Block 64 – DATA PROTECTION ADDENDUM for Customers in EU Countries

For the purposes of compliance with Article 28(3) of General Data Protection Regulation 2016/679 (the "GDPR")

In this Addendum Block 64 Corporation shall be referred to as the "**data processor"** and the **Customer** (as defined in the Agreement) will also be referred to as the "**data controller".**

Data Controller and Data Processor have agreed upon the following in order to meet the requirements of the GDPR.

1. This Addendum sets out the rights and obligations of the data controller and the data processor, when processing personal data of Customer on behalf of the data controller.

2. This Addendum has been designed to ensure the parties' compliance with Article 28(3) of the GDPR on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

3. In the context of the provision of the Services as defined in the Agreement, the data processor will process personal data on behalf of the data controller in accordance with this Addendum.

4. This Addendum shall take priority over any similar provisions contained in the Agreement between the parties.

5. Two appendices are attached to this Addendum and form an integral part of this Addendum.

6. Appendix A contains details about the processing of personal data, including the purpose and nature of the processing, type of personal data, categories of data subject and duration of the processing.

7. Appendix B contains provisions for other activities which are not covered by this Addendum.

8. This Addendum along with appendices shall be retained in writing, including electronically, by both parties.

9. This Addendum shall not exempt the data processor from obligations to which the data processor is subject pursuant to the GDPR or other legislation.

3. The rights and obligations of the data controller

1. The data controller is responsible for ensuring that the processing of personal data takes place in compliance with the GDPR (see Article 24 GDPR), the applicable EU or Member State data protection provisions and this Addendum.

2. The data controller has the right and obligation to make decisions about the purposes and means of the processing of personal data.

3. The data controller shall be responsible, among other things, for ensuring that the processing of personal data, which the data processor is instructed to perform, has a legal basis.

4. The data processor acts according to instructions

1. The data processor shall process personal data only on acceptance of the Block 64 End User License Agreement, unless required to do so by Union or Member State law to which the processor is subject. Subsequent instructions can also be given by the data controller throughout the duration of the processing of personal data, but such instructions shall always be documented and kept in writing, including electronically, in connection with this Addendum.

2. The data processor shall immediately inform the data controller if instructions given by the data controller, in the opinion of the data processor, contravene the GDPR or the applicable EU or Member State data protection provisions.

5. Confidentiality

1. The data processor shall only grant access to the personal data being processed on behalf of the data controller to persons under the data processor's authority who have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and only on a need to know basis. The list of persons to whom access has been granted shall be kept under periodic review. On the basis of this review, such access to personal data can be withdrawn, if access is no longer necessary, and personal data shall consequently not be accessible anymore to those persons.

2. The data processor shall at the request of the data controller demonstrate that the concerned persons under the data processor's authority are subject to the abovementioned confidentiality.

6. Security of processing

1. Article 32 GDPR stipulates that, 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 controller and data processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk.

   The data controller shall evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. Depending on their relevance, the measures may include the following:

   a. Pseudonymization and encryption of personal data;

   b. the ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services;

   c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

   d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

2. The data processor shall also – independently from the data controller – evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. To this effect, the data controller shall provide the data processor with all information necessary to identify and evaluate such risks.

3. Furthermore, the data processor shall assist the data controller in ensuring compliance with the data controller's obligations pursuant to Articles 32 GDPR, by *inter alia* providing the data controller with information concerning the technical and organizational measures already implemented by the data processor pursuant to Article 32 GDPR along with all other information necessary for the data controller to comply with the data controller's obligation under Article 32 GDPR.

   If subsequently – in the assessment of the data controller – mitigation of the identified risks requires further measures to be implemented by the data processor, than those already implemented by the data processor pursuant to Article 32 GDPR, the data controller shall specify these additional measures to be implemented.

7. Use of sub-processors

1. The data processor shall not use sub-processors.

8. Transfer of data to third countries or international organizations

1. Any transfer of personal data to third countries or international organizations by the data processor shall only occur on the basis of documented instructions from the data controller and shall always take place in compliance with Chapter V GDPR.

2. In case transfers to third countries or international organizations, which the data processor has not been instructed to perform by the data controller, is required under EU or Member State law to which the data processor is subject, the data processor shall inform the data controller of that legal requirement prior to processing unless that law prohibits such information on important grounds of public interest.

3. Without documented instructions from the data controller, the data processor therefore cannot within the framework of this Addendum:

   a. transfer personal data to a data controller or a data processor in a third country or in an international organization

   b. transfer the processing of personal data to a sub-processor in a third country

   c. have the personal data processed in by the data processor in a third country

4. The data controller's instructions regarding the transfer of personal data to a third country including, if applicable, the transfer tool under Chapter V GDPR on which they are based, shall be set out in Appendix B.6.

5. This Addendum shall not be confused with standard data protection clauses within the meaning of Article 46(2)(c) and (d) GDPR, and this Addendum cannot be relied upon by the parties as a transfer tool under Chapter V GDPR.

9. Assistance to the data controller

1. Taking into account the nature of the processing, the data processor shall assist the data controller by appropriate technical and organizational measures, insofar as this is possible, in the fulfilment of the data controller's obligations to respond to requests for exercising the data subject's rights laid down in Chapter III GDPR.

   This entails that the data processor shall, insofar as this is possible, assist the data controller in the data controller's compliance with:

   a. the right to be informed when collecting personal data from the data subject
   b. the right to be informed when personal data have not been obtained from the data subject
   c. the right of access by the data subject
   d. the right to rectification
   e. the right to erasure ('the right to be forgotten')
   f. the right to restriction of processing
   g. notification obligation regarding rectification or erasure of personal data or restriction of processing
   h. the right to data portability
   i. the right to object
   j. the right not to be subject to a decision based solely on automated processing, including profiling

2. In addition to the data processor's obligation to assist the data controller pursuant to Clause 6.3, the data processor shall furthermore, taking into account the nature of the processing and the information available to the data processor, assist the data controller in ensuring compliance with:

   a. The data controller's obligation to without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the competent supervisory authority, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons;

   b. the data controller's obligation to without undue delay communicate 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;

   c. the data controller's 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);

   d. the data controller's obligation to consult the competent supervisory authority, 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 data controller to mitigate the risk.

3. The parties shall define in Appendix B the appropriate technical and organizational measures by which the data processor is required to assist the data controller as well as the scope and the extent of the assistance required. This applies to the obligations foreseen in Clause 9.1. and 9.2.

10. Notification of personal data breach

1. In case of any personal data breach, the data processor shall, without undue delay after having become aware of it, notify the data controller of the personal data breach.

2. The data processor's notification to the data controller shall, if possible, take place within 48 hours after the data processor has become aware of the personal data breach to enable the data controller to comply with the data controller's obligation to notify the personal data breach to the competent supervisory authority, cf. Article 33 GDPR.

3. In accordance with Clause 9(2)(a), the data processor shall assist the data controller in notifying the personal data breach to the competent supervisory authority, meaning that the data processor is required to assist in obtaining the information listed below which, pursuant to Article 33(3)GDPR, shall be stated in the data controller's notification to the competent supervisory authority:

    a. 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;

    b. the likely consequences of the personal data breach;

    c. 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.

4. The parties shall define in Appendix B all the elements to be provided by the data processor when assisting the data controller in the notification of a personal data breach to the competent supervisory authority.

11. Erasure and return of data

1. On termination of the provision of personal data processing services, the data processor shall be under obligation to delete all personal data processed on behalf of the data controller within 90 days, and if requested certify to the data controller that it has done so unless Union or Member State law requires storage of the personal data.

12. Audit and inspection

1. The data processor shall make available to the data controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 and this Addendum and allow for and contribute to audits, including inspections, conducted by the data controller or another auditor mandated by the

data controller.

2. Procedures applicable to the data controller's audits, including inspections, of the data processor and sub-processors are specified in appendices C.7. and C.8.

3. The data processor shall be required to provide the supervisory authorities, which pursuant to applicable legislation have access to the data controller's and data processor's facilities, or representatives acting on behalf of such supervisory authorities, with access to the data processor's physical facilities on presentation of appropriate identification.

13. The parties' agreement on other terms

1. The parties may agree other clauses concerning the provision of the personal data processing service specifying e.g. liability, as long as they do not contradict directly or indirectly this Addendum or prejudice the fundamental rights or freedoms of the data subject and the protection afforded by the GDPR.

14. Commencement and termination

1. This Addendum shall become effective on the date of both parties' signature.

2. Both parties shall be entitled to require this Addendum renegotiated if changes to the law or inexpediency of this Addendum should give rise to such renegotiation.

3. This Addendum shall apply for the duration of the provision of personal data processing services. For the duration of the provision of personal data processing services, this Addendum cannot be terminated unless other Clauses governing the provision of personal data processing services have been agreed between the parties.

4. If the provision of personal data processing services is terminated, and the personal data is deleted or returned to the data controller pursuant to Clause 11.1. and Appendix B.4., this Addendum may be terminated by written notice by either party.

Appendix A

A.1. The purpose of the data processor's processing of personal data on behalf of the data controller is:

To provide recommendations regarding the data controller's installed software, hardware, and cloud services.

A.2. The data processor's processing of personal data on behalf of the data controller shall mainly pertain to (the nature of the processing):

The inventory of the records within the data controller's directory service (Active Directory, Azure Active Directory, etc.) and the inventory of endpoints and usernames thereon.

A.3. The processing includes the following types of personal data about data subjects:

- Given Name
- Surname
- Email address
- Username
- SIP address
- Email mailbox name

A.4. Processing includes the following categories of data subject:

Records contained within the data controller's directory service, which typically are limited to:

- Employees
- Contractors
- Trainees
- Visitors

A.5. The data processor's processing of personal data on behalf of the data controller may be performed when this Addendum commence. Processing has the following duration:

Processing is conducted solely during engagement between the data controller and data processor.

Appendix B

B.1. The subject of/instruction for the processing

The data processor's processing of personal data on behalf of the data controller shall be carried out by the data processor performing the following:

To provide solutions assessments regarding the data controller's software, hardware, and services.

B.2. Security of processing

The level of security shall consider the nature, scope, and context of the datapoints referenced in Appendix A and the limited risk to natural persons.

The data processor shall – in any event and at a minimum – implement the following measures that have been agreed with the data controller:

- Encryption of data at rest
- Encryption of data in transit

The data processor shall maintain the following policies to ensure ongoing confidentiality, integrity, availability, and resilience of systems and services:

- Acceptable Use Policy
- System Access Control Policy
- Encryption Policy
- Information Security Policy
- Data Protection Policy
- Physical Security Policy

The data processor shall maintain both a Backup Policy and a Disaster Recovery Plan that cover the case of a physical or technical incident that may impact the data controller's personal data.

B.3. Assistance to the data controller

The data processor shall insofar as this is possible – within the scope and the extent of the assistance specified below – assist the data controller in accordance with Clause 9.1. and 9.2. by implementing the following technical and organizational measures:

- Tier 1 support staff response within 24 hours
- Tier 2 support staff made available upon request

B.4. Storage period/erasure procedures

Personal data is stored for 90 days after the disengagement with the data controller, after which the personal data is automatically erased by the data processor.

Upon termination of the provision of personal data processing services, the data processor shall either delete

or return the personal data in accordance with Clause 11.1., unless the data controller – after the signature of the contract – has modified the data controller's original choice. Such modification shall be documented and kept in writing, including electronically, in connection with this Addendum.

B.5. Processing location

Processing of the personal data under this Addendum will only be processed in one or more of the following locations, upon authorization from the data controller provided to data processor during the setup and configuration of Block 64 applications:

- Canada
- United States
- United Kingdom
- Germany
- Western Europe
- United Arab Emirates
- Japan
- Australia

B.6. Instruction on the transfer of personal data to third countries

Pertaining to the transfer of personal data to a third country, the data processor shall not be entitled within the framework of this Addendum to perform such transfer.

B.7. Procedures for the data controller's audits, including inspections, of the processing of personal data being performed by the data processor

The data processor shall annually perform a self-attestation and report of GDPR compliance.

The resulting report shall, without undue delay, be submitted to the data controller upon request. The data controller may contest the scope and/or methodology of the report and may in such cases request an audit/inspection under a revised scope and/or different methodology.

Based on the results of such an audit/inspection, the data controller may request further measures to be taken to ensure compliance with the GDPR, the applicable EU or Member State data protection provisions and this Addendum.

The data controller or the data controller's representative shall in addition have access to inspect, including physically inspect, the places, where the processing of personal data is carried out by the data processor, including physical facilities as well as systems used for and related to the processing. Such an inspection shall be performed when the data controller deems it required.