DATA PROCESSOR AGREEMENT

between

IT Relation

and

Cira Apps Limited

dated

Thursday, August 27, 2020

This data processor agreement ("Data Processor Agreement") has been concluded on August 27, 2020 between:

IT Relation, with address Dalgas Pl. 7B, 1. Sal, 7400 Herning, Denmark (referred to below as "Data Controller" or "the Customer"); and

Cira Apps Limited, with address 2255 South Bascom Avenue, Campbell, CA, (referred to below as "Data Processor" or "the Supplier"),

individually called "Party", and together "Parties".

1 DEFINITIONS

"Processing"	means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
"Data Protection Directives"	refers to the Directive 95/46/EC of the European Parliament and of the Council, and the General Data Protection Regulation ("GDPR") (EU) 2016/679, with accompanying implementing regulations and any subsequent legislation that replaces or complements these. In the event of a conflict between the abovementioned regulations, GDPR shall take precedence from 27 August 2020.
"Personal Data"	refers to any information that, directly or indirectly, relates to an identified or identifiable natural person.
"Third Country"	refers to a country which is not a member of the EU or the EEA.
"Subprocessor"	means any data processor employed by the Data Processor who is a Party in this Data Processor Agreement and who processes personal data on behalf of the Data Controller.
"Personal Data Breach"	means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data that is transferred, stored or otherwise processed.

2 BACKGROUND AND PURPOSE

2.1 On 2020-August-27 the Parties have concluded an agreement whereby the Supplier shall assist the Customer with Microsoft 365 Contact and Calendar synchronization ("Main Agreement"). In conjunction with this, the Supplier will process personal data on behalf of the Customer.

2.2 The purpose of this Data Processor Agreement is to regulate the rights and obligations of the Parties that are involved in this assignment by way of processing personal data, and thus ensure that Personal Data is processed in accordance with the applicable Data Protection Directives.

DS

2.3 The Data Processor Agreement shall take precedence over the corresponding provisions of the Main Agreement, provided that nothing is expressly stated in the Main Agreement.

2.4 The purpose of the Processing of Personal Data, as well as the categories of data subjects and categories of personal data that may be included in the execution of the Main Agreement, are set out in Appendix 1 of this Data Processor Agreement.

3 OBLIGATIONS OF THE DATA PROCESSOR

3.1 Security Measures

The Data Processor possesses the necessary technical and organizational capabilities, including technical solutions, skills, financial and human resources, routines and methods, to fulfill their obligations in accordance with this Data Processor Agreement and the applicable Data Protection Directives.

The Data Processor shall, at the request of the Data Controller, prove that the obligations set out in this Data Processor Agreement and applicable Data Protection Directives are fulfilled by providing relevant documentation, referring to relevant and approved code of conduct or certification, enabling and contributing to audits and inspections, or providing the Data Controller with other appropriate evidence.

The Data Processor shall, at the request of the Data Controller, and without undue delay, give the Data Controller or an independent third party upon instructions from the Data Controller, access to necessary information in order to demonstrate that the Data Processor fulfils their obligations under applicable Data Protection Directives and this Data Processor Agreement.

3.2 Instructions

The Data Processor may only process Personal Data on behalf of the Data Controller and for purposes only as set out in Appendix 1 in accordance with the Data Controller's documented instructions unless the Data Processor is required by the applicable provision to process Personal Data for any other purpose or otherwise. If the Data Controller has submitted incomplete or incorrect instructions, the Data Processor shall promptly inform the Data Controller. In case of conflict between various instructions, Appendix 1 shall take precedence over other instructions, provided that nothing else is explicitly agreed between the Parties.

The Data Processor shall without delay inform the Data Controller should it consider that processing has been carried out in violation of applicable Data Protection Directives or other applicable law, and thereafter await instructions from the Data Controller. However, the Data Processor is not entitled to cancel the assignment because of that. What is stated above is only valid if the Data Processor is not by law prevented from providing such notification.

The Data Processor shall keep a record of all categories of processing of Personal Data carried out on behalf of the Data Controller in accordance with the regulations in force at any given time.

3.3 Disclosure of Personal Data

The Data Processor may not transfer or grant access to Personal Data that falls within the scope of this Data Processor Agreement to an external party without the prior written consent of the Data Controller, except when there is a statutory obligation for the Data Processor to do so. If such statutory obligation exists, the Data Processor shall notify the Data Controller before the processing of personal data commences, provided that such notification is not prohibited by law.

3.4 Use of subprocessors

The Data Processor may not employ subprocessors to carry out all or part of the processing of personal data without the prior written consent of the Data Controller. Such approval is hereby given to those subprocessors listed in Appendix 2 of this Data Processor Agreement.

After obtaining consent, the Data Processor shall enter into a written agreement with the subprocessors, which binds the subprocessor to at least the same obligations as the Data Processor under the Main Agreement and this Data Processor Agreement, before the subprocessor can begin the processing of personal data on behalf of the Data Controller. The Data Processor is fully responsible for the way in which the subprocessors process personal data, including security measures.

The Data Processor shall, at the request of the Data Controller, send a copy of the agreement signed by both the Data Processor and the subprocessor.

If a subprocessor is replaced or a new subprocessor is employed, the Data Processor shall inform the Data Controller about this at least 3 months before the change occurs, and obtain their written approval. Approval should be given without undue delay. In the event that the change cannot be accepted by the Data Controller, the Data Processor must find another subprocessor and inform and obtain approval as described above.

3.5 Transfer of Personal Data to a Third Country

The Data Processor may not transfer or disclose Personal Data to a third country or international organization other than in accordance with the Data Controller's written instructions, except when required under applicable Data Protection Directives. If that happens, then the Data Processor shall inform the Data Controller about the legal requirement before transfer, unless such information is prohibited by reference to important public interest or law.

3.6 Confidentiality

The Data Processor shall treat Personal Data in accordance with the confidentiality agreement between the Parties and this Data Processor Agreement, which means that the Data Processor, their employees or subprocessors may not disclose any information to third parties without first obtaining the consent of the Data Controller. In the absence of any applicable confidentiality agreement between the Parties, the Data Processor shall process confidential Personal Data in accordance with the Public Access to Information and Secrecy Act (2009:400).

The Data Processor shall restrict access to the Personal Data and only grant permission to personnel who require access to the Personal Data in order to fulfill their obligations under this Data Processor Agreement. Personnel who have access to Personal Data have entered into a particular obligation of confidentiality or have been informed to abide by a duty of confidentiality in accordance with an agreement or law.

Notwithstanding the foregoing, the confidentiality clause of the Main Agreement shall apply to the extent that it contains more far-reaching confidentiality obligations for both Parties compared with this Data Processor Agreement.

3.7 Notification of breach

The Data Processor shall promptly and within 24 hours from the time that the Data Processor becomes aware of it, notify the Data Controller of the occurrence or risk of a Personal Data Breach. Such notification shall include all necessary and accessible information required by the Data Controller in order to be able to take appropriate preventive measures and fulfill their obligations regarding the notification of personal data breaches to the competent regulatory authority.

All such breaches shall be documented by the Data Processor and the documentation shall be delivered without undue delay upon the Data Controller's request.

3.8 Assistance to fulfill obligations towards data subjects

The Data Processor shall assist the Data Controller to fulfill their obligations towards the data subjects when exercising their rights under applicable Data Protection Directives, such as the right to information and records, data portability, the right to be forgotten, rectification and erasure. This shall be done without undue delay and without further financial compensation, unless otherwise agreed between the Parties.

In the event that the data subjects, authority or other third-party request information from the Data Processor regarding the processing of Personal Data, the Data Processor shall forward such a request to the Data Controller without delay. The Data Processor shall assist, where necessary, the Data Controller with gathering the information requested by the data subjects, authority or other third party.

The Data Processor shall maintain a record of all processing of Personal Data, which is performed on behalf of the Data Controller, and provide a legible record of data at the request of the Data Controller or the competent authority, including at least:

(a) name and contact details of the Data Processor and, where applicable, names and contact details of representatives employed by the Data Processor, their data protection representative and, where appropriate, those employed by the Subprocessors,

(b) the processing carried out by the Data Processor on behalf of the Data Controller, the type of personal data and, where applicable, the specific categories,

(c) in this case, the transfer of personal data to a third country, the third country where the data is processed and the appropriate security measures taken, and

(d) a general description of the technical and organizational measures taken to maintain an appropriate level of protection.

3.9 Rectification and deletion of personal data

The Data Processor undertakes to rectify incorrect or incomplete Personal Data without delay, following instructions from the Data Controller.

After the Data Controller has requested the deletion of Personal Data in writing, the Data Processor may process the Personal Data only as part of the deletion process and undertakes to delete the Personal Data without undue delay.

Upon termination of the Data Processor Agreement, the Data Processor and any Subprocessors, as requested by the Data Controller, shall either return all transferred Personal Data and copies thereof to the Data Controller, or destroy all Personal Data (and copies thereof) and testify to the Data Controller that this has been done.

If this is not technically possible, the Data Processor will ensure that it will preserve the confidentiality of the transferred Personal Data, and not further process the transferred Personal Data, or anonymize it in ways that render it impossible to recreate. This should be done within a reasonable period of time, but always within 4 months of termination, and without further financial compensation, unless the Parties agree otherwise.

4 COMPENSATION

4.1 The Data Processor shall keep the Data Controller free from harm in the event that the Data Controller is subject to harm that is attributable to the Data Processor's processing of Personal Data which is in violation of this Data Processor Agreement, applicable legislation or contrary to instructions from the Data Controller.

5 RIGHT TO RENEGOTIATION

5.1 Either Party is entitled to call for a renegotiation of this Data Processor Agreement, including its attachments, in the event that the Data Processor's ownership changes substantially, or an applicable legislation or its interpretation is amended in a way that affects the processing of Personal Data.

5.2 A Party is not entitled to terminate the assignment solely on the grounds that the right of renegotiation has been invoked or a renegotiation has been commenced.

6 TRANSFER

6.1 This Data Processor Agreement may not be transferred without the prior approval of the other Party.

7 TERM OF THE AGREEMENT

7.1 This Data Processor Agreement is valid from the time of signing it and as long as the Data Processor Processes Personal Data on behalf of the Data Controller.

8 DISPUTES AND APPLICABLE LAW

8.1 Disputes arising from the agreement shall be finalized in the state of California, USA.

This Agreement has been drawn up in two (2) identical copies and each of the Parties has taken their copy.

8/27/2020	31 August 2020 | 15:07:11 EDT 8/27/2020
IT Relation	Cira Apps Limited
DPO	DocuSigned by: Vernon L. Weitzman 60A74ADBB0644D8... Vernon Weitzman, President

CIRASYNC

APPENDIX 1

INSTRUCTIONS

These instructions form an integral part of the Data Processor Agreement and shall be followed by the Data Processor in the execution of the Processing of Personal Data, unless expressly stated otherwise in the Data Processor Agreement. By signing this Data Processor Agreement, the Data Processor has confirmed the scope of these instructions. In order to be valid, any changes and additions to these instructions shall be in writing.

Purpose

To facilitate smartphone access to corporate data stored in Microsoft 365 and Azure Active Directory.

Type of Processing

State type of processing:

Contact and Calendar synchronization from a master data source to Mailboxes on Microsoft 365

Type of Personal Data

Phone and email contact information.

Category

CiraSync does not currently process any data that is categorized as "Special category" under GDPR.

Place of Processing

Azure Data Centers located in the European Union.

Duration

From: Thursday, August 27, 2020
To: August 27, 2021

Transfer to a third country

No personal data is transferred, directly or indirectly, to a country/state outside the EU/EEA.

DATA PROTECTION

The Supplier has taken the following technical and organizational measures regarding built-in data protection:

For the CiraSync SaaS platform, additional precautions are taken for data at rest:

- Any instances of customer proprietary data or records will be encrypted and stored only in Azure hosted servers which are managed by Cira Apps Limited.
- Information will be physically stored in an Azure Data Center as close as possible to the primary region of the customers Microsoft 365 tenant.
- A decryption key will be required to read this data. However, the decryption key will be stored in a hidden attribute, stored in a mailbox managed by the customers Microsoft 365 tenant.
- When CiraSync is processing customer data, it will request the decryption key, and use it only in transient and protected memory (such as RAM).
- When the scheduled processing of customer data is complete, both the decrypted data and the decryption key are immediately erased from memory.
- When the customer uses the CiraSync tenant dashboard, (or permits a CiraSync technician to access their dashboard), the decryption key may be persisted in transient memory up to 15 minutes.
- If the hidden attribute or mailbox containing the decryption key is lost, certain types of customer data may be permanently lost.
- If a customer revokes Azure consent to their tenant, all data at rest stored in CiraSync will be orphaned. However, this encrypted data can be safely retained in case the customer chooses to once again grant consent. By default, the encrypted data will be retained for no more than 90 days. However, the customer can request to have it purged at any time.

CIRASYNC

APPENDIX 2

SUBPROCESSORS

The Data Controller has approved the following company as sub processor, provided that the Data Processor concludes a written agreement with the sub processor in accordance with clause 3.4 of this Data Processor Agreement.

Microsoft Corporation
See Online Services Terms
http://www.microsoftvolumelicensing.com/Downloader.aspx?DocumentId=13782

Navigate to "Data Protection Terms"
Subsection: Processing of Personal Data; GDPR

.....