Data Processing Agreement
for Arrow Cloud Backup for 365 (ACB365)

Provided by Anycloud A/S

(version January 1st, 2023)

You agree that this Data Processing Agreement ("DPA") sets forth the obligations with respect to the data processing activities performed with Anycloud's offering of ACB365. You agree that the DPA governs the processing and security of all personal data which is stored and processed through the ACB365 platform.

ACB365 is a generic product and all services offered is provided by Anycloud to all users of ACB365. Anycloud makes the commitments in this DPA to all customers with licenses to ACB365. These commitments are binding on Anycloud for Anycloud's handling of customer data and provides instructions for Anycloud for processing of personal data.

The DPA is an integrated part of the General Terms and conditions which must be concluded to access ACB365, and when accepting the General Terms and conditions, you have also accepted the DPA and its terms and conditions. In the event of any conflict or inconsistency between this DPA and any other terms in the Agreement, this DPA shall prevail. The provisions of this DPA supersede any conflicting provisions of Anycloud's Privacy Statements.

To access ACB365 portals, you must confirm when you check the box, that you have read and accepted this DPA with your purchase of a license to ACB365.

You represent to us that you are lawfully able to enter into this DPA, and if you are entering into the DPA on behalf of a company or other legal entity, you represent that you have the authority to bind such entity to the DPA, and the terms "you" shall refer to such entity. If you do not have such authority, or if you do not agree with the terms and conditions of the DPA, you must not accept this DPA, and you therefor may not use ACB365.

When you renew or purchase a new subscription for licenses to ACB365, the thencurrent DPA will apply.

If you for purpose of the data processing activities in ACB365 requires any further action to protect personal data, you must contact Anycloud to agree on additional actions. All such actions must be agreed in a written as supplements to this DPA before Anycloud can submit and adhere to such actions.

Data Processing Terms

For the purposes of Article 28(3) of Regulation 2016/679 (the GDPR)

Between you (the data controller), and

Anycloud A/S, a company duly organised and existing under the laws of Denmark with reg.no DK31161509, having its registered address at

Anycloud A/S
Hedegaardsvej 88
DK-2300 Copenhagen S
Denmark
(the data processor)

each a 'party'; together 'the parties'

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to meet the requirements of the GDPR and to ensure the protection of the rights of the data subject.

1. Table of Contents

2. Preamble

1. These Contractual Clauses (the Clauses) set out the rights and obligations of the data controller and the data processor, when processing personal data on behalf of the data controller.

2. The Clauses have been designed to ensure the parties' compliance with Article 28(3) of Regulation 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).

3. In the context of the provision of access to server management services offered by the data processor as ACB365 for backup storage, restoring, and other management activities of data from customers' Microsoft 365 environment, the data processor will process personal data on behalf of the data controller in accordance with the Clauses.

4. The Clauses shall take priority over any similar provisions contained in other agreements between the parties.

5. Four appendices are attached to the Clauses and form an integral part of the Clauses.

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 the data controller's conditions for the data processor's use of sub-processors and a list of sub-processors authorised by the data controller.

8. Appendix C contains the data controller's instructions with regards to the processing of personal data, the minimum security measures to be implemented by the data processor and how audits of the data processor and any sub-processors are to be performed.

9. The Clauses along with appendices shall be retained in writing, including electronically, by both parties.

10. The Clauses shall not exempt the data processor from obligations to which the data processor is subject pursuant to the General Data Protection Regulation (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[1] data protection provisions and the Clauses.

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

[1] References to "Member States" made throughout the Clauses shall be understood as references to "EEA Member States".

3. The data controller shall be responsible, among other, 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 documented instructions from the data controller, unless required to do so by Union or Member State law to which the processor is subject. Such instructions shall be specified in appendices A and C. 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 the Clauses.

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 organisational 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. Pseudonymisation 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 organisational measures for ensuring the security of the processing.

2. According to Article 32 GDPR, 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 organisational 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 in Appendix C.

7. Use of sub-processors

1. The data processor shall meet the requirements specified in Article 28(2) and (4) GDPR in order to engage another processor (a sub-processor).

2. The data processor shall therefore not engage another processor (sub-processor) for the fulfilment of the Clauses without the prior written general authorisation of the data controller.

3. The data processor has the data controller's general authorisation for the engagement of sub-processors. The data processor shall inform in writing the data controller of any intended changes concerning the addition or replacement of sub-processors at least 30 days in advance, thereby giving the data controller the opportunity to object to such changes prior to the engagement of the concerned sub-processor(s). Longer time periods of prior notice for specific sub-processing services can be provided in Appendix B. The list of sub-processors already authorised by the data controller can be found in Appendix B.

4. Where the data processor engages a sub-processor for carrying out specific processing activities on behalf of the data controller, the same data protection obligations as set out in the Clauses shall be imposed on that sub-processor by way of a contract or other legal act under EU or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the Clauses and the GDPR.

   The data processor shall therefore be responsible for requiring that the sub-processor at least complies with the obligations to which the data processor is subject pursuant to the Clauses and the GDPR.

5. A copy of such a sub-processor agreement and subsequent amendments shall – at the data controller's request – be submitted to the data controller, thereby giving the data controller the opportunity to ensure that the same data protection obligations as set out in the Clauses are imposed on the sub-processor. Clauses on business related issues that do not affect the legal data protection content of the sub-processor agreement, shall not require submission to the data controller.

6. The data processor shall agree a third-party beneficiary clause with the sub-processor where – in the event of bankruptcy of the data processor – the data controller shall be a third-party beneficiary to the sub-processor agreement and shall have the right to enforce the agreement against the sub-processor engaged by the data processor, e.g. enabling the data controller to instruct the sub-processor to delete or return the personal data.

7. If the sub-processor does not fulfil his data protection obligations, the data processor shall remain fully liable to the data controller as regards the fulfilment of the obligations of the sub-processor. This does not affect the rights of the data subjects under the GDPR – in particular those foreseen in Articles 79 and 82 GDPR – against the data controller and the data processor, including the sub-processor.

8. Transfer of data to third countries or international organisations

1. Any transfer of personal data to third countries or international organisations 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 organisations, 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 the Clauses:

    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 C.5.

5. The Clauses shall not be confused with standard data protection clauses within the meaning of Article 46(2)(c) and (d) GDPR, and the Clauses 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 organisational 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 C the appropriate technical and organisational 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 72 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 C 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 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, no later than 30 days after termination, and 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 the Clauses 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 Appendix C to this Data Processing Agreement.

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 the Clauses or prejudice the fundamental rights or freedoms of the data subject and the protection afforded by the GDPR.

14. Commencement and termination

1. The Clauses shall become effective on the date of acceptance of this document in the web-portal.

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

3. The Clauses shall apply for the duration of the provision of personal data processing services. For the duration of the provision of personal data processing services, the Clauses 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 C.4., the Clauses may be terminated by written notice by either party.

5. Only If requested Anycloud will supply a signed copy of this agreement

15. Data controller and data processor contacts/contact points

1. The data controller may contact Anycloud in relation to this agreement using the following contact point:

Name	Adrian Frimodt-Møller
Telephone	+45 70 20 40 67
E-mail	gdpr@anycloud.dk

2. The parties shall be under obligation continuously to inform each other of changes to contacts/contact points.

Appendix A Information about the processing

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

The data controller and the data processor have entered into an Agreement pursuant to which the data controller is granted a license to access and use the ACB365 services for the duration of the subscription period. In providing the service, the data processor will engage, on behalf of the data controller, in the processing of personal data submitted and stored within the service by the data controller or persons authorised by the data controller.

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 data processor will host and process personal data in the course of providing its management facilities and services offered with ACB365

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

The data processer will process personal data to mirror the data collected and stored in the data controller's Microsoft 365 Environment.

The data will include general personal data which the data controller has stored in its Microsoft 365 Environment such as:

- Names of persons
- Job titles
- Email addresses
- Identification numbers
- Competencies
- Human Resource data on employees

The data may include sensitive personal data which the data controller has stored in its Microsoft 365 environment including for purpose of human resource management such as:

- Health data
- ETC

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

The data processor will offer server storage facilities to all personal data included in the data controller's Microsoft 365 Environment which may include personal data about the following categories of data subjects:

- Employees
- Consultants
- Customer contacts

- Vendor contacts
- Other data controller contacts
- Other data subjects data recorded by the data controller .

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

The processing activities continues for the duration of the subscription. When the subscription expires or is terminated, the data processor will process data only for purpose of concluding the services.

Appendix B Authorised sub-processors

B.1. Approved sub-processors

On commencement of the Clauses, the data controller authorises the engagement of the following sub-processors:

NAME	REG NO	ADDRESS	DESCRIPTION OF PROCESSING
IBM	DK65305216	Prøvensvej 1 2605 Brøndby Denmark	Data Storage
any.cloud a/s	DK31161509	Hedegaardsvej 88 2300 Copenhagen S Denmark	Service provider for Arrow ECS and Data storage

The data controller shall on the commencement of the Clauses authorise the use of the abovementioned sub-processors for the processing described for that party. The data processor shall not be entitled – without the data controller's explicit written authorisation – to engage a sub-processor for a 'different' processing than the one which has been agreed upon or have another sub-processor perform the described processing.

Appendix C Instruction pertaining to the use of personal data

C.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 activities:

The data processor will make server facilities and web portals available for the data controller. The data controller elects the country to host the data among the options provided by the data processor.

The data controller will manage its data using the webportal provided by the data processor. The data processor is instructed to access the data stored in the servers for the following purposes and processing activities:

- Backup and restore of Microsoft 365 data
- Support when requested by customer.

C.2. Security of processing

The data processing involves a large volume of personal data which are subject to Article 9 GDPR on "special categories of personal data" which is why a high level of security is established.

All datacentres are at least tier 3 classified and either SOC 2 or ISO27001 certified and follow all applicable requirements.

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 Datacentre owners and Anycloud, so only selected employees can apply for extraordinary access for new employees.

Authorised members of staff have remote access to Anycloud systems. Access to Anycloud systems is only possible through either MAC address limited networks or through Anycloud SSL VPN

Data traffic 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.

Anycloud 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 Anycloud ticket system.

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.

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

C.3. Storage period/erasure procedures

Personal data is stored for 1, 3, 5, 10 or 25 years the customer selects in the portal 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 delete the personal data in accordance with Clause 11.1.

C.4. Processing location

Processing of the personal data under the Clauses cannot be performed at other locations than the following without the data controller's prior written authorisation:

Anycloud offers the following data locations which is selected by the Customer.
Australia, Brazil, Canada, Denmark (by invitation only), France, Germany, India, Italy, Japan, Mexico, Netherlands, Singapore, South Korea, United Kingdom and United States.

All locations are hosted in IBM Cloud Datacentres with the exception of Denmark that is hosted by Anycloud.

C.5. Instruction on the transfer of personal data to third countries

The data processor shall and will not transfer personal data out of the Member States unless Customer specifically has chosen a data location outside of this area themselves.
In the case the Customer has selected a location outside the Member States we refer to the EU Commision's Standard Contractual Clauses (SCC). Information regarding this can be found following this link:
https://link.anycloud.dk/SCC

C.6. Procedures for the data controller's audits, including inspections, of the processing of personal data being performed by the data processor

There is not agreed any Procedures for the Data Controller's inspection of the processing being performed by the Data Processor.