# Data Processing Agreement

Standard Contract Terms

In accordance with Article 28 (3) of Regulation (EU) 2016/679 (General Data Protection Regulation, GDPR) regarding the Data Processor's processing of personal data.

Between

The customer (as defined in the agreement document).

hereinafter referred to as **(the) Data Controller**

and

RSM Danmark Statsautoriseret Revisionspartnerselskab
Thyparken 10
7700 Thisted
Company registration no. 25492145

hereinafter referred to as **(the) Data Processor**

Each is referred to individually as a “Party” and collectively as “the Parties”.
The Parties’ respective contact persons are listed in the main agreement/agreement document signed by both Parties.

The Parties have agreed to the provisions of the following Data Processing Agreement (DPA) with a view to compliance with the GDPR and protecting the privacy and rights and freedoms of natural persons.

Table of Contents

1. **Contents**

## 2. Preamble

1. The provisions of this DPA set out the rights and undertakings that apply when the Data Processor processes personal data on behalf of the Data Controller.
2. The provisions of this DPA are based on compliance by the Parties with Article 28 (3) 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, GDPR), which sets out specific requirements for the content of a Data Processor Agreement.
3. In connection with delivery of the agreed services described in Appendix D, the Data Processor processes personal data on behalf of the Data Controller in accordance with the provisions of this DPA.
4. The provisions of this DPA take precedence in relation to any corresponding provisions in other agreements between the Parties.
5. There are four appendices to the DPA, each of which constitutes an integral part of the agreement.
6. Appendix A contains detailed information about the processing of personal data, including the purpose and character of processing, types of personal data, categories of data subjects and duration of processing.
7. Appendix B contains the terms and conditions stipulated by the Data Controller for the Data Processors use of Sub-processors and a list of Sub-processors, whose use the Data Controller has approved.
8. Appendix C contains the Data Controller's instructions with regard to the Data Processor's processing of personal data, a description of the minimum of security measures that the Data Processor shall implement and how the Data Processor's and Sub-processors' (if any) activities shall be audited.
9. Appendix D contains provisions regarding other activities that are not subject to the provisions of the DPA.
10. Both Parties shall store the DPA and its associated appendices in writing, including by electronic means.
11. The provisions of the DPA do not relieve the Data Processor of any obligations the Data Processor may be subject to in pursuance of the GDPR and any other legal act.

## 3. The Data Controller's rights and obligations

1. The Data Controller is responsible for ensuring that personal data are processed in accordance with the GDPR (see Article 24 of the regulation) and data protection provisions in Union or Member State/EEA State law and in the present DPA.
2. The Data Controller is both entitled and obliged to determine to which purpose or purposes, and by which means personal data shall be processed.
3. Among other responsibilities, the Data Controller shall ensure that there is good reason to process the personal data that the Data Processor is instructed to process.

## 4. The Data Processor shall act on instructions

1. The Data Processor may only process personal data on the Data Controller's documented instructions, unless required to do so by Union or Member State/EEA State law. The Data Controller's instructions are specified collectively in Appendices A, C and D. Subsequent instructions can also be given by the Data Controller whilst personal data is being processed, but shall always be documented and stored in writing, including electronically along with the DPA.

2. The Data Processor shall notify the Data Controller without delay if it believes that an instruction given contravenes the GDPR or data protection provisions contained in other EU or Member State law.

## 5. Duty of Confidentiality

1. The Data Processor may only provide access to personal data processed on the Data Controller's behalf to personnel who are subject to the Data Processor's instructions and provisions and have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality, although only to the extent that this is necessary. The list of personnel who have such access shall be evaluated at regular intervals. Based on an evaluation, access to personal data may be denied if access is no longer necessary and the person(s) in question no longer need to have access to it.
2. Upon request from the Data Controller, the Data Processor shall be able to prove that the relevant personnel are subject to the above duty of confidentiality.

## 6. Security of processing

1. Article 32 of the GDPR stipulates that, in consideration of the current technical level, implementation costs and the nature, scope, context and purposes of processing and the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Data Controller and the 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 risk presented by processing to the rights and freedoms of natural persons and implement measures to mitigate these risks. Depending on their relevance, such measures can include:

   a. the pseudonymisation and encryption of personal data;
   b. the ability to ensure the 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 of GDPR, the Data Processor – acting independently of the Data Controller – shall also evaluate the risk presented by processing to the rights and freedoms of natural persons and implement measures to gate such risks. With a view to making this evaluation, the Data Controller is obliged to place information at the Data Processor's disposal to allow to the Data Processor to identify and evaluate the risks involved.
3. Moreover, the Data Processor shall assist the Data Controller in meeting the latter's obligations pursuant to Article 32 of the GDPR, including, among other ways, providing the Data Controller with information about the technical and organisational security measures that Data Controller has already implemented in compliance with Article 32 and any other information that may be necessary for the Data Controller to meet its obligations in pursuance of Article 32 of the GDPR.

   If the Data Controller evaluates that mitigating the risks thus identified requires the implementation of further measures than those the Data Processor has already implemented, the Data Controller shall note the additional measures that shall be implemented in Appendix C.

## 7. Use of Data Sub-processors

1. The Data Processor shall fulfil the conditions referred to in Article 28 (2) and (4) of the GDPR for engaging another processor (Sub-Processor).
2. As such, the Data Processor shall not use another Data Sub-Processor for fulfilment of the DPA without the prior general written consent of the Data Controller.
3. The Data Processor has the Data Controller's general consent to use Sub-processors. The Data Processor shall notify the Data Controller in writing of any planned changes in connection with adding new or replacing Data Sub-processors giving at least 30 days' notice and therefore allowing the Data Controller the opportunity to object to such changes before the aforementioned Data Sub-processors are brought into use  A longer period of notification in connection with specific data processing activities may be given in Appendix B. Appendix B includes a list of Data Sub-processors that the Data Controller has already authorised.
4. Where the Data Processor engages a Data Sub-processor to carry out specific processing activities on behalf of the Data Controller, the same data protection obligations as set out in the DPA or other legal act between the Data Controller and the Data Processor shall be imposed on the Sub-processor by way of a contract or other legal act under Union 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 this DPA and the GDPR.
   The Data Processor is therefore responsible for requiring that the Data Sub-processor at least meets the obligations imposed on it via the provisions of the DPA and the GDPR.

5. On receipt of a request from the Data Controller to this effect, the Data Sub-processor(s) and subsequent changes to their number shall be submitted in copy to the Data Controller to allow it the chance to ensure that Data Sub-processors are subject to corresponding data protection obligations in pursuance of these provisions. There is no need to submit to the Data Controller any provisions regarding commercial arrangements that have no impact on data protection-related content of the Sub-processor agreement.

6. Where a Sub-processor fails to fulfil its data protection obligations, the Data Processor shall remain fully liable to the Data Controller for the performance of the Sub-processor's obligations. This provision shall apply without prejudice to the data subject's rights arising from the GDPR, in particular from Articles 79 and 82 of the Regulation, to claim against the Data Controller and Data Processor, including the Data Sub-processor.

## 8. Transfer of personal data to third countries or international organisations

1. With regard to transfers of personal data to a third country or an international organisation, the Data Processor may act only on documented instructions from the Data Controller and always in compliance with Chapter V of the GDPR.
2. Should transfers of personal data to a third country or an international organisation, for the performance of which the Data Processor has not received instructions from the Data Controller and that are required by Union or Member State law to which the Data Processor is subject, the Data Processor shall notify the Data Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.
3. This DPA stipulates therefore that, in the absence of documented instructions from the Data Controller, the Data Processor may not:
    a. transfer personal data to a Data Controller or Data Processor in a third country or an international organisation
    b. assign the processing of personal data to a Data Sub-processor in a third country

c. process personal data in a third country

4. The Data Controller's instructions regarding the transfer of personal data to a third country, including the legal basis for processing transfers as laid down in Chapter V of the GDPR on which the transfer is based, shall be stated in Appendix C.6.
5. These instructions shall be regarded as distinct from standard contractual provisions laid down in Article 46 (2) c and d of the GDPR and may not constitute the legal grounds for the transfer of personal data laid down in Chapter V of the GDPR.

## 9. Assistance for the Data Controller

1. The Data Processor shall assist the Data Controller taking into account the nature of the processing using appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Data Controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of the GDPR.
   This means that the Data Processor shall where possible, assist the Data Controller in connection with the Data Controller's obligation to fulfil the following requirements of the GDPR:

   a. information to be provided where personal data are collected from the data subject
   b. information to be provided where personal data have not been obtained from the data subject
   c. right to access
   d. right to correct
   e. right to erasure ('right to be forgotten')
   f. right to restriction of processing
   g. notification obligation regarding rectification or erasure of personal data or restriction of processing
   h. right to data portability
   i. right to object
   j. right to request not to be the object of a decision based solely on automatic processing, including profiling.
2. In addition to the Data Processor's obligation to assist the Data Controller in accordance with Provision 6.3, taking into account the nature of the processing, the Data Processor shall also assist the Data Controller under the following circumstances:
   a. In the event of a personal data breach, the Data Controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to Datatilsynet (The Danish Data Protection Agency), unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons
   b. When the Data Controller has an obligation to communicate to the data subject a personal data breach, without undue delay, where that personal data breach is likely to result in a high risk to the rights and freedoms of the natural person
   c. When the Data Controller has an obligation, prior to the processing, to assess the impact of the envisaged processing operations on the protection of personal data
   d. When the Data Controller has an obligation to consult the 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 that risk.
3. The Parties shall list in Appendix C the necessary technical and organisational measures with which the Data Processor shall assist the Data Controller and to what extent. This applies to the obligations laid down in items 9.1 and 9.2 of this DPA.

## 10. Reporting breaches of personal data security

1. The Data Processor shall notify the Data Controller without undue delay after becoming aware of a personal data breach.
2. The Data Processor shall report to the Data Controller, if possible, within 24 hours of becoming aware of a breach, such that the Data Controller can fulfil any undertaking it may have to report the breach to a supervisory authority within 72 hours (cf. Article 33 of the GDPR).
3. The Data Processor shall assist the Data Controller in reporting the breach to the correct supervisory authority. This means that the Data Processor shall assist by providing the information listed below that, in accordance with Article 33 (3), shall be included in the Data Controller's notification of a personal data breach to the appropriate supervisory authority.
    a. describe the nature of the personal data breach including, where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of personal data records concerned
    b. describe the likely consequences of the personal data breach
    c. describe the measures taken or proposed to be taken by the Data Controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.
4. The Parties shall list in Appendix D the information that the Data Processor shall provide in connection with assisting the Data Controller in pursuit of his obligation to report a data security breach to the supervisory authority.

## 11. Erasure and return of data

1. In the event of the cessation of personal data processing services, the Data Processor shall erase all personal data processed on behalf of and confirm to the Data Controller that they are erased, unless Union or Member State law prescribes retention of the personal data.

    The Data Processor is obliged solely to process personal data for the purpose(s), in the period and under the terms and conditions prescribed by these rules.

## 12. Audits & inspections

1. The Data Processor shall make available to the Data Controller all information necessary to demonstrate compliance with the undertakings set out in Article 28 of the GDPR and this DPA, and allow for and contribute to audits, including inspections, conducted by the Data Controller or another auditor mandated by the Data Controller.
2. Procedures for the Data Controller's audits, including inspections, with the Data Processor and Sub-processors are listed Appendix C (C.7 and C.8).
3. The Data Processor shall give access to its physical facilities upon presentation of the appropriate legitimation to supervisory authorities given access by law to facilities of the Data Controller or Data Processor, or to representatives acting on behalf of the inspection authority.

## 13. The Parties' agreement on other provisions

1. The Parties may negotiate other provisions with regard to providing a personal data processing service, regarding e.g. liability, as long as these other provisions neither contravene directly or indirectly the provisions of this DPA nor compromise the basic rights and freedoms of the data subject as a result of the GDPR.

## 14. Date effective and termination

1. The provisions of the DPA are effective from the date on which both Parties have signed the agreement document.

2. Either Party may request renegotiation of the provisions, if changes in the law or anything inappropriate in the Agreement gives reason for doing so.

3. The provisions are effective for as long as the personal data processing service remains in operation. During this period, the provisions are irrevocable, unless the Parties agree to other provisions regulating the supply of personal data processing services.

4. If the supply of personal data processing services ceases and the personal data are erased or returned to the Data Controller in accordance with item 11.1 and Appendix C.4, either Party can give written notice of termination of the DPA in its entirety.

5. Signatures
   With their signatures on the agreement document, the Parties agree to the present Data Processor Agreement.

6. Contact persons:
   The Parties may contact each other via the contact details stated in the agreement document.

## Appendix A Information about data processing

**A.1. Purpose of the Data Processor's processing personal data on the Data Controller's behalf**

| Type of person | Purpose |
|---|---|
| Customers | Assist the Data Controller with invoicing work done or goods delivered, registration of payments from their customers and recovery of receivables |
| Employees | Assist the Data Controller with payroll administration, including processing employees' wage slips, reporting to Skattestyrelsen (The Danish Tax Agency), applying for refunds and other personnel administration matters. |
| Suppliers | Assist the Data Controller with the registration of purchased goods or services, processing of proposals for payment based on approved invoices and settlement of debts due to suppliers. |

**A.2. The Data Processor's processing of personal data on behalf of the Data Controller is primarily a matter of the services described in Appendix D or in the main agreement (character of processing)**

**A.3. Processing comprises the following types of personal data concerning the data subjects**

**Non-sensitive personal data** (name, e-mail address, phone number, address, etc.)

**Sensitive personal data** (personal ID number, significant social difficulties)

**Sensitive and special categories of personal data** (trade union membership, data concerning health, political opinions, ethnic origin, religious beliefs, data concerning a natural person's sexual orientation, criminal convictions and legal offences (special personal data)

**A.4. Processing comprises the following categories of data subjects**

| Data subject category | Description |
|---|---|
| Customers | Persons who are or have been customers/members/client/patients of the Data Controller. |
| Employees | Persons who are or have been employees of the Data Controller |
| Suppliers | Persons who are or have been business associates of the Data Controller, including suppliers and business partners. |

**A.5. The Data Processor's processing of personal data on behalf of the Data Controller may commence once the DPA comes into force. Processing may continue for as long as stated in Appendix D or main agreement.**

## Appendix B Data Sub-processors

### B.1. Approved Data Sub-processors

The following is a list of the Data Sub-processors used by the Data Processor.

| Supplier | Country | Legal basis for data processing outside the EU | Function |
|---|---|---|---|
| Uniconta A/S | Denmark | n/a | Accounting |
| Visma e-conomic A/S | Denmark | n/a | Accounting |
| Visma Bluegarden A/S (Dataløn) | Denmark | n/a | Payroll administration |
| Unik System Design A/S (Unik Bolig) | Denmark | n/a | Real estate administration and accounting |
| MS D365 (Business Central) | USA | EU's SCC, EU-US Data Privacy Framework (DPF) | Accounting |

When the DPA came into force, the Data Controller authorised the use of the above-mentioned Data Sub-processors for the processing activity stated. The Data Processor may not without the prior written consent of the Data Controller make use of a Data Sub-processor for a processing activity other than that described and agreed or make use of another Data Sub-processor for the activity in question.

## Appendix C Instructions regarding the processing of sensitive personal data

### C.1. Processing instructions

The Data Processor undertakes the processing of personal data on behalf of the Data Controller such that the Data Processor conducts the processing as described in the agreement document/main agreement or in Appendix D.

### C.2. Security of processing

The following data security measures are implemented:

High-level security measures shall always be implemented in connection with the processing of confidential, sensitive and special types of personal data.

Technical security measures (external):

- SSL-encrypted connections between client and server
- Two-factor validation for external login
- Passwords stored in encrypted form
- Passwords changed at regular intervals
- Continuous back-up and logging
- The Data Sub-processors are in the EU or USA (all have legal grounds for processing).

Technical security measures (internal):

- Up-to-date antivirus software on all devices that may receive personal data
- Up-to-date firewall protection on devices that may receive personal data and servers/operation centres that may store personal data
- Passwords changed at regular intervals
- Continuous upgrading of operative systems and applications
- Continuous back-up and logging
- In connection with transfers of confidential, sensitive and special types of personal data, encryption is applied.

Organisational security measures:

- All employees have received personal data protection training and have signed the employee instructions.
    - Employee instructions are updated and reviewed at least once a year
    - Every new employee receives the employee instructions
- All employees have a duty of confidentiality.
- The Data Processor's executive management, typically represented by the IT Manager, is ultimately responsible for compliance with IT data security requirements.

- Personal data is only accessible to employees who are authorised and have good reason to access them. The data shall always be processed as confidential information.
    - The employee declaration includes a provision that permits access only to cases/data that the employee in question has good reason to access
- In case of large volumes of sensitive personal data, the data should, where possible, be separated to ensure that access to them is restricted to the absolute minimum.

Physical security measures:

- Offices and other buildings are locked when unoccupied and protected by an alarm system.
- Measures are implemented to ensure that the company continues to operate during a power cut and a breakdown in channels of communication.
- Sensitive personal data is always stored in a locked facility protected by an alarm system.
- All physical media (paper, USB flash drives, etc.) are disposed of responsibly if they have been used to store personal data.

Operational security

- Capacity is continuously adapted and monitored to maintain stable operations.
- Failed login-in attempts are logged.

**C.3 Assistance for the Data Controller**
The Data Processor shall assist the Data Controller, insofar as this is possible, in accordance with items 9.1 and 9.2 by implementing the technical and organisational measures stated in Appendix C.2.

**C.4 Data storage period/erasure routine**
Personal data shall be stored on the Data Processor's premises until such time as the Data Controller requests to have the data deleted or returned, unless otherwise agreed in Appendix D/the main agreement or in special circumstances.

In the event of the cessation of personal data processing services, the Data Processor shall either erase or return the personal data in accordance with item11.1, unless, after signing this DPA, the Data Controller has amended its original choice. Such amendments shall be documented and stored in writing and electronically alongside the DPA.

**C.5 Data processing location**
The processing of data that are subject to the provisions of the DPA may not be performed at locations other than the Data Processor's and Sub-processor's premises, except with the Data Controller's prior written consent.

### C.6 Instructions regarding the transfer of personal data to a third country

The Data Processor shall not transfer personal data to a third country, with exception of the generally authorised Data Sub-processors listed in Appendix B.

If, in this DPA or subsequently, the Data Controller has not issued documented instructions regarding the transfer of personal data to a third country, the Data Processor is not entitled within the bounds of the DPA to make any such transfer.

### C.7 Procedures for Data Controller audits & inspections including personal data processing that is delegated to the Data Processor

The Data Controller or its representative shall conduct as needed an inspection of facilities at which the Data Processor processes personal data, including physical facilities and systems used or associated with data processing, with a view to establishing the extent to which the Data Processor complies with the GDPR and data protection provisions elsewhere in Union and Member State law and this DPA.

The Data Controller's expenses (if any) incurred in connection with a physical inspection shall be met by the Data Controller itself. However, the Data Processor is obliged to allocate resources (primarily time) necessary for the Data Controller to conduct its inspection.

### C.8 Audit & inspection procedures including personal data processing that is delegated to the Data Processor

The Data Processor's audits, including inspections, of the processing of personal data that are delegated to a Data Sub-processor shall be conducted in the same way as the Data Controller's audits on the Data Processor's premises.

## Appendix D. The Parties' regulation of other provisions, including instructions regarding personal data processing

See the agreement document/main agreement between the Parties.

Breach of personal data security:
In the event of a breach of personal data security, the Data Processor shall enclose documentation for the actual circumstances of the breach, its impact and remedial measures implemented. Moreover, if the Data Processor is authorised to notify data subjects of a breach, the Data Processor shall inform the Data Controller that the data subjects have been notified and how.