Appendix 2 – Data processing agreement

Standard contractual clauses

SECTION I

Clause 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.

Clause 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.

Clause 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.

Clause 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.

Clause 5

Docking clause

a) Any entity that is not a Party to these Clauses may, with the agreement of all the Parties, accede to these Clauses at any time as a controller or a processor by completing the Annexes and signing Annex I.

b) Once the Annexes in (a) are completed and signed, the acceding entity shall be treated as a Party to these Clauses and have the rights and obligations of a controller or a processor, in accordance with its designation in Annex I.

c) The acceding entity shall have no rights or obligations resulting from these Clauses from the period prior to becoming a Party.

Section II

Obligations of the parties

Clause 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.

Clause 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 organizational 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, unauthorized 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 authorized 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 authorization 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 4 weeks 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 organization 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.

Clause 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 authorized 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 organizational 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.

Clause 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.

Section III

Final Provisions

Clause 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):

Name:
Address:
Contact person’s name, position and contact details:

Signature and accession date

Processor(s):

Strategy Compass GmbH

Engerstraße 21

40235 Düsseldorf

Name, Funktion und Kontaktdaten der Kontaktperson: Achim Sztuka, CEO

Rolle (Processor): CEO

info@strategy-compass.com

A. Sz

Düsseldorf, 01.04.2023

Annex II

Description of the processing

Categories of data subjects whose personal data is processed

Customer employees

Categories of personal data processed

The data entered or uploaded by the user, as well as the e-mail address, first and last name of the user and the information whether the user is a regular user or guest user in Azure Active Directory.

Nature of the processing

Continuous transmission

Purpose(s) for which the personal data is processed on behalf of the controller

Deployment of the processor's software solutions (Microsoft365 integrations)

Duration of the processing

The data is stored for the fulfillment of the contractual main performance obligations of the processor and stored until the expiry of the purpose, alternatively in accordance with the statutory specified retention obligations and then deleted.

Annex III

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

If the services of the Processor are provided by means of a so-called Software-as-a-Service (SaaS) solution, the software will be operated in an infrastructure of the third-party provider Microsoft specified in Annex III. In this relationship, the following technical and organizational measures are agreed:

1. Organization of Information Security

Security Ownership. Microsoft has appointed one or more security officers responsible for coordinating and monitoring the security rules and procedures.

Security Roles and Responsibilities. Microsoft personnel with access to Customer Data or Professional Services Data are subject to confidentiality obligations.

Risk Management Program. Microsoft performed a risk assessment before processing the Customer Data or launching the Online Services service and before processing Professional Service Data or launching the Professional Services.

Microsoft retains its security documents pursuant to its retention requirements after they are no longer in effect.

2. Asset Management

Asset Inventory. Microsoft maintains an inventory of all media on which Customer Data or Professional Services Data is stored. Access to the inventories of such media is restricted to Microsoft personnel authorized in writing to have such access.

Asset Handling

- Microsoft classifies Customer Data and Professional Services Data to help identify it and to allow for access to it to be appropriately restricted.
- Microsoft imposes restrictions on printing Customer Data and Professional Services Data and has procedures for disposing of printed materials that contain such data.

Microsoft personnel must obtain Microsoft authorization prior to storing Customer Data or Professional Services Data on portable devices, remotely accessing such data, or processing such data outside Microsoft’s facilities.

3. Human Resources Security

Security Training. Microsoft informs its personnel about relevant security procedures and their respective roles. Microsoft also informs its personnel of possible consequences of breaching the security rules and procedures. Microsoft will only use anonymous data in training.

4. Physical and Environmental Security

Physical Access to Facilities. Microsoft limits access to facilities where information systems that process Customer Data or Professional Services Data are located to identified authorized individuals.

Physical Access to Components. Microsoft maintains records of the incoming and outgoing media containing Customer Data or Professional Services Data, including the kind of media, the authorized sender/recipients, date and time, the number of media and the types of such data they contain.

Protection from Disruptions. Microsoft uses a variety of industry standard systems to protect against loss of data due to power supply failure or line interference.

Component Disposal. Microsoft uses industry standard processes to delete Customer Data and Professional Services Data when it is no longer needed.

5. Communications and Operations Management

Operational Policy. Microsoft maintains security documents describing its security measures and the relevant procedures and responsibilities of its personnel who have access to Customer Data or Professional Services Data.

Data Recovery Procedures

- On an ongoing basis, but in no case less frequently than once a week (unless no updates have occurred during that period), Microsoft maintains multiple copies of Customer Data and Professional Services Data from which such data can be recovered.
- Microsoft stores copies of Customer Data and Professional Services Data and data recovery procedures in a different place from where the primary computer equipment processing the Customer Data and Professional Services Data are located.
- Microsoft has specific procedures in place governing access to copies of Customer Data and Professional Services Data.
- Microsoft reviews data recovery procedures at least every six months, except for data recovery procedures for Professional Services and for Azure Government Services, which are reviewed every twelve months.
- Microsoft logs data restoration efforts, including the person responsible, the description of the restored data and where applicable, the person responsible and which data (if any) had to be input manually in the data recovery process.

Malicious Software. Microsoft has anti-malware controls to help avoid malicious software gaining unauthorized access to Customer Data and Professional Services Data, including malicious software originating from public networks.

Data Beyond Boundaries

- Microsoft encrypts, or enables Customer to encrypt, Customer Data and Professional Services Data that is transmitted over public networks.
- Microsoft restricts access to Customer Data and Professional Services Data in media leaving its facilities.

Event Logging. Microsoft logs, or enables Customer to log, access and use of information systems containing Customer Data or Professional Services Data, registering the access ID, time, authorization granted or denied, and relevant activity.

6. Access Control

Access Policy. Microsoft maintains a record of security privileges of individuals having access to Customer Data or Professional Services Data.

Access Authorization

- Microsoft maintains and updates a record of personnel authorized to access Microsoft systems that contain Customer Data or Professional Services Data.

- Microsoft deactivates authentication credentials that have not been used for a period of time not to exceed six months.
- Microsoft identifies those personnel who may grant, alter or cancel authorized access to data and resources.
- Microsoft ensures that where more than one individual has access to systems containing Customer Data or Professional Services Data, the individuals have separate identifiers/log-ins.

Least Privilege

- Technical support personnel are only permitted to have access to Customer Data and Professional Services Data when needed.
- Microsoft restricts access to Customer Data and Professional Services Data to only those individuals who require such access to perform their job function.

Integrity and Confidentiality

- Microsoft instructs Microsoft personnel to disable administrative sessions when leaving premises Microsoft controls or when computers are otherwise left unattended.
- Microsoft stores passwords in a way that makes them unintelligible while they are in force.

Authentication

- Microsoft uses industry standard practices to identify and authenticate users who attempt to access information systems.
- Where authentication mechanisms are based on passwords, Microsoft requires that the passwords are renewed regularly.
- Where authentication mechanisms are based on passwords, Microsoft requires the password to be at least eight characters long.
- Microsoft ensures that de-activated or expired identifiers are not granted to other individuals.
- Microsoft monitors, or enables Customer to monitor, repeated attempts to gain access to the information system using an invalid password.
- Microsoft maintains industry standard procedures to deactivate passwords that have been corrupted or inadvertently disclosed.
- Microsoft uses industry standard password protection practices, including practices designed to maintain the confidentiality and integrity of passwords when they are assigned and distributed, and during storage.

Network Design. Microsoft has controls to avoid individuals assuming access rights they have not been assigned to gain access to Customer Data or Professional Services Data they are not authorized to access.

7. Information Security Incident Management

Incident Response Process

- Microsoft maintains a record of security breaches with a description of the breach, the time period, the consequences of the breach, the name of the reporter, and to whom the breach was reported, and the procedure for recovering data.
- For each security breach that is a Security Incident, notification by Microsoft (as described in the “Security Incident Notification” section above) will be made without undue delay and, in any event, within 72 hours.
- Microsoft tracks, or enables Customer to track, disclosures of Customer Data and Professional Services Data, including what data has been disclosed, to whom, and at what time.

Service Monitoring. Microsoft security personnel verify logs at least every six months to propose remediation efforts if necessary.

8. Business Continuity Management

- Microsoft maintains emergency and contingency plans for the facilities in which Microsoft information systems that process Customer Data or Professional Services Data are located.
- Microsoft's redundant storage and its procedures for recovering data are designed to attempt to reconstruct Customer Data and Professional Services Data in its original or last-replicated state from before the time it was lost or destroyed.

Annex IV

List of sub-processors

The controller has authorized the use of the following subcontracted processor:

Microsoft Enterprise Service-Privacy

Microsoft Corporation

One Microsoft Way

Redmond, Washington 98052, USA

Description of the processing: The SaaS solution of the processor is operated in a data center of the sub-processor (hosting).