

Based on the Standard Contractual Clauses of the European Commission pursuant to Implementing Decision (EU) 2021/915

1. Purpose and scope

(a) The purpose of these Standard Contractual Clauses (the Clauses) is to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 of the European Parliament and of the Council 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, and repealing Directive 95/46/EC (General Data Protection Regulation).

(b) The controllers and processors listed in Annex I have agreed to these Clauses in order to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 and/or Article 29(3) and (4) of Regulation (EU) 2018/1725.

(c) These Clauses apply to the processing of personal data as specified in Annex II.

(d) Annexes I to IV are an integral part of the Clauses.

(e) These Clauses are without prejudice to obligations to which the controller is subject by virtue of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(f) These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

2. Invariability of the Clauses

(a) The Parties undertake not to modify the Clauses, except for adding information to the Annexes or updating information in them.

(b) This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a broader contract, or from adding other clauses or additional safeguards provided that they do not directly or indirectly contradict the Clauses or detract from the fundamental rights or freedoms of data subjects.

3. Interpretation

(a) Where these Clauses use the terms defined in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively.

(c) These Clauses shall not be interpreted in a way that runs counter to the rights and obligations provided for in Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or in a way that prejudices the fundamental rights or freedoms of the data subjects.

4. Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties existing at the time when these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

5. Docking clause (not applicable)

6. Description of processing(s)

The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the controller, are specified in Annex II.

7. Obligations of the Parties

7.1. Instructions

(a) The processor shall process personal data only on documented instructions from the controller, unless required to do so by Union or Member State law to which the processor is subject. In this case, the processor shall inform the controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the controller throughout the duration of the processing of personal data. These instructions shall always be documented.

(b) The processor shall immediately inform the controller if, in the processor's opinion, instructions given by the controller infringe Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or the applicable Union or Member State data protection provisions.

7.2. Purpose limitation

The processor shall process the personal data only for the specific purpose(s) of the processing, as set out in Annex II, unless it receives further instructions from the controller.

7.3. Duration of the processing of personal data

Processing by the processor shall only take place for the duration specified in Annex II.

7.4. Security of processing

(a) The processor shall at least implement the technical and organisational measures specified in Annex III to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data (personal data breach). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for the data subjects.

(b) The processor shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the contract. The processor shall ensure that persons authorised to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

7.5. Sensitive data

If the processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences ("sensitive data"), the processor shall apply specific restrictions and/or additional safeguards.

7.6. Documentation and compliance

(a) The Parties shall be able to demonstrate compliance with these Clauses.

(b) The processor shall deal promptly and adequately with inquiries from the controller about the processing of data in accordance with these Clauses.

(c) The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and stem directly from Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725. At the controller's request, the processor shall also permit and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, the controller may take into account relevant certifications held by the processor.

(d) The controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the processor and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/ies on request.

7.7. Use of sub-processors

(a) The processor has the controller's general authorisation for the engagement of sub-processors from an agreed list. The processor shall specifically inform in writing the controller of any intended changes of that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s). The processor shall provide the controller with the information necessary to enable the controller to exercise the right to object.

(b) Where the processor engages a sub-processor for carrying out specific processing activities (on behalf of the controller), it shall do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the data processor in accordance with these Clauses. The processor shall ensure that the sub-processor complies with the obligations to which the processor is subject pursuant to these Clauses and to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(c) At the controller's request, the processor shall provide a copy of such a sub-processor agreement and any subsequent amendments to the controller. To the extent necessary to protect business secret or other confidential information, including personal data, the processor may redact the text of the agreement prior to sharing the copy.

(d) The processor shall remain fully responsible to the controller for the performance of the sub-processor's obligations in accordance with its contract with the processor. The processor shall notify the controller of any failure by the sub-processor to fulfil its contractual obligations.

(e) The processor shall agree a third party beneficiary clause with the sub-processor whereby - in the event the processor has factually disappeared, ceased to exist in law or has become insolvent - the controller shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

7.8. International transfers

(a) Any transfer of data to a third country or an international organisation by the processor shall be done only on the basis of documented instructions from the controller or in order to fulfil a specific requirement under Union or Member State law to which the processor is subject and shall take place in compliance with Chapter V of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725.

(b) The controller agrees that where the processor engages a sub-processor in accordance with Clause 7.7. for carrying out specific processing activities (on behalf of the controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the processor and the sub-processor can ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the Commission in accordance with of Article 46(2) of Regulation (EU) 2016/679, provided the conditions for the use of those standard contractual clauses are met.

8. Assistance to the controller

(a) The processor shall promptly notify the controller of any request it has received from the data subject. It shall not respond to the request itself, unless authorised to do so by the controller.

(b) The processor shall assist the controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with (a) and (b), the processor shall comply with the controller's instructions

(c) In addition to the processor's obligation to assist the controller pursuant to Clause 8(b), the processor shall furthermore assist the controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the processor:

(1) the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a 'data protection impact assessment') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;

(2) the obligation to consult the competent supervisory authority/ies prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk;

(3) the obligation to ensure that personal data is accurate and up to date, by informing the controller without delay if the processor becomes aware that the personal data it is processing is inaccurate or has become outdated;

(4) the obligations in Article 32 of Regulation (EU) 2016/679.

(d) The Parties shall set out in Annex III the appropriate technical and organisational measures by which the processor is required to assist the controller in the application of this Clause as well as the scope and the extent of the assistance required.

9. Notification of personal data breach

In the event of a personal data breach, the processor shall cooperate with and assist the controller for the controller to comply with its obligations under Articles 33 and 34 of Regulation (EU) 2016/679 or under Articles 34 and 35 of Regulation (EU) 2018/1725, where applicable, taking into account the nature of processing and the information available to the processor.

9.1 Data breach concerning data processed by the controller

In the event of a personal data breach concerning data processed by the controller, the processor shall assist the controller:

(a) in notifying the personal data breach to the competent supervisory authority/ies, without undue delay after the controller has become aware of it, where relevant/(unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);

(b) in obtaining the following information which, pursuant to Article 33(3) of Regulation (EU) 2016/679, shall be stated in the controller's notification, and must at least include:

(1) the nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

(2) the likely consequences of the personal data breach;

(3) the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(c) in complying, pursuant to Article 34 of Regulation (EU) 2016/679, with the obligation to communicate without undue delay the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

9.2 Data breach concerning data processed by the processor

In the event of a personal data breach concerning data processed by the processor, the processor shall notify the controller without undue delay after the processor having become aware of the breach. Such notification shall contain, at least:

(a) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);

(b) the details of a contact point where more information concerning the personal data breach can be obtained;

(c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

The Parties shall set out in Annex III all other elements to be provided by the processor when assisting the controller in the compliance with the controller's obligations under Articles 33 and 34 of Regulation (EU) 2016/679.

10. Non-compliance with the Clauses and termination

(a) Without prejudice to any provisions of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725, in the event that the processor is in breach of its obligations under these Clauses, the controller may instruct the processor to suspend the processing of personal data until the latter complies with these Clauses or the contract is terminated. The processor shall promptly inform the controller in case it is unable to comply with these Clauses, for whatever reason.

(b) The controller shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with these Clauses if:

  (1) the processing of personal data by the processor has been suspended by the controller pursuant to point (a) and if compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;

  (2) the processor is in substantial or persistent breach of these Clauses or its obligations under Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725;

  (3) the processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to these Clauses or to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(c) The processor shall be entitled to terminate the contract insofar as it concerns processing of personal data under these Clauses where, after having informed the controller that its instructions infringe applicable legal requirements in accordance with Clause 7.1 (b), the controller insists on compliance with the instructions.

(d) Following termination of the contract, the processor shall, at the choice of the controller, delete all personal data processed on behalf of the controller and certify to the controller that it has done so, or, return all the personal data to the controller and delete existing copies unless Union or Member State law requires storage of the personal data. Until the data is deleted or returned, the processor shall continue to ensure compliance with these Clauses.

ANNEX I

List of parties

Controller(s): The data controller is the relevant Client of BOC Group named in the underlying contract.

Processor(s): The data processor is the BOC Group company named as the contracting party in the underlying contract.

ANNEX II

Description of the processing

Categories of data subjects whose personal data is processed

- Contact Persons
- Employees

Categories of personal data processed

- Contact Details (Name, E-Mail)
- Organisational Information
- Responsibilities
- Application Usage Data

Nature and purposes of the processing

The nature and purposes of the processing of personal data by the processor on behalf of the controller are, depending on the specific subject matter of the contract, one or more of the following:

- Development/Adaptation of a customised software solution and tests with transmitted data.
- Implementation of consulting projects with access to personal data of the Client.
- Support in the scope of the maintenance of the software, where personal data of Client may be viewed or processed.
- Operation of ADONIS NP / ADOIT / ADOGRC as Software-as-a-Service (SaaS).
- Retention of transmitted data sets to enable faster processing of future support cases or faster creation/adaptation/testing of future customer-specific software solutions.

Duration of the processing

During the term of the underlying contract.

ANNEX III

Technical and organisational measures including technical and organisational measures to ensure the security of the data

- Physical access control measures (e.g. physical security of premises housing data processing equipment, access restricted to authorised persons only, appropriate organisational arrangements for visitors and external third parties)
- Logical access control measures (e.g. use of appropriate authentication procedures, protection of system access against unauthorised use, regulated granting and revocation of user access, regular review of access grants)
- Data access control measures (e.g. access to personal data restricted to authorised persons, role based access concepts, access authorization to be granted by data owner)
- Measures for disclosure control (e.g. protection of personal data during transmission and transport, use of appropriate technical and organisational security measures, such as encryption, and regulations for the data protection-compliant destruction of data storage media)
- Input control measures (e.g. traceability of the input, modification and deletion of personal data, use of appropriate logging mechanisms)
- Measures for order control (e.g. processing of personal data exclusively on the instructions of the controller, controlled engagement of sub-processors, obligation of persons entrusted with processing to maintain confidentiality)

- Measures for availability control (e.g. protection of personal data against loss and destruction, use of appropriate measures for data backup and recovery)
- Processing of personal data only for specified purposes
- Ensuring that data collected for different purposes can be processed separately
- Operation of the SaaS environment's IT systems in data centres certified to ISO 27001 and ISO 27018

The technical and organisational measures used may be further developed in line with the state of the art. The data processor may implement appropriate alternative measures, provided these offer at least an equivalent level of security. It further undertakes to maintain continuous certification to ISO 27001 and ISO 27018.

A detailed description of the technical and organisational measures taken will be provided to the data controller for inspection upon request.

ANNEX IV

List of sub-processors

The controller has authorised the use of the following sub-processors:

Sub-Processor	Address	Description of Processing
BOC Products & Services AG	Operngasse 20b, 1040 Vienna, Austria	Client Support (Hotline), Cloud Services, Marketing Services, Customer Relationship Management, Consulting Projects, Partner Management, Solution Projects, Back Office Services (System Administration)
BOC Information Technologies Consulting Ltd.	21 Priory Office Park, Stillorgan, Co Dublin, A94 F660, Ireland	Consulting Projects, Solution Projects
BOC Information Technologies Consulting GmbH	Naglerstraße 5, 10245 Berlin, Germany	Client Support (Hotline), Consulting Projects, Solution Projects
BOC Information Technologies Consulting GmbH	Stadthausstraße 14, 8400 Winterthur, Switzerland	Consulting Projects, Solution Projects
BOC Information Technologies Consulting Sp. Z o.o.	Ul. Panska 96 lok. 59, 00-837 Warsaw, Poland	Consulting Projects, Solution Projects
BOC Business Objectives Consulting Ibérica S.L.U.	Velazquez 71, 28006 Madrid, Spain	Client Support (Hotline), Consulting Projects, Solution Projects
BOC Information Technologies Consulting SaS	5 Rue du Helder, 75009 Paris, France	Consulting Projects, Solution Projects
BOC Information Technologies Consulting GmbH	Avlidos 5 & Kessarias, 11527 Athen, Greece	Consulting Projects, Solution Projects

Insofar as the main contract relates to hosted services in the data processor's cloud, the data processor also makes use of standardised infrastructure services (IaaS) provided by the following providers. The data controller hereby confirms one of the following options, depending on the subject matter and terms of the contract:

Option 1:

Sub-Processor	Address	Description of Processing
Amazon Web Services EMEA Sàrl	38 Avenue John F. KennedyL-1855 Luxembourg; Data Center: Germany (eu-central-1)	Infrastructure-as-a-Service (IaaS) for the operation of hosted cloud services (primary systems)
Amazon Web Services EMEA Sàrl	Amazon Web Services EMEA Sàrl, 38 Avenue John F. KennedyL-1855, Luxembourg; Data Center: France (eu-west-3)	Infrastructure-as-a-Service (IaaS) for disaster recovery purposes

Option 2:

Sub-Processor	Address	Description of Processing
CloudSigma AG	Badenerstraße 549, 8048 Zurich, Switzerland; Data Center: Switzerland	Infrastructure-as-a-Service (IaaS) for the operation of hosted cloud services (primary systems)
Amazon Web Services EMEA Sàrl	Amazon Web Services EMEA Sàrl, 38 Avenue John F. KennedyL-1855, Luxembourg; Data Center: France (eu-west-3)	Infrastructure-as-a-Service (IaaS) for disaster recovery purposes