Data Processing Agreement

ADDENDEM TO VALID SERVICE AGREEMENT

Between

Company Name _____

Company Registration no. _____

("The Controller")

And

RINA Digital Solutions

CVR no. 32670334

("The Processor")

(together "The Parties")

03-11-2022

SERTICA BY RINA

All Rights Reserved

Classification and Approval

Classification:
Confidential

Status:
Final

Publisher:
RINA Digital Solutions
Sofiendalsvej 5B
9200 Aalborg SV
Denmark

Content

1 The objective 4

2 Processing of personal data....4

3 Instruction 5

4 Processing a request from a registered person 6

5 Geographical requirements....6

6 Precautionary measures....6

7 Utilisation of sub processors 7

8 Security breach 8

9 Termination of the agreement 8

10 Changes to the agreement 9

11 Governing law....9

12 Signatures....9

1 The objective

1.1 The controller is an organization using Sertica.

1.2 The processor is a software company, developing, selling and servicing Sertica.

1.3 In the context of the Parties' license- and service agreement regarding delivery of Sertica theprocessor undertakes processing of personal data, that the controller is accountable for. As aresult, the processor processes personal data on behalf of the controller.

1.4 The processor and the controller have concluded this Data Processing Agreement ("The Agreement") to describe the terms of the processor's role and the processing and the personal data that the processor is entrusted. Additionally, the precautionary measures, thatthe processor has taken to protect the controller's data against erasure or improper utilization are described. The objective with the agreement is to ensure that the processor acts according to instructions from the controller regarding the processing of the related personal data.

2 Processing of personal data

2.1 The applicable personal data law obliges a controller to ensure that the processor to whichthe controller transfers data complies with certain requirements and conditions. The agreement has been concluded to ensure that these requirements in the personal data laware complied with. The processor is obliged to comply with the personal data protection rules currently in force regarding the processing of personal data.

2.2 The processor is, on behalf of the controller, processing following general information: *(Allinformation that is not sensitive information)*

- → User names, e-mail addresses, telephone numbers of employees in the data controller's organization
- → Names, e-mail addresses, phone numbers and addresses of customers and suppliers
- → Location data and deviceID of registrations made on the App (optional)

The processor is, on behalf of the controller, processing following sensitive personal information: (Information on racial or ethnic origin, political, religious or philosophical beliefs or trade union affiliation, health information, sexual orientation and information, as well as information on crimes and genetic and biometric data)

- → No sensitive information

2.3 The categories of registered persons to which personal data relate are primarily thecontrollers' employees, suppliers and partners.

3 Instruction

3.1 The extent of the tasks that the processor must deliver and support means that, under theterms of the Parties license- and service agreement, there will be different forms of processing personal data.

3.2 The processor solely acts on the basis of documented instructions from the controller. The processor must ensure that the personal transferred are not utilized for other purposes or otherwise processed than what is stated in the instruction. The processor may not, in any event, disclose the personal data to third parties unless such disclosure follows the law or adecision of a national or international court/data protection authority or consent from the controller for the disclosure.

3.3 The processor processes both personal data on behalf of the controller in connection withthe data controller's general operation and in connection with testing of the software provided to the controller.

3.4 When the processor provides IT support in connection with the controller's general operation, the processor may only perform the task that the controller specifically requests, including access, copy, move and collate data. However, the processor must always move thecontroller's data if this is for security reasons. The processor must never delete the controller's data without a specific (written) instruction.

3.5 When the processor provides IT support in connection with test/development of the controller's software/systems, this is done by taking a copy/backup of the controller's systemin agreement with the controller (test data). This copy/backup will in some cases contain personal data. In this connection, the processor is entitled to utilize the test data for all typesof test/development in connection with the development of the software/system. Therefore,the processor must always access, move, collate, copy, separate or delete personal data contained in test data.

3.6 If, according to the processor, an instruction contravenes The Personal Data Act or ThePersonal Data Regulation, the processor must inform the controller accordingly.

4 Processing a request from a registered person

4.1 The processor must, as far as possible, assist the controller in fulfilling the controller's obligations to respond to requests for the exercise of the rights of the data subjects, including insight, rectification, limitation or deletion if the relevant personal data is processedby the processor. If the processor receives a request from a registered person, the processor is obliged to inform the controller accordingly.

4.2 The controller must cover all data processing costs of such assistance, including sub processors. The processor's assistance is settled at the processor's timetable at any time.Before the work is initiated by the processor the controller is notified. The controller may request a forecast at any time.

5 Geographical requirements

5.1 The processing of personal data that the processor undertakes on the instructions of thecontroller may only be performed by the processor or sub processor within the EU. The processor may not allow data processing to take place outside the EU limits without the controller's written consent.

6 Precautionary measures

6.1 The processor must take appropriate technical and organizational precautionary measures against accidental or illegal destruction, loss or deterioration of information, as well as unauthorized disclosure, abuse of processed in breach of The Personal Data Protection Act.

6.2 Therefore, the processor has established several safety requirements to be followed by all employees and a number of technical requirements for the protection of all IT equipment and network. There are also instructions for employee processing of personal data utilizingremote connection.

6.3 The processor has also ensured that only persons authorized to do so have access to thepersonal data/data processed on behalf of the controller.

6.4 The processor is subject to confidentiality in respect of all of the information, including personal data, which is available to the processor. The processor is required to process allreceived material and all

information received with full confidentiality. On request from the controller, the processor must provide the controller with a copy of the processor's IT Security Policies and Contingency Plan, which describes the precautionary measures initiated by the processor. Upon request, the processor must provide documentation that the precautionary measures have been initiated and supervised.

7 Utilisation of sub processors

7.1 Upon the conclusion of this agreement the controller accepts that the processor is entitled to utilize and substitute the sub processor, provided that: a) any new sub processor complies with the corresponding terms set forth in the agreement; and b) the controller, at the latest at the commencement of any other sub processor processing personal data, for which the controller is responsible for, is informed of the identity of the new sub processor.

7.2 In any event, the processor must inform the controller if it utilizes sub processors.

7.3 The sub processor is subject to the processor's instructions. The processor has also entered into a Data Processing Agreement with the sub processor in which it is ensured that the sub processor meets requirements similar to those provided to the processor under the agreement.

7.4 Costs incurred in establishing the contractual relationship with a sub processor, including costs for the preparation of a Data Processing Agreement and possible establishment of a basis for transfer to third countries must be defrayed by the processor, unless the controller has requested to utilize a particular sub processor. In that case, all costs are defrayed by the controller.

7.5 If the controller may wish to instruct the sub processor directly, this should only be done after consultation with and through the processor. If the controller chooses to directly instruct the sub processor, then the processor is exempt from liability and consequence of such instructions, and the controller is liable for any costs that the instruction may cause to the processor and sub processor. The processor is entitled to invoice the controller with the usual hourly rate for all working hours that such direct instruction may cause to the processor.

7.6 At the present, the processor is utilizing the following sub processors to operate and service the IT-systems of the processor:
7.6.1 ITSecurity A/S, CVR-no. 26091896

8 Security breach

8.1 If the processor becomes aware of a security breach, which means a breach of security that leads to accidental or illegal destruction, loss, alteration, unauthorized disclosure or access topersonal data stored or otherwise processed, the processor is required to, without unnecessary delay, seek to locate such breaches and seek to minimize the occurrence of injury, and to the extent that it is possible to re-establish any lost data.

8.2 The processor is also obliged to inform the controller without undue delay after being awarethat there has been a violation of personal data security. The processor must then, without undue delay, notify the controller with a written statement that must, as far as possible, contain:

8.3 A description of the nature of the breach, including the categories and the approximatenumber of registered and registered personal data.

8.3.1 Name and contact details of the person at the processor, (to be contacted by theauthorities in the event of a security breach)

8.3.2 A description of the likely consequences of the breach.

8.3.3 A description of the measures taken or proposed by the processor or sub processorto handle the violation, including measures to limit its possible adverse impact.

8.4 For that matter, it is not possible to provide the information as one, the information may becommunicated in stages without unnecessary delay.

Similarly, the sub processor utilized must be instructed to inform the processor withoutunnecessary delay.

9 Termination of the agreement

9.1 The agreement enters into force that the Parties' signature.

9.2 I the event that the license- and service agreement terminates, regardless of the reason forthis, the agreement will terminate as well. Upon termination of the agreement, the controller has the right to obtain all stored information from the processor on a readable medium. The controller pays all related costs.

9.3 If the processor undertakes hosting for the controller, it must as soon as possible and no laterthan 2 weeks before the termination of the hosting- and support

services agreement, inform the processor in writing of the wishes of the controller in relation to the processed information, including who to provide the information to and in what way. Based on this conclusion, a specific agreement between the Parties on extradition and deletion of all data will be formed.

9.4 All information must be delivered and/or deleted within 1 month after the end of the license-and service agreement.

10 Changes to the agreement

10.1 This agreement may only be amended if there is agreement between the Parties. Changes tothe agreement must be made in writing, signed by both Parties and attached to this agreement.

11 Governing law

11.1 The agreement is governed by Danish law.

12 Signatures

The processor:

Name:	**Signature:**	**Date:**
Michael Paarup		03-11-2022
Navn		

The controller:

Name:	**Signature:**	**Date:**
Navn		