ReVirt

Data Processing Agreement

(version november 9, 2020)

This Data Processing Agreement ("**Agreement**") forms part of the Contract for Services under the Terms and Conditions from the distributor (the "**Principal Agreement**"). This Agreement is an amendment to the Principal Agreement and is effective upon its incorporation to the Principal Agreement, which incorporation may be specified in the Principal Agreement or an executed amendment to the Principal Agreement. Upon its incorporation into the Principal Agreement, this Agreement will form a part of the Principal Agreement.

The term of this Agreement shall follow the term of the Principal Agreement. Terms not defined herein shall have the meaning as set forth in the Principal Agreement.

WHEREAS

(A) Your company act as a Data Controller (the "Controller").

(B) Your company wishes to subcontract certain Services (as defined below), which imply the processing of personal data, to any.cloud a/s, acting as a Data Processor (the "Processor").

(C) The Parties seek to implement a data processing agreement that complies with the requirements of the current legal framework in relation to data processing and with the 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).

(D) The Parties wish to lay down their rights and obligations.

IT IS AGREED AS FOLLOWS:

1. Definitions and Interpretation

1.1
Unless otherwise defined herein, capitalized terms and expressions used in this DPAshall have the following meaning:

• "Company Personal Data" means any Personal Data Processed by a Contracted Processor on Controller's behalf pursuant to or in connection with the Principal Agreement;

• "Contracted Processor" means a Subprocessor;

• "Data Protection Laws" means EU Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other country;

• "EEA" means the European Economic Area;

• EU Data Protection Laws" means EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR;

• "GDPR" means EU General Data Protection Regulation 2016/679;

• "Data Transfer" means:
• a transfer of Company Personal Data from Controller to a Contracted Processor; or
• an onward transfer of Company Personal Data from a Contracted Processor to a Subcontracted Processor, or between two establishments of a Contracted Processor,

in each case, where such transfer would be prohibited by Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection Laws);

• "Services" means online backup of Microsoft 365 data. The Service is described more in detail in Schedule 1.

• "Subprocessor" means any person appointed by or on behalf of Processor to process Personal Data on behalf of Controller in connection with the Agreement.

1.2
The terms, "**Commission**", "**Controller**", "**Data Subject**", "**Member State**", "**Personal Data**", "**Personal Data Breach**", "**Processing**" and "**Supervisory Authority**" shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly.

2. Processing of Company Personal Data

2.1
Processor shall:
• comply with all applicable Data Protection Laws in the Processing of Company Personal Data; and
• not process Company Personal Data other than on Controller's documented instructions.

2.2
Controller instructs Processor to process Company Personal Data to provide the Services and related technical support.

3. Processor Personnel

Processor shall take reasonable steps to ensure the reliability of any employee, agent or contractor of any Contracted Processor who may have access to Company Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know / access the relevant Company Personal Data, as strictly necessary for the purposes of the Principal Agreement, and to comply with Applicable Laws in the context of that individual's duties to the Contracted Processor, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

4. Security

4.1

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, Processor shall in relation to the Company Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR.

4.2
In assessing the appropriate level of security, Processor shall take account in particular of the risks that are presented by Processing, in particular from a Personal Data Breach.

5. Subprocessing

5.1
Processor shall not appoint (or disclose any Company Personal Data to) any Subprocessor unless required or authorized by Controller.

6. Data Subject Rights

6.1
Taking into account the nature of the Processing, Processor shall assist Controller by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of Controller obligations, as reasonably understood by Controller, to respond to requests to exercise Data Subject rights under the Data Protection Laws.

6.2
Processor shall:
• promptly notify Controller if it receives a request from a Data Subject under any Data Protection Law in respect of Company Personal Data; and
• ensure that it does not respond to that request except on the documented instructions of Controller or as required by Applicable Laws to which the Processor is subject, in which case Processor shall to the extent permitted by Applicable Laws inform Controller of that legal requirement before the Contracted Processor responds to the request.

7. Personal Data Breach

7.1
Processor shall notify Controller without undue delay upon Processor becoming aware of a Personal Data Breach affecting Company Personal Data, providing Controller with sufficient information to allow Controller to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.

7.2
Processor shall co-operate with Controller and take reasonable commercial steps as are directed by Controller to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

8. Data Protection Impact Assessment and Prior Consultation

8.1

Processor shall provide reasonable assistance to Controller with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which Controller reasonably considers to be required by article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law, in each case solely in relation to Processing of Company Personal Data by, and taking into account the nature of the Processing and information available to, the Contracted Processors.

9. Deletion or return of Company Personal Data

9.1
Subject to this section 9 Processor shall promptly and in any event within 10 business days of the date of cessation of any Services involving the Processing of Company Personal Data (the "Cessation Date"), delete and procure the deletion of all copies of those Company Personal Data.

9.2
Processor shall provide written certification to Controller that it has fully complied with this section 9 within 10 business days of the Cessation Date.

10. Audit rights

10.1
Subject to this section 10, Processor shall make available to Controller on request all information necessary to demonstrate compliance with this Agreement, and shall allow for and contribute to audits, including inspections, by Controller or an auditor mandated by Controller in relation to the Processing of the Company Personal Data by the Contracted Processors.

10.2
Information and audit rights of Controller only arise under section 10.1 to the extent that the Agreement does not otherwise give them information and audit rights meeting the relevant requirements of Data Protection Law.

11. Data Transfer

11.1
The Processor may not transfer or authorize the transfer of Data to countries outside the EU and/or the European Economic Area (EEA) without the prior written consent of Controller. If personal data processed under this Agreement is transferred from a country within the European Economic Area to a country outside the European Economic Area, the Parties shall ensure that the personal data are adequately protected. To achieve this, the Parties shall, unless agreed otherwise, rely on EU approved standard contractual clauses for the transfer of personal data.

12. General Terms

12.1
Confidentiality. Each Party must keep any information it receives about the other Party and its business in connection with this Agreement ("Confidential Information") confidential and must not use or disclose that Confidential Information without the prior written consent of the other Party except to the extent that:

(a) disclosure is required by law;
(b) the relevant information is already in the public domain.

12.2
Notices. All notices and communications given under this Agreement must be in writing and will be sent by email. Controller shall be notified by email sent to the address related to its use of the Service under the Principal Agreement. Processor shall be notified by email sent to the address: gdpr@revirt.global

13. Governing Law and Jurisdiction

13.1
This Agreement is governed by Danish law.

13.2
Any dispute arising in connection with this Agreement, which the Parties will not be able to resolve amicably, will be submitted to the exclusive jurisdiction of the courts of Denmark.

Schedule 1: Service Description

The Service offered by any.cloud a/s is ReVirt365.

ReVirt365 is an easy-to-use web portal, and from where you can easily connect to your Office 365. When you have connected your Microsoft admin account to ReVirt365 you are now able to do backup your entire organization, or groups, giving you and all other employees a safety net like never before, covering your entire data consortium with Microsoft.

Not only will you be able to manage all backup jobs in a glance – you can also restore any file from the backup if needed. The service is available 24/7 if you need it outside business hours. Your data is safely stored in our private cloud up to 10 years, and you decide if you want a managed solution, partially managed solution or if you want to use the portal entirely on your own. Whichever you choose, you'll be able to restore the data, but when it comes to retention periods, we offer four types of licenses:

Platinum – 10-year retention
Gold – 5-year retention
Silver – 3-year retention
Bronze – 1-year retention

All are designed for a business, which needs to safely store and secure data. With our four options you can select the retention period that suits your company. Microsoft secures the infrastructure uptime, whereas being responsible for the data stays with the customer. We would like to help you with ensuring your data.

Schedule 2: Data Processing and Security

Description of the data processing carried out on behalf of the Controller.

In addition to the information provided elsewhere in the Agreement, the Parties wish to document the following information in relation to the data processing activities.

1. PHYSICAL SECURITY

1.1 Fire, power outages, flooding etc.

Our datacentres are equipped with the technical resources belonging to a state-of-the-art hosting environment. Both the equipment and the procedures in our datacentres are under constant evaluation by internal and external experts.

The cooling systems in each of the rooms are redundant which ensures sure that any arbitrary component may break down without it impacting the temperature in the datacentre significantly. All air is cooled to approx. 22 degrees centigrade.

Our datacentre is protected by a sniffer system which ensures a fast alarming procedure and activation of the inergen facility, so a local fire in a server does not spread to other equipment.

All any.cloud datacentres are tier 4 classified and SOC 2 certified and follow all applicable requirements.

All electrical installations are supplied by 2 independent sources, which means even if source 1 may suffer a breakdown, source 2 ensures that all equipment is still running. In case of power outages, UPS will be the first to take over followed by diesel generators, thereby ensuring a stable power supply. The diesel generators guarantee a minimum of 24 hours of operation on one tank. For longer power outages, an agreement has been made with fuel company re. further delivery of fuel.

All electrical installations are considered redundant due to the main supply, the UPS and the diesel generators each being redundant from one another.

1.2 Access control

Only authorised personnel have access to our systems. Each person accessing our systems is logged via access cards, iris scans or fingerprint scans. An agreement has been made between Datacenter owners and any.cloud, so only selected employees can apply for extraordinary access for new employees.

2. TECHNICAL SECURITY

2.1 Firewalls and antivirus

any.cloud networks have been segmented in order to keep data separate. This is handled by the Operations Department of any.cloud.

All networks have been segmented in such a way that client use is separated from internal use. The networks for internal use are furthermore segmented into more networks to avoid security incidents, if a service is down. This is handled by the Operations Department, and any.cloud CTO is responsible for compliance with any.cloud security policy.

Authorised members of staff have remote access to any.cloud systems. Access to any.cloud systems is only possible through either MAC address limited networks or through any.cloud SSL VPN. A guest network has been established for externals visiting our offices.

Due to malware having significant impact on the availability of systems and services, any.cloud has set up efficient malware protection.

Every any.cloud server has antivirus protection. Only select members of staff with admin access can remove that software from the systems. All incoming email traffic is scanned for malicious content which is then removed. According to any.cloud SLA (service level agreement), customer data requires full protection on servers rented by any.cloud.

We have implemented scan and surveillance systems to safeguard us from known and malicious code, i.a. anything we and our customers may pick up from the internet or via emails etc. We have antivirus systems as well as systems for monitoring use of the internet, traffic and resources on the SaaS platforms, as well as security warning in other technical and central installations (firewall etc.)

2.2 Encryption

Data traffic containing confidential or sensitive information via public networks is always encrypted.

The use of unauthorised and unsafe data media is not permitted for exchanging data or storing data containing confidential or sensitive information.

2.3 Backup and restore

any.cloud infrastructure team is responsible for backup and restore with a minimum retention of 1 day, in case a restore is required. In order to make sure that the restored data is working correctly, a restore procedure is performed at least quarterly. To keep backed up data from being accessed by unauthorised personnel, access controls are inserted, so only the infrastructure team has access.

During backup and restore, a log is kept, documenting the backed up elements. The employee controlling the process is responsible for both documenting and filing the incident correctly in the any.cloud ticket system.

2.4 Redundant operation

All equipment is, as a minimum, in a cluster and is run, as a minimum in an active-passive setup. This helps ensure that the operation remains intact in case of service windows, breakdowns or other such incidents.

3. ORGANISATIONAL SAFETY

3.1 Access rights

All passwords to internal systems are individual and personal and, where possible, there is always personal admin access to systems.

Mobile equipment constitutes computers, smartphones, tablets and other such devices. Mobile equipment with access to any.cloud network or assests must always be locked and comply with the standards for IT security described in this document. VPNs are always used where access via public networks applies. "Jailbreaked” mobile equipment, or equipment that in other way is not working via its original operating system is not permitted and will be denied access.

any.cloud logs successful as well as unsuccessful attempts at access. any.cloud reserves the right to scrutinise such attempts in case we suspect neglect.

3.2 Confidentiality

The infrastructure team of any.cloud is responsible for our operations and secures that our operational activities are performed in a stable, qualified and secure manner, keeping confidentiality, reliability and availability concerns safe. Planned service work is primarily performed outside of regular working hours and always in a manner that causes the least possible disturbance to the customers. All members of any.cloud staff with access to confidential information have signed a confidentiality clause.

3.3 Logging

The infrastructure team of any.cloud ensures that surveillance is made of both networks and other IT equipment. It happens via an automated surveillance where we secure that follow-up is made to errors, problems or safety issues that may require scrutiny or follow-up. Incidents are logged automatically in our ticket system.

4. ERASURE AND DESTRUCTION

All data carrying equipment is destroyed prior to disposal in order to secure that no data is accessible from a device. This happens through a cooperation with a 3rd party business partner where destruction happens via a certified procedure and always includes a certificate confirming the destruction.

When an employee leaves any.cloud, comprehensive procedures state how to ensure that an employee hands over all relevant assets, including mobile media etc., as well as they ensure that employee access to buildings, systems and data is revoked. The overall responsibility for keeping all control measures during the termination period of an employee lies with any.cloud CTO.