

Data Processor Agreement

Regarding RentLog

Between

The Data Controller

Name:

CVR:

Address:

Zip & City:

Country:

and

The Data Processor:

mSystems ApS

CVR 39424207

Vejlsøvej 51

8600 Silkeborg

Denmark

who each are a "party" and together constitute the "parties."

On the nature and scope of the agreement

This agreement governs the processing of personal data carried out by the data processor on behalf of the data controller. Where, in certain cases, the data controller itself acts as a data processor for a third party (the original data controller), this agreement shall correspondingly function as a sub-processor agreement, and the term "the data controller" shall in that context be understood as "the data processor".

Unless expressly stated otherwise, the terms "the data controller" and "the data processor" shall therefore be interpreted in accordance with the specific allocation of roles in the relevant processing relationship.

The parties have subsequently agreed on the following standard contractual clauses (the "Clauses") for the purpose of complying with the General Data Protection Regulation and ensuring the protection of privacy and the fundamental rights and freedoms of natural persons.

Table of Contents

1.	Preamble	3
2.	The Data Controller's Rights and Obligations.....	3
3.	The Data Processor Acts According to Instructions	4
4.	Confidentiality	4
5.	Processing Security	4
6.	Use of Sub-Processors	5
7.	Transfer to Third Countries or International Organizations.....	6
8.	Assistance to the Data Controller	6
9.	Notification of Personal Data Breaches	7
10.	Deletion and Return of Information	8
11.	Audit, including inspection	8
12.	Agreement on Other Matters	8
13.	Commencement and Termination	8
14.	Contact Persons for the Data Processor	9
	Appendix A: Information on Processing	10
	Appendix B: Sub-processors	12
	Appendix C Instructions regarding the processing of personal data	14
	Appendix D Regulation of Other Matters by the Parties	19

1. Preamble

- 1.1. These Clauses lay down the rights and obligations of the data processor when processing personal data on behalf of the data controller.
- 1.2. These Clauses are drafted with a view to the parties' compliance 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 (the General Data Protection Regulation).
- 1.3. In connection with the provision of RentLog, the data processor processes personal data on behalf of the data controller in accordance with these Clauses.
- 1.4. The Clauses have precedence over any corresponding provisions in other agreements between the parties.
- 1.5. Four annexes are attached to these Clauses, and the annexes constitute an integral part of the Clauses.
- 1.6. Annex A contains detailed information about the processing of personal data, including the purpose and nature of the processing, the type of personal data, the categories of registered individuals, and the duration of the processing.
- 1.7. Annex B contains the data controller's conditions for the data processor's use of sub-processors and a list of sub-processors that the data controller has approved for use.
- 1.8. Annex C contains the data controller's instructions regarding the data processor's handling of personal data, a description of the minimum security measures that the data processor must implement, and how supervision of the data processor and any sub-processors is conducted.
- 1.9. Annex D contains provisions concerning other activities that are not covered by the Clauses.
- 1.10. The Clauses and accompanying annexes must be kept in writing, including electronically, by both parties.
- 1.11. These Clauses do not release the data processor from obligations that the data processor is subject to under the General Data Protection Regulation or any other legislation.

2. The Data Controller's Rights and Obligations

- 1.1. The data controller is responsible for ensuring that the processing of personal data is conducted in accordance with the General Data Protection Regulation (see Article 24 of the regulation), data protection provisions of other EU laws, or the national laws of member states¹, and these Clauses.
- 1.2. The data controller has the right and duty to make decisions about the purposes for which and how personal data may be processed.
- 1.3. The data controller is responsible, among other things, for ensuring that there is a legal basis for the processing of personal data which the data processor is instructed to carry out.

¹ The references to 'Member States' in these provisions shall be understood as references to 'EFTA Member States'

3. The Data Processor Acts According to Instructions

- 3.1. The data processor may only process personal data based on documented instructions from the data controller unless required to do so by EU law or the national law of the member states to which the data processor is subject. This instruction must be specified in Annexes A and C. Subsequent instructions may also be given by the data controller during the processing of personal data, but the instruction must always be documented and kept in writing, including electronically, along with these Clauses.
- 3.2. The data processor shall immediately inform the data controller if, in its opinion, an instruction is in violation of this regulation or data protection provisions of other EU laws or national laws of member states.

4. Confidentiality

- 4.1. The data processor may only grant access to personal data processed on behalf of the data controller to persons who are subject to the data processor's instructions, who have committed themselves to confidentiality, or are subject to an appropriate statutory duty of confidentiality, and only to the extent necessary. The list of persons who have been granted access must be reviewed continually. Based on this review, access to personal data may be closed if it is no longer necessary, and thereafter, the personal data should no longer be accessible to these persons.
- 4.2. The data processor must be able to demonstrate at the request of the data controller that the relevant persons who are subject to the data processor's instructions are subject to the confidentiality obligation.

5. Processing Security

- 5.1. Article 32 of the General Data Protection Regulation stipulates that the data controller and the data processor, taking into account the current state of the art, the costs of implementation, and the nature, scope, context, and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk.

The data controller must assess the risks to the rights and freedoms of natural persons posed by the processing and implement measures to address these risks. Depending on their relevance, this may include:

- a. Pseudonymization and encryption of personal data
 - b. Ability to ensure ongoing confidentiality, integrity, availability, and resilience of processing systems and services
 - c. 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 organizational measures for ensuring the security of the processing.
- 5.2. According to Article 32 of the regulation, the data processor, independent of the data controller, must also assess the risks to the rights of natural persons posed by the processing and implement measures to address these risks. For this assessment, the data controller must provide the necessary information to the data processor to enable it to identify and evaluate such risks.

- 5.3. Moreover, the data processor must assist the data controller in complying with the data controller's obligation under Article 32 of the regulation by, among other things, providing the necessary information about the technical and organizational security measures that the data processor has already implemented in accordance with Article 32 and any other information necessary for the data controller to fulfill its obligation under Article 32.

If addressing the identified risks, in the assessment of the data controller, requires the implementation of additional measures beyond those measures already implemented by the data processor, the data controller shall specify the additional measures to be implemented in Annex C.

6. Use of Sub-Processors

- 6.1. The data processor must fulfill the conditions outlined in Article 28(2) and (4) of the General Data Protection Regulation to use another data processor (a sub-processor).
- 6.2. Thus, the data processor may not use a sub-processor to fulfill these Provisions without prior general written approval from the data controller.
- 6.3. *The data processor has the data controller's general authorisation to engage sub-processors. The data processor shall notify the data controller in writing of any planned changes concerning the addition or replacement of sub-processors with at least six (6) weeks' prior notice, thereby giving the data controller the opportunity to object to such changes before the use of the relevant sub-processor(s).*

A longer notice period for notification in connection with specific processing activities may be specified in Appendix B. The list of sub-processors already approved by the data controller is set out in Appendix B.

- 6.4. When the data processor uses a sub-processor in the performance of specific processing activities on behalf of the data controller, the data processor must, through a contract or other legal document under EU law or the national law of the Member States, impose on the sub-processor the same data protection obligations as those set forth in these Provisions, thereby ensuring the necessary guarantees that the sub-processor will implement the technical and organizational measures in such a way that the processing complies with the requirements of these Provisions and the General Data Protection Regulation.

The data processor is therefore responsible for requiring the sub-processor to comply with, at a minimum, the data processor's obligations under these Provisions and the General Data Protection Regulation.

- 6.5. Sub-processor agreement(s) and any subsequent amendments thereto shall be provided - upon the data controller's request - in copy to the data controller, who thereby has the opportunity to ensure that similar data protection obligations as set forth in these Provisions are imposed on the sub-processor. Provisions regarding commercial terms that do not affect the data protection content of the sub-processor agreement need not be sent to the data controller.
- 6.6. The data processor shall include the data controller as a third-party beneficiary in its agreement with the sub-processor in case of the data processor's bankruptcy, enabling the data controller to enforce its rights against sub-processors, such as instructing the sub-processor to delete or return the personal data.
- 6.7. If the sub-processor fails to fulfill its data protection obligations, the data processor remains fully liable to the data controller for the fulfillment of the sub-processor's obligations. This does not affect the rights of the data subjects under the General Data Protection Regulation, including in particular Articles 79 and 82, against the data controller and the data processor, including the sub-processor.

7. Transfer to Third Countries or International Organizations

- 7.1. Any transfer of personal data to third countries or international organizations may only be made by the data processor based on documented instructions from the data controller and must always be in accordance with Chapter V of the General Data Protection Regulation.
- 7.2. If the transfer of personal data to third countries or international organizations, which the data processor has not been instructed to make by the data controller, is required under EU law or the national law of the Member States to which the data processor is subject, the data processor must inform the data controller of this legal requirement before processing, unless the relevant law prohibits such notification for reasons of important public interest.
- 7.3. Without documented instructions from the data controller, the data processor may not, within the framework of these Provisions:
 - a. Transfer personal data to a data controller or data processor in a third country or international organization
 - b. Entrust the processing of personal data to a sub-processor in a third country
 - c. Process the personal data in a third country
- 7.4. The data controller's instructions regarding the transfer of personal data to a third country, including the possible transfer basis in Chapter V of the General Data Protection Regulation, upon which the transfer is based, shall be specified in Appendix C.6.
- 7.5. These Provisions shall not be confused with standard contractual clauses as referred to in Article 46(2)(c) and (d) of the General Data Protection Regulation, and these Provisions cannot constitute a basis for the transfer of personal data as referred to in Chapter V of the General Data Protection Regulation.

8. Assistance to the Data Controller

- 8.1. The data processor assists, considering the nature of the processing, as far as possible the data controller by means of appropriate technical and organizational measures in fulfilling the data controller's obligation to respond to requests for the exercise of the rights of the registered individuals as laid down in Chapter III of the General Data Protection Regulation.

This means that the data processor should assist the data controller as much as possible in ensuring compliance with:

 - a. The duty to inform when collecting personal data from the data subject.
 - b. The duty to inform when personal data have not been collected from the data subject.
 - c. The right of access.
 - d. The right to rectification.
 - e. The right to erasure ("the right to be forgotten").
 - f. The right to restriction of processing.

- g. The obligation to notify in the context of 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.
- 8.2. In addition to the data processor's obligation to assist the data controller as per Clause 5.3, the data processor also assists, considering the nature of the processing and the information available to the data processor, the data controller with:
- a. The data controller's obligation to report personal data breaches to the competent supervisory authority (the Data Protection Agency) without undue delay and, if possible, no later than 72 hours after having become aware of it, 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 communicate the personal data breach to the data subject without undue delay, where the breach is likely to result in a high risk to the rights and freedoms of natural persons.
 - c. The data controller's obligation to conduct an impact assessment of the envisaged processing activities on the protection of personal data (a data protection impact assessment).
 - d. The data controller's obligation to consult the competent supervisory authority (the Data Protection Agency) prior to processing if 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.
- 8.3. The parties must specify in Annex C the necessary technical and organizational measures with which the data processor should assist the data controller, as well as the extent and scope. This applies to the obligations under Clauses 9.1 and 9.2.

9. Notification of Personal Data Breaches

- 9.1. The data processor shall notify the data controller without undue delay after becoming aware of a personal data breach.
- 9.2. The data processor's notification to the data controller should, if possible, occur no later than 24 hours after becoming aware of the breach, so that the data controller can fulfill its obligation to report the data breach to the competent supervisory authority, according to Article 33 of the General Data Protection Regulation, within 72 hours.
- 9.3. In accordance with Clause 9.2. the data processor shall assist the data controller in reporting the breach to the competent supervisory authority. This means that the data processor must help provide the following information, which according to Article 33(3) should be included in the data controller's notification of the breach to the competent supervisory authority:
- a. 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. The likely consequences of the personal data breach.
 - c. 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.

- 9.4. The parties must specify in Annex C the information that the data processor is to provide in connection with its assistance to the data controller in fulfilling its obligation to report personal data breaches to the competent supervisory authority.

10. Deletion and Return of Information

- 10.1. Upon termination of the services related to the processing of personal data, the data processor is obliged to delete all personal data processed on behalf of the data controller and confirm to the data controller that the data has been deleted unless EU law or national law of the member states requires the storage of the personal data.

11. Audit, including inspection

- 11.1. The data processor shall make available all information necessary to demonstrate compliance with Article 28 of the General Data Protection Regulation and these Clauses, to the data controller, and facilitate and contribute to audits, including inspections, conducted by the data controller or another auditor authorized by the data controller.
- 11.2. Procedures for the data controller's audits, including inspections, with the data processor and sub-processors are specified in Annex C.7. and C.8.
- 11.3. The data processor is obliged to allow supervisory authorities, which under applicable legislation have access to the data controller's or data processor's facilities, or representatives acting on behalf of the supervisory authorities, access to the data processor's physical facilities upon proper identification.

12. Agreement on Other Matters

- 12.1. The parties may agree on other provisions regarding the service relating to the processing of personal data, such as liability, as long as these other provisions do not directly or indirectly contradict the Clauses or impair the fundamental rights and freedoms of the data subjects as stipulated by the General Data Protection Regulation.

13. Commencement and Termination

- 13.1. The provisions come into effect on the date of signature by both parties.
- 13.2. Both parties may request renegotiation of the provisions if legal changes or impracticalities in the provisions give cause for this.
- 13.3. The provisions are valid as long as the service regarding the processing of personal data lasts. During this period, the provisions cannot be terminated unless other provisions regulating the delivery of the service concerning the processing of personal data are agreed upon between the parties.
- 13.4. If the delivery of the services concerning the processing of personal data ceases, and the personal data have been deleted or returned to the data controller in accordance with Provision 10.1 and Annex C.4, the provisions can be terminated with written notice by both parties.

On behalf of the data controller:

Name:

Title:

Phone:

E-mail:

Date and Signature:

On behalf of the data processor:

Name: Anja Kjeldahl Østergaard

Position: Director

Telephone Number: +45 40 37 16 31

Email: anja@msystems.dk

Date and Signature:

06-10-2025



14. Contact Persons for the Data Processor

14.1. The parties may contact each other via the contact persons listed below.

14.2. The parties are obligated to continuously inform each other of any changes regarding contact persons.

Name: Anja Kjeldahl Østergaard

Position: Director

Telephone Number: +45 40 37 16 31

Email: anja@msystems.dk

A.1. Purpose of the Data Processor's Processing of Personal Data on Behalf of the Data Controller

The purpose of the processing is to enable the data controller to use the RentLog system, which is developed and owned by the data processor. The system is made available to the data controller for the purpose of managing processes related to the rental and lending of vehicles, including documentation and customer communication.

The processing covers the personal data that the data controller registers in RentLog concerning its customers.

The system is used to support communication with end customers in connection with the rental agreement where such use has been agreed, including the sending of messages containing rental contracts and similar documents.

Where the data controller itself acts as a data processor for a third party (e.g. a car dealer), the data processor carries out the processing as a sub-processor on behalf of the original data controller.

A.2. Nature of the Data Processor's Processing of Personal Data on Behalf of the Data Controller

The data processor's processing of personal data primarily consists of operating and maintaining the RentLog system, including processing and storing the personal data that are registered or transferred to RentLog in connection with the administration of rental agreements, including to:

- Receive, register, and store information about companies, private customers, users, and vehicles.
- Support communication with customers, including the sending of messages containing rental contracts and similar documents.
- Provide technical support to, and carry out troubleshooting for, the data controller.
- Delete customer data in accordance with the agreement entered into, so that the customer's data are removed.
- Delete or anonymise other information in accordance with the data controller's instructions.

For data controllers who use an integration between RentLog and an external DMS system (Dealer Management System), the processing may also include the automatic transfer, receipt, and updating of information about customers and vehicles from the DMS system to RentLog. The purpose of the integration is the automatic exchange and updating of information between the systems.

Communication with end customers, including the sending of rental contracts, is carried out solely on the instructions of the data controller. It is the data controller in the specific situation who is responsible for ensuring that the necessary legal basis and any required consents under the Danish Marketing Practices Act and the General Data Protection Regulation are in place for such communications.

The data processor does not carry out any independent processing, matching, or enrichment of data from the DMS system and processes the data solely on the instructions of the data controller as part of the provision of RentLog's functionality.

A.3. The Processing Involves the Following Types of Personal Data about the Registered

The following information about the data controller's customers is processed:

- Customers of the data controller: full name, address, telephone number, email address, driver's licence number, and, where applicable, CPR number.
- Registration number of the customer's own vehicle.
- If the customer enters into the rental agreement through their employer, the company name, CVR number, address, telephone number, and email address are registered.
- Any internal notes – e.g. specific requests from a customer. Internal notes are the sole responsibility of the data controller.
- Any external notes – e.g. a description of vehicle damage. External notes are the sole responsibility of the data controller.
- Employees of the data controller: full name, email address, and the data controller's name, address, and CVR number.

In addition, technical and operational data are processed as part of RentLog's functionality, including login and access data, technical event data, etc. Such data are used solely for system operation, security, support, and troubleshooting.

As a general rule, only ordinary personal data covered by Article 6 of the General Data Protection Regulation are processed.

A.4. The Processing Involves the Following Categories of Registered

- Customers who borrow/rent or have borrowed/rented a demo, loan, or rental car from the data controller.
- Selected employees of the data controller, who are authorized to use the RentLog system.

A.5. The Data Processor's Processing of Personal Data on Behalf of the Data Controller Can Commence After the Provisions Come into Effect. The Processing has the Following Duration

The processing is not time-limited and lasts until the agreement is terminated or dissolved by one of the parties.

Appendix B: Sub-processors

B.1. Approved Sub-processors

Upon the commencement of these provisions, the data controller has approved the use of the following sub-processors

Name	CVR	ADRESS	processing description	Location(s) for processing
ScanNet A/S	DK 29412006	Højvangen 4 8600 Skanderborg	Hosting of servers for RentLog, including firewall management and backup	Denmark
ONLINECITY.IO ApS	DK 27364276	Buchwaldsgade 50 5000 Odense	SMS service for sending contracts to the customer/driver of a demo, loan, or rental car.	EU
Brevo S.A.S.	FR 80498019298	106 boulevard Haussmann, 75008 Paris, Frankrig	Distribution of newsletters and service announcements	EU (DE + FR primarily)
SMTP2GO	1842323	Epic Centre, 96-106 Manchester Street, Christchurch 8011, New Zealand	Email SMTP Service	EU (Amsterdam)
Zendesk Inc.	2894469 (Delaware, USA)	989 Market Street, San Francisco, CA 94103, USA	Customer Support Platform	EU (Frankfurt / Dublin)

By using Billwerk + online payment solution in RentLog the Data Controller accepts the use of following sub processors.

Name	CVR	ADRESS	processing description	Location(s) for processing
Frisbii Denmark A/S	DK 32097901	Pilestræde 52A, 1. – 1112 Copenhagen K	Online payment service, allowing rental car customers to register their payment card and settle payments online.	Denmark

By using Digital signature solution in RentLog the Data Controller accepts the use of following sub processors.

Name	CVR	ADRESS	processing description	Location(s) for processing
Idura ApS	DK 35142207	Gammel Kongevej 3E 1610 Copenhagen V	Online signing of rental contracts with NemID and MitID	Denmark

B.2. Notice period for approval of sub-processors

If, due to unforeseen circumstances and without prior notice, the data processor is compelled to replace a sub-processor with a new sub-processor in order to maintain delivery of the system to the data controller, the failure to comply with the prior approval deadline set out in Clause 6.3 shall not constitute a breach.

However, the data processor shall immediately notify the data controller of such a situation, including the choice of the new sub-processor, and the data controller shall thereafter have six (6) weeks to decide whether the new sub-processor can be approved as a future sub-processor in accordance with these Clauses.

C.1. Object/Instruction of the Processing

The data processor processes personal data solely on the instructions of the data controller and for the purpose of delivering, operating, and maintaining the RentLog system and related services, as described in Appendix A.

The data processor may process personal data only to the extent necessary to fulfil the agreement and the data controller's written or otherwise documented instructions. The data processor shall not use the data for its own purposes or for purposes that have not been expressly agreed between the parties.

In accordance with Appendix A.2, the data processor's processing of personal data includes, inter alia:

- Receiving, registering, and storing information about companies, private customers, users, and vehicles.
- Supporting communication with customers, including the sending of messages containing rental contracts and similar documents.
- Providing technical support to, and carrying out troubleshooting for, the data controller.
- Deleting customer data in accordance with the agreement entered into, so that the customer's data are removed.
- Deleting or anonymising other information in accordance with the data controller's instructions.

The data processor supports the functionality in RentLog that enables communication with end customers, including the transmission of rental contracts. Such communications are carried out solely on the instructions of the data controller.

It is the data controller in the specific situation (e.g. the dealer) who is responsible for ensuring that a valid legal basis and any required consents are in place in accordance with the Danish Marketing Practices Act and the General Data Protection Regulation.

If the data controller uses integrations between RentLog and external DMS systems, the data processor shall only carry out the automatic exchange and updating of data between the systems in accordance with the data controller's instructions. The data processor does not make any independent use of the data exchanged via integrations and has technical access only to the extent necessary to deliver the system's functionality.

C.2. Processing Security

The level of security shall reflect the following:

The processing comprises the personal data set out in section A.3. Taking into account the nature, scope, and purpose of the processing, in particular that only ordinary personal data are processed and that the volume of data is limited, it is assessed that a low to medium level of security shall be established.

The data processor is therefore entitled and obliged to decide which technical and organisational security measures shall be implemented in order to establish the necessary (and agreed) level of security.

However, the data processor shall, in all circumstances and as a minimum, implement the following measures, as agreed with the data controller:

The data processor shall protect personal data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure, or access. The measures shall be based on a risk assessment and subject to ongoing evaluation and improvement.

The data controller may at any time request documentation of the security measures implemented.

Organisational measures

- All employees complete mandatory awareness training in information security and data protection.
- New employees are introduced to the data processor's IT policies, code of conduct, and procedures upon commencement of employment.
- Access to personal data is granted solely on a work-related need-to-know basis.
- Access rights are reviewed regularly, at least once annually.
- Employees and external consultants sign confidentiality agreements.
- Procedures are in place for the closure of user access upon termination of employment or inactivity.
- Guidelines for remote and home working are in place, including requirements for secure connections, passwords, and screen locking.
- Changes to systems and functionalities are handled through change and release management processes.
- The data processor maintains contingency and business continuity plans for system operations.
- Internal audits and management reviews of information security are carried out at least once annually.

Physical measures

- Access to server facilities is secured through access control, alarm systems, and surveillance.
- Visitors are registered and escorted in secured areas.
- Workstations and server rooms are located and arranged in such a way that unauthorised visual access is limited.
- Documents and media containing personal data are stored in locked facilities and disposed of securely (e.g. shredding).

Technical measures

Hosting and infrastructure:

The data processor uses ScanNet as the hosting provider for the RentLog system and the associated databases.

ScanNet is responsible for operating the infrastructure, including firewall, backup, data storage, and physical security.

ScanNet is ISO- and ISAE-certified. Their compliance documentation is available here:

<https://www.zitcom.dk/vores-forretning/compliance>

All communication lines between ScanNet and RentLog / the RentLog app are encrypted using TLS, and no personal data are stored locally on users' devices (PCs or mobile phones).

All passwords in RentLog are encrypted (hashed and salted).

- ISO 27001 (information security)
- ISAE 3402
- ISAE 3000

ScanNet complies with the requirements of the EU General Data Protection Regulation (GDPR), and a data processing agreement has been entered into with ScanNet.

ScanNet performs daily backups of data, which are retained for a minimum of 21 days, and the data processor has implemented procedures for tested data restoration.

General technical measures

- Encryption of data in transit over external networks (TLS 1.2 or later).
- Two-factor authentication (2FA) for external access.
- Unique user IDs and access control based on roles and need.
- Automatic session time-out.
- Logging of user activities, access, and errors.
- Up-to-date patch and vulnerability management.
- Regular backups and testing of data restoration.
- Network segmentation between development, test, and production environments.
- Monitoring and alerting in the event of unauthorised login attempts or system errors.

Access control

- Access rights are granted and modified through a formal approval process.
- User permissions are reviewed on a regular basis.
- Automatic deactivation upon termination of employment or inactivity.
- Access logs are maintained, retained, and reviewed in accordance with internal policies.

C.3. Assistance to the Data Controller

The data processor shall, to the extent possible and within the scope and extent set out below, assist the data controller in accordance with Clauses 8.1 and 8.2 by implementing the following technical and organisational measures:

The data processor shall assist the data controller in obtaining the necessary information for the data controller's notification of a personal data breach, should a personal data breach occur at the data processor. The information shall enable the data controller to fulfil its obligations under Article 33(3) of the General Data Protection Regulation and shall, inter alia, include information on the nature of the personal data breach.

If the data processor receives a request from a data subject pursuant to Chapter III of the General Data Protection Regulation concerning personal data processed by the data processor on behalf of the data controller, the data processor shall immediately forward such request to the data controller's IT manager.

C.4. Retention Period/Deletion Routine

The data processor shall delete personal data in accordance with the data controller's documented instructions.

At the time of entering into this agreement, the following deletion procedures apply to the processing in RentLog:

1. Deletion of customer data:
The personal data contained in RentLog are stored by the data processor for five (5) years after the end of the rental period, in accordance with the applicable Danish Executive Order on the rental of motor vehicles, and are thereafter deleted automatically, or until the data controller requests that the data be deleted or returned.
Any image(s) of driving licences are automatically deleted two (2) months after the end of the rental period.
2. Deletion or return upon termination of the agreement:
Upon termination of the agreement, the data processor shall delete or return all personal data processed on behalf of the data controller, unless storage is required under EU law or national legislation.
3. Manual deletion upon instruction:
If the data controller requests deletion at an earlier point in time than set out above, the data processor shall carry out such deletion manually in accordance with the data controller's instructions.

C.5. Location of Processing

Processing of the personal data covered by these Clauses may not, without the prior approval of the data controller, take place at locations other than those of the data processor and the sub-processors listed in Appendix B.

C.6 Instructions Regarding Transfer of Personal Data to Third Countries

If the data controller does not, in these Clauses or subsequently, provide a documented instruction regarding the transfer of personal data to a third country, the data processor is not authorised to carry out such transfers within the framework of these Clauses.

The data controller acknowledges and has granted permission for the data processor, in general, to transfer personal data to locations in third countries as set out in the lists of approved sub-processors above. In this connection, the data processor shall ensure that the necessary transfer mechanism is in place in accordance with Clause 7.

C.7 Procedures for the Data Controller's Audits, Including Inspections, of the Processing of Personal Data Entrusted to the Data Processor

The data controller shall supervise the data processor's compliance with this agreement and applicable data protection legislation. As a general rule, such supervision shall be carried out by the data processor preparing and making available a self-assessment statement to the data controller once annually.

The self-assessment statement shall include an account of:

- the data processor's compliance with the General Data Protection Regulation,
- implemented and planned security measures,
- any changes in the use of sub-processors, and
- the results of internal controls, audits, or certifications, where relevant.

On the basis of the self-assessment statement, the data controller may request additional documentation, clarifications, or the implementation of supplementary measures if deemed necessary to ensure compliance with the General Data Protection Regulation and this agreement.

The data controller reserves the right, as needed, to carry out supplementary supervision or physical inspections, including at the locations or systems where the data processor processes personal data. Such inspections shall be conducted with reasonable prior notice and in cooperation with the data processor.

The data processor is obliged to make the necessary resources available for the conduct of supervision, including for the preparation of the annual self-assessment statement. The data controller shall bear its own costs associated with any physical inspections.

C.8 Procedures for Audits, Including Inspections, of the Processing of Personal Data Entrusted to Sub-Processors

The data processor shall ensure that appropriate supervision is carried out of all sub-processors that process personal data on behalf of the data controller.

The supervision shall be proportionate to the risk associated with the relevant processing and shall be carried out on a regular basis as well as in connection with material changes to the sub-processor's services or level of security.

Supervision of sub-processors shall be carried out by the data processor. The data controller may request the data processor to provide the necessary documentation to demonstrate that the sub-processor complies with the requirements arising from this agreement and the General Data Protection Regulation.

Upon request from the data controller, the data processor shall present:

- relevant audit or certification reports (e.g. ISO 27001, ISAE 3402, ISAE 3000),
- descriptions of the sub-processor's technical and organisational security measures, and
- information on any material changes in the sub-processor's circumstances that may affect processing security.

For sub-processors such as ScanNet, supervision is carried out through a review of the available security and compliance reports made available by the supplier.

On the basis of the material provided by the data processor, the data controller may request additional documentation or supplementary controls if deemed necessary to ensure an appropriate level of security.

D.1 Compensation

The parties shall be liable for damages in accordance with the general rules of Danish law on liability, provided, however, that neither party shall be entitled to claim compensation for indirect losses or consequential damages, regardless of whether such indirect losses or consequential damages are suffered by the data controller, the data processor, or a third party. Loss of business opportunities, loss of profit, operating losses, loss of revenue, loss of goodwill, and loss of data, including losses incurred in connection with the restoration of data, shall in all cases be considered indirect losses or consequential damages.

The data processor's total liability for damages under the Main Agreement shall, however, under no circumstances exceed the amount invoiced under the Main Agreement in the preceding year.

D.2 Error Reporting

In order to continuously improve the stability of RentLog, mSystems reserves the right to send error reports from RentLog and the RentLog app to mSystems. The error reports contain no personal data relating to the data controller's customers. The error reports are used solely for the purpose of improving stability and for no other purpose.